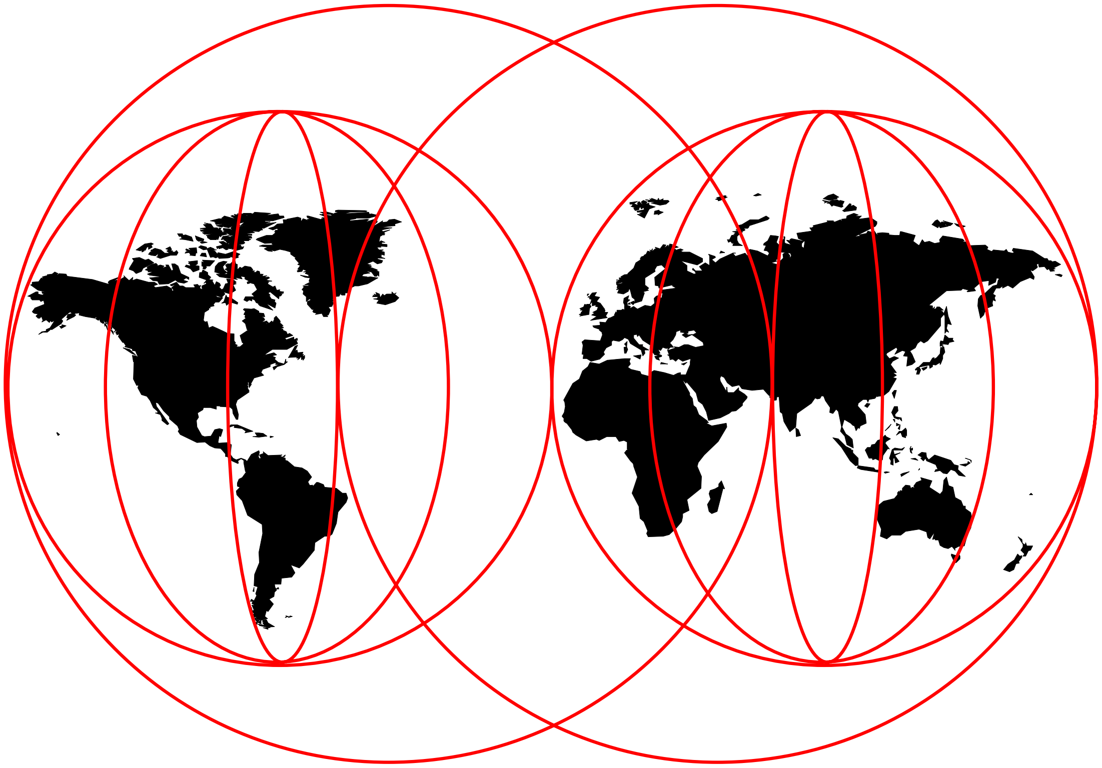
Netfinity Server Management

David Watts, Bernd Baeuml, John Doyle, Ricardo Rondon



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5208-00

SG24-5208-00

International Technical Support Organization

Netfinity Server Management

April 1998

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, "Special Notices" on page 199.

First Edition (April 1998)

This edition applies to IBM Netfinity Manager Version 5.1 and the Advanced Systems Management Adapter with Version 2.20 of the Configuration Utility. Servers used in the book are the Netfinity 7000, the Netfinity 5500, the PC Server 330 and the Netfinity 3500 running Windows NT Server 4.0, OS/2 Warp Server 4.0 and Novell NetWare 4.1.

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

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

Contents

Preface

This redbook describes how to use the managment hardware and software that is shipped with IBM Netfinity servers. In particular, it covers Netfinity Manager Version 5.1, the Advanced Systems Management Adapter and the management hardware that is integrated in the Netfinity 7000, 5500, 3500, 3000 systems and PC Server 330 and 325 systems.

The book explains each of the functions of Netfinity Manager as it applies to server management and goes into great detail on sending and receiving alerts from local and remote systems. We explain how to integrate a UPS into your managment environment and how to use the event scheduler. We examine the security ramifications of implementing remote access to your systems through Netfinity Manager.

The redbook also examines the Advanced Systems Management Adapter and how to configure it to send alerts and to let you dial into the server to perform remote diagnostics and recovery.

For each of our currently available server systems, we describe the system status indicators and management fuctions. We also explain how to install the Advanced Systems Management Adapter. For Microsoft Cluster Server systems, we have included a chapter on how to use IBM Cluster Systems Management, IBM's cluster administration product.

Sample scenarios are provided to give the reader a deeper understanding of the process involved in configuring the software and hardware and show what the products can do in combination. We describe how to perform specific tasks explaining each step of the process in detail.

The redbook also provides steps on how to integrate Netfinity Manager into Microsoft's Systems Management Server to maximize a customer's investment in SMS and Netfinity.

This redbook is aimed at customers, business partners and IBMers who need to how to implement Netfinity Manager and the Advanced Systems Management Adapter in IBM's servers. It will help them tailor and configure the products and show them how to best use them to maximize your investment in IBM technology.

The Team That Wrote This Redbook

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

David Watts is an Advisory Specialist for Netfinity Servers at the ITSO Center in Raleigh. He conducts residencies and writes redbooks on IBM Netfinity Servers and network operating systems. His most recent publications include the *Clustering and High Availability Guide for Netfinity and PC Servers* and fourth edition of the *IBM Netfinity and PC Server Technology and Selection Reference*. He has been working with PCs for the past 14 years, most recently as a server specialist for the IBM PC Company in Australia. He has a Bachelor of Engineering degree from the University of Queensland and had worked for IBM Australia for nine years.

Bernd Baeuml is a Level 2 Post Sales Support Engineer for the EMEA region based in Greenock, Scotland. He has two years of experience in supporting IBM hardware and software. He is involved in a pilot project that tests remote support capabilities to implement IBM's “Calling Home” strategy in EMEA. He has a Masters of Engineering degree from the Hochschule fuer Technik and Wirtschaft Dresden. He is PSE and CNE. His areas of expertise include Windows NT Server and Novell IntranetWare.

John Doyle is a Help Center Product specialist for the EMEA region based in Greenock, Scotland. He has four years experience in supporting IBM business partners and end users, particularly for the IBM Intel-based server range. He currently supports IBM Netfinity servers, the operating systems that run on them, and Netfinity Manager. He has an Honors degree from the University of Newcaslte-upon-Tyne.

Ricardo Rondon is a Level 2 Post Sale Support Engineer for Peru and Andean region. He has two years of experience working with hardware and software for both IBM Servers and Networking. He is PSE, MCSE, and CNE. His areas of experties include Windows NT Server and Communications Server.

Thanks to the following people in the International Technical Support Organization, Raleigh Center for their invaluable contributions to this project:

Paul Braun
Kathryn Casamento
Rufus Credle
Mike Haley
Barry Nusbaum

Thanks to the following IBMers:

Paul Chenger, Server Technology Center, Raleigh
Wouter Cloetens, Senior Server Specialist, Greenock
Jane Cornelius, Netfinity Server Information Development, Raleigh
Susan Davi, Netfinity Management Software Brand Manager, Raleigh
Dottie Gardner, Netfinity Server Information Development, Raleigh
Dave Laubscher, Server Technology Center, Raleigh
David Leskovec, Service Processor Development, Raleigh
Wade Mahan, Netfinity Manager Development, Raleigh
Rick Muse, High Volume Server Development, Raleigh
Lee Pisarek, Server Technology Center, Raleigh
Debbie Richmond, IBM Photo Library, Thornwood
Randy Stark, Netfinity Manager Development, Raleigh
Eric Stonehouse, Service Processor Development, Raleigh
Angela Taylor, Netfinity Server Information Development, Raleigh
Jon Thompson, Netfinity Manager Development, Raleigh
Shawn Whalen, Worldwide IBM Netfinity Server Marketing, Raleigh
Ronny Winick, Server Technology Center, Raleigh

Thanks also to Jeff Meyer of American Power Conversion for his assistance.

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in “ITSO Redbook Evaluation” on page 211 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

For Internet users	`http://www.redbooks.ibm.com/`
For IBM Intranet users	`http://w3.itso.ibm.com/`

- Send us a note at the following address:

  `redbook@us.ibm.com`

Chapter 1. Introduction

Today's IT environments can be very complex. End users are so dependent on their systems that they are increasingly frustrated by system outages, print problems, anything that keeps them from being productive. And they expect immediate assistance from the help desk or support center to fix a problem or even just to show them how to use an application. IT personnel are challenged to keep system availability high, and also handle end-user requests quickly and efficiently. Yet their environments are more complex today than ever with diverse manageability tools that have no common characteristics and little to no integration.

All you want is to be able to spend more time managing your business and less time managing your IT assets.

IBM's goal for Netfinity systems is to provide a systems management solution that will provide you with comprehensive control of your IBM systems in this complex environment, thereby enabling you to spend more time on your business. Our systems management strategy is threefold:

1. Provide a standards-based foundation that removes the confusion and complexity as technology evolves. The foundation of this strategy is to help remove the guesswork from the industry confusion — because the foundation will be based on existing standards, and allied with other industry leaders such as Tivoli, Microsoft and Intel to help ensure that customers have access to the cutting edge of technology.
2. Provide industry-leading control of IBM PC-based systems in heterogeneous environments. We can accomplish this by developing value-add tools that allow you unparalleled control of your IBM systems during their life cycle — from procurement through retirement or disposal. Tools targeted at helping you reduce your total cost of ownership.
3. Provide seamless integration with leading enterprise and workgroup managers, for a comprehensive solution and clear, comprehensive systems management foundation that fits with your existing assets and grows with your business. Our strategy can initially support any management strategy that you choose because our foundation and value-add tools integrate with Tivoli Management Software (TME 10) Microsoft System Management Server (SMS) and Intel LANDesk.

The bottom line is the system management solution from IBM for servers allows you to run your business-critical applications with the confidence that they will be there when your end users need them. When this happens, you can spend less time running your networked systems and more time running your business, which is exactly what you want.

Today IBM has made great strides toward this systems management strategy. Netfinity Manager is central to this strategy, providing a suite of tools designed to help you reduce the total cost of owning your IBM server, desktop and mobile systems. Other products that are key to managing your IBM Netfinity and IBM PC Server systems during their life cycle are the Advanced System Management Adapter for remote monitoring and problem management, and ServerGuide to simplify installation and set up.

This redbook will concentrate on these products, explaining how they can be used to maximize your ability to manage you servers and the users they support. We describe the functions of IBM Netfinity Manager, the Advanced Systems Management Adapter and the management components of the IBM Netfinity and PC Server systems. We then provide example scenarios of how these products work together to provide a solid server management platform. Finally, we show how to integrate the products with Microsoft SMS.

Chapter 2. Netfinity Manager

This chapter describes what IBM Netfinity Manager is and how it can be used to maximize control over your servers.

2.1 Introduction

Netfinity Manager is IBM's comprehensive hardware systems management environment for IBM Netfinity and PC Servers. It provides an easy-to-use graphical set of local and remote services designed to make the server and client systems simple and affordable to manage. It is shipped with all IBM Netfinity and PC Server systems as part of ServerGuide. The whole aim of Netfinity Manager is to give you, the network administrator, a suite of tools designed to assist in the management and monitoring of you server platform both remotely and locally from the server console.

Netfinity Manager operates in a peer-to-peer mode that minimizes the need for expensive system management hardware. All that is required is the presence of a physical network or a serial link. Netfinity Manager has its own interprocess communication (IPC) system that is used for communication between Netfinity Manager modules and services, locally and when operating remotely over a network. It has a very flexible, modular design that allows for a variety of system-specific installations and plug-in options to be used.

There are two “flavors” of Netfinity Manager:

1. IBM Netfinity Manager
2. Client Services for Netfinity Manager (Client Services)

Wherever you want to *manage* some other PC or server, you would use Netfinity Manager. Whichever machines you want to be *manageable* remotely or only want that machine to be able to manage itself and no other machines, you would install Client Services for Netfinity Manager.

Netfinity Manager is included with every IBM PC Server and Netfinity system. One license of the manager code and 10 licenses of the Client Services are included.

What do I Install on My Servers?

There are two schools of thought. If you do all your administration from your own workstation and not from the server keyboard, then it makes sense to install Client Services on your servers. If you administer your servers while sitting at the keyboard, then you will need to install Netfinity Manager on your servers.

IBM Netfinity Manager and Client Services for Netfinity Manager (Client Services) are both split up in to two components:

1. Base program, comprised of a group of base services
2. User interface, comprised of a group of matching GUI components

During the installation of Netfinity Manager, all of the base services are installed. At the same time some optional plug-in modules are also installable. These are:

- Remote Workstation Control

- Service Processor Enhancement
- World Wide Web Enhancement
- Capacity Management

Each icon in the user interface has a corresponding base service. Each of these base/GUI combinations is explained in 2.3, “Functions” on page 10.

During the installation of Client Services, only the base services necessary to control the installed hardware are installed and depending on the type of client you request, the matching GUI components are also installed.

Note: All services will be installed if you are installing the Netfinity Manager regardless of whether the system has a DMI Service Layer, ECC Memory, a System Partition, a RAID adapter, or a PFA-enabled disk drive. This enables a network administrator to remotely access these services on other systems within the network.

We now discuss the two flavors of Netfinity Manager: Netfinity Manager and Client Services. In 2.3, “Functions” on page 10, we will go in to details about each of the functions. As this book is concerned in most part with the management of servers, Netfinity Manager will be the side of Netfinity that will be concentrated upon the most.

2.1.1 IBM Netfinity Manager

Netfinity Manager is the managing portion of the system. In a normal PC environment, this component would normally be installed on the administrator's workstation and/or the servers themselves.

Netfinity Manager is used for managing remote systems as well as the server or workstation it is installed on. As a result a Netfinity Manager installation includes the code for all Netfinity functions and communications drivers to enable management of all other machines with Netfinity installed. As well as having all the base services locally, it can include the following extra functions if they are chosen at install time:

- Remote Workstation Control
- Service Processor Enhancement
- World Wide Web Enhancement
- Capacity Management

For further details on all the Netfinity Manager functions, see 2.3, “Functions” on page 10.

2.1.2 Client Services for Netfinity Manager

Client Services for Netfinity Manager is the *managed* portion of the system. It can be configured in three client modes of operation:

1. Stand-alone client

   Stand-alone mode allows an individual user, who is not connected to a network, to effectively manage or monitor their own system including hardware, resources and performance. Only those base services and matching user interfaces that work with the installed hardware and do not require a network connected machine are installed.

2. Passive client

The passive client cannot manage itself. Instead, Netfinity Manager on another machine in the network must be used to manage this workstation or server. This mode is most effective for Network administrators who do not want individual users or server consoles to have management capability. Only the Alert Manager, Serial control and Security Manager functions are available on this machine.

3. Active client

   The active client can manage itself or it can be managed by other systems with Netfinity Manager installed. Like the other clients, only the services and network protocols required for this particular machine are installed.

2.1.2.1 Supported Platforms

Netfinity Manager runs on the following operating systems:

- OS/2 Warp V3.0, or later
- OS/2 Warp Server (including the SMP version)
- Windows 95
- Windows NT 3.51 or 4.0

Client Services for Netfinity Manager runs on the following operating systems:

- OS/2 Warp V3.0, or later
- OS/2 Warp Server (including the SMP version)
- Windows 95
- Windows NT 3.51 or 4.0
- NetWare 3.12, 4.1 or 4.11
- Windows 3.x

Netfinity Manager is designed to work with the following network protocols:

- NetBIOS
- TCP/IP
- IPX
- Serial
- SNA (LU. 6.2) (except on NetWare and Windows 3.x)

Note: For information on the revisions of network stacks supported, see Chapter 2 of *Netfinity Manager Quick Beginnings*.

2.2 Installing Netfinity Manager

As described in 2.1, “Introduction” on page 3, there are two “flavors” of Netfinity Manager:

1. IBM Netfinity Manager
2. Client Services for Netfinity Manager (Client Services)

This chapter describes how to install Netfinity Manager, Client Services and Netfinity Manager plug-in for the Advanced Systems Management Adapter for each of the following operating systems:

- Windows NT Server
- OS/2 Warp Server
- NetWare

The installation process for Windows NT and OS/2 Warp are basically the same and will be handled together.

2.2.1 Windows NT and OS/2 Warp

Netfinity Manager is supplied on the ServerGuide ApplicationGuide 3A CD-ROM. Insert it and change the appropriate directory:

```
ServerGuide ApplicationGuide 3A CD-ROM
│
├──┬─ Netfin
│  ├──┬─ EN
   │  ├──┬─ OS2
      │  ├──── Manager
      │  └──── Services
      ├──┬─ WINNT
      │  ├──── Manager
      │  └──── Services
      │
```

Run `INSTALL.BAT` for Windows NT or `INSTALL.CMD` for OS/2.

If you are installing on Windows NT you will get the option to install any of the following additional functions:

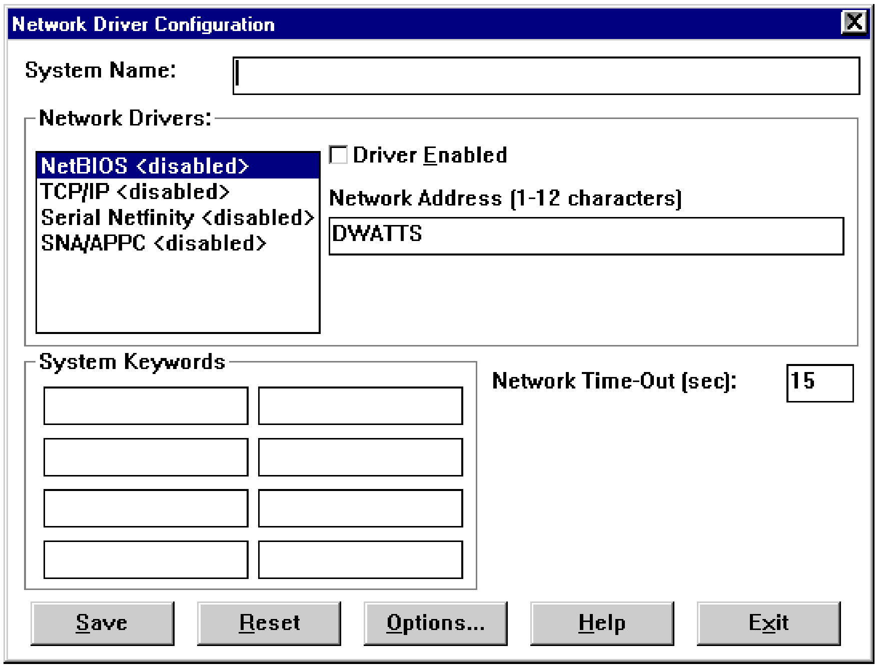
- Remote Workstation Control, as described in 2.3.14, “Remote Workstation Control” on page 19.
- Service Processor Enhancement, as described in 2.3.18, “Service Processor Manager” on page 21.
- World Wide Web Enhancement, as described in 2.3.22, “Web Manager Configuration” on page 22.
- Capacity Management, as described in 2.3.3, “Capacity Management” on page 12.

If you are installing on OS/2, you will not get the Capacity Management option as this is a WIN32 application for Windows NT and Windows 95 only. If you wish to use Capacity Management on your OS/2 server, you must install and run it from a Windows 95 or Windows NT system.

After you select the desired options, the installation will proceed.

2.2.1.1 Network Driver Configuration

After installation, Figure 1 on page 7 appears, letting you configure the software.



Network Driver Configuration

System Name:

Network Drivers:

NetBIOS <disabled>
TCP/IP <disabled>
Serial Netfinity <disabled>
SNA/APPC <disabled>

☐ Driver Enabled

Network Address (1-12 characters): DWATTS

System Keywords

Network Time-Out (sec): 15

Figure 1. Network Driver Configuration

This windows has the following fields:

- **System Name**

  This is the name that Netfinity Manager will report to a remote system. It can be anything you like up to 32 characters including spaces.

- **Network Drivers**

  This is a list of the protocols that Netfinity Manager detects on your system. The serial interface is always in the list.

  The supported drivers under OS/2 Warp and Windows NT are:

  – TCP/IP
  – NetBIOS
  – IPX
  – SNA/APPC
  – Serial

- **Driver Enabled**

  By default, all network protocols are disabled. In order for Netfinity Manager on this system to be accessible via a specific protocol, that protocol driver must first be enabled.

- **Protocol Addressing**

  If the selected protocol requires addressing information from you, a field will appear requesting the information, as follows:

  – NetBIOS: Network address
  – TCP/IP: (none)
  – Serial: Unique machine dialup name
  – SNA: Mode name
  – IPX: (none)

When enabling the IPX or TCP/IP Network Driver, the network address cannot be altered and it will not appear on the screen. No field will appear beneath the Driver Enabled check box if the IPX or TCP/IP Network Driver is selected.

When enabling the NetBIOS Network Driver, a network address will be assigned and displayed automaticaly in the Network Address field. To change this default name just enter a new address, however this address must be unique to network that the system is on. If this NetBIOS address is identical to the NetBIOS address of another system on the network, it will prevent Netfinity Manager from starting properly.

When enabling the Serial Netfinity driver, identify the system with a Unique Machine Dialup Name. This name can be up to 32 characters long, and must be unique to the system. If this name is not unique, it can prevent remote Netfinity Managers from using the Serial Connection Control service to access the system.

- **System Keywords**

  Enter your chosen keywords, remembering that they are case sensitive. This section is optional, but is useful for categorizing the servers and for later management in the Remote Systems Manager.

- **Network Time-Out**

  The Network Timeout field shows the number of seconds that Netfinity Manager will wait when attempting to communicate with a remote system that is not responding. If Netfinity does not establish contact with the remote system within this time, it cancels the communication attempt and displays an error. The Network Timeout default setting is 15 seconds. This default setting may not need to be altered, but is useful for systems that are under heavy load or are connecting over a unreliable or stressed links. Increasing it can help to correct application time-out problems.

Save your settings by clicking on **Save** and then exit by clicking on **Exit**. Netfinity Manager is now installed.

Under OS/2, you may presented with a box asking whether you want to route FFST/2 alerts to Netfinity Manager. If you would like to take advantage of this feature then select **Yes** to enable it. If you enable this feature you will be able to receive alerts from FFST/2-enabled products, such as IBM Warp Server or IBM Communications Manager.

For Windows and OS/2, you must reboot once the installation is complete.

2.2.1.2 Security

Once installation is complete, one user ID will be defined in the security manager, with all accesses granted. Since this user ID is the <PUBLIC> user ID, it means that everyone has access to your system.

The first step after installation and reboot should be to open the Security Manager, and revoke all disallowed actions to <PUBLIC>.

Security Not Set By Default!

If you do not change the security settings, any Netfinity Manager system will be able to access every function on your system. This can lead to disastrous results.

Don't forget to uncheck the box that authorizes security manager access. If this is box remains checked, <PUBLIC> will still have the ability to change the security access, regardless of whether or not they have that access now.

See 2.7, "Netfinity Manager Security Implications" on page 48 for more information about security.

2.2.2 NetWare

Only Client Services for Netfinity Manager is available for NetWare. You can install the Client Services for NetWare in two ways:

1. Client based
2. Server based

2.2.2.1 Client Based Installation

To install Client Services for NetWare on a Windows NT or Windows 95 client, follow these steps.

1. Map a Network drive of the server you want Client Services installed to
2. Insert the ServerGuide ApplicationGuide 3A CD-ROM. The installation program starts automatically.
3. Select your language
4. Select **Client Services for Netfinity for NetWare (Installation from a Windows NT client)**
5. Click on the install button.
6. When prompted, change your installation drive to your mapped network drive and change your the directory name to NETFIN.
7. When prompted, select you Client Services network interfaces you want enabled on your NetWare server.

   Note: Do **NOT** enable **Serial Netfinity**. Serial connections NetWare are not supported.
8. Follow the instruction to change your AUTOEXEC.NCF file. Add these lines to the bottom of the file:

   ```
   search add <vol>:netfin
   load netfbase.nlm
   ```
9. You can either restart the server or simply type the two commands you just added on the server console prompt.

2.2.2.2 Server Based Installation

If you wish to install Client Services for NetWare from your server console follow these steps.

1. Insert your ServerGuide CD-ROM in your server CD-ROM drive.
2. Mount the CD-ROM as a volume
3. At the console type:

   ```
   LOAD <vol:>NETFIN\EN\NETWARE\SERVICES\NETFINST.NLM
   ```

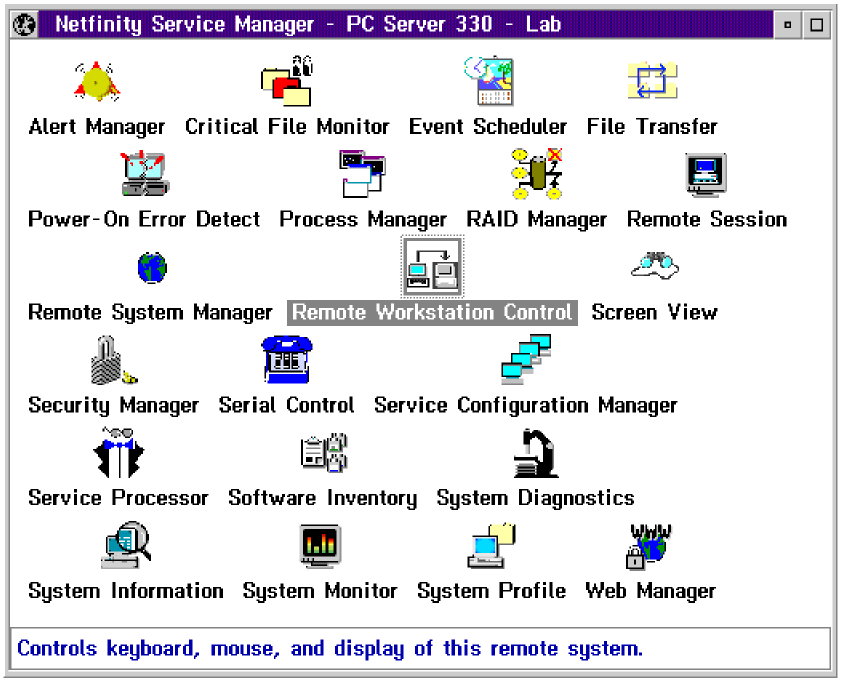
4. When prompted select the network driver you want to enable.
5. Confirm the changes to the AUTOEXEC.NCF file.
6. You can either restart the server or simply type the two commands you just added on the server console prompt.

Note: If you need to re-configure Client Services from your server console, issue the following command:

```
LOAD NFCONFIG.NLM
```

2.3 Functions

The Netfinity Manager main window consists of a set of icons which constitute the user interface component of Netfinity Manager and provide an interface to the base services. It is the base services that perform all the interactions with the hardware and communcations drivers. See for 2.1.1, "IBM Netfinity Manager" on page 4 and 2.1.2, "Client Services for Netfinity Manager" on page 4 for further details.



Controls keyboard, mouse, and display of this remote system.

Figure 2. A Typical Netfinity Manager Window

A full list of functions that are available in a standard installation are briefly discussed below and complete instructions on how to use each of these services can be found in the online help provided with the product. The following manuals are also available:

- *Netfinity Manager Quick Beginnings*
- *Netfinity Manager User Guide*
- *Netfinity Manager Command Reference*
- *Netfinity Services Quick Beginnings*
- *Netfinity Services User Guide*

These manuals are available on ServerGuide on the Book Factory CD in PostScript format. The files are in the \PUBS\EN directory.

- OWMGREN.PS — Netfinity Manager User's Guide
- OWSVCEN.PS — Client Services for Netfinity Manager User's Guide
- COMREFEN.PS — Netfinity Manager Command Reference
- NETSVCEN.PS — Client Services for Netfinity Manager for NetWare User's Guide

On the SoftwareGuide CD-ROM in the ServerGuide package you can also obtain these manuals in OS/2 Help File (INF) format. They are in the \PUBS\EN directory of that CD-ROM.

INF files can be viewed without additional software under OS/2. The viewer for Windows (XVIEW) can be obtained from

`http://www3.pc.ibm.com/techinfo/b216.html`

Extra! — Other Redbooks

You will also find other IBM Redbooks on Netfinity topics also on the Book Factory CD-ROM:

- CLHAGEN.PS — Clustering and High Availability Guide
- NOVLIGEN.PS — Novell NetWare Integration Guide
- RAIDGEN.PS — Implementing ServeRAID SCSI and SSA RAID Subsystems
- SSGEN.PS — Netfinigy Technology and Selection Reference
- WINLIGEN.PS — Windows NT 4.0 Integration Guide

2.3.1 Advanced System Managment

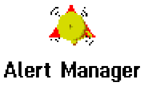
Advanced System Management

The Advanced System Management service (recently renamed from Service Processor Manager) enables communication between Netfinity Manager and the Advanced Systems Management Adapter or the Netfinity Advanced Remote Management. It can be used to configure and monitor many of your system's features. With the Advanced System Management service, you can configure events such as POST, loader, and O/S timeouts, critical temperature, voltage, and tamper alerts and redundant power supply failures. This service also enables you to dial-out and directly access and control a remote system's Advanced Systems Management Adapter or Advanced Remote Management processor.

In addition, the Advanced System Management service enables you to remotely monitor, record, and replay all textual data generated by a remote system during

POST. While monitoring a remote system during POST, you can enter key commands on your keyboard which will then be relayed to the remote system. A fuller description of this function can be found in Chapter 3, “Advanced Systems Management Adapter” on page 63.

2.3.2 Alert Manager



The Alert Manager is an extendable facility that allows receiving and processing of application-generated alerts. A predefined set of alert profiles is available to monitor the subsystems of the servers (for example RAID alerts, PFA alerts, ECC memory monitors).

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, generating an SNMP alert message, dialing out to a digital pager service (with a modem), or taking an application-defined action. Actions are user-definable, using a highly flexible action management interface. For further details see 2.4, “Alerts” on page 24.

You can list, view, and modify alerts from the command line using the NFALRTCL command. See Chapter 2 of *Netfinity Manager Command Reference* for details.

Alerts can also be generated from the command line using the GENALERT command. See Appendix G, “Netfinity Command Line Operations” of *Netfinity Manager User's Guide* for details.

2.3.3 Capacity Management

All Netfinity Manager 5.1 (or later) systems automatically monitor and store data on the performance of your system. Up to a month of data is stored on each system. You can use the Capacity Management feature to collect this data from multiple systems on your network, compile the data into reports, and view the data in simple to read line graphs. You can use Capacity Management to:

- Generate reports on data captured within the last month
- Schedule reports to be generated automatically at a later time
- View previously generated reports

Capacity Management includes extensive online help, including online tours and interactive help pages that guide you through all of Capacity Managements functions, making it especially simple to learn and understand this service.

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

Note: Capacity Management is a new function to Netfinity Manager v5.1 and to collect data from a remote system that system must be running Netfinity v5.1 or higher.

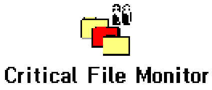
Refer to `http://www.pc.ibm.com/us/server/capmgr/` for more information and an online demo of the Capacity Management function.

2.3.4 Cluster Management

This icon is available when you have the MSCS (Microsoft Cluster Server) Cluster Administrator installed on your system. This includes the MSCS nodes and any remote cluster adminstrator consoles you've configured. Double-clicking on this icon starts IBM Cluster Systems Management, IBM's tool for improved MSCS management.

See Chapter 5, “IBM Cluster Systems Management” on page 117 for details on the tool.

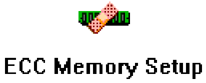
2.3.5 Critical File Monitor



Critical File Monitor enables you to be warned whenever critical system files on your system are deleted or altered. There is a set of standard files that can be monitored, and user-specified files can be added to the list. For example it will monitor the CONFIG.SYS for changes in its size, date and time stamp.

You can list, view, and modify the Critical File Monitor configuration from the command line using the NFCRTFCL command. See Chapter 3 of *Netfinity Manager Command Reference* for details.

2.3.6 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 non-maskable interrupt (NMI) if the ECC single-bit error threshold is exceeded.

Current IBM implementations of ECC memory, like EOS and ECC-P are not supported through this service. Only those systems using ECC controller and ECC memory. The PC Server 704 and the Netfinity 7000 are supported by ECC memory setup.

2.3.7 Event Scheduler

Event Scheduler

You can use Event Scheduler to automate many Netfinity Manager 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 Manager systems on your network. Scheduled events can be performed one time only, or can be performed according to a user-defined schedule.

A new feature in Netfinity Manager 5.01 or higher is the ability to perform a scheduled RAID Data Scrubbing (also know as synchronization). The Event Scheduler is treated as a remote service in Netfinity Manager so requires a valid incoming UserID and password. See 2.7, “Netfinity Manager Security Implications” on page 48 for further details.

2.3.8 File Transfer

File Transfer

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

2.3.9 Predictive Failure Analysis

Predictive Failure Analysis

The Predictive Failure Analysis (PFA) service enables you to continually monitor and manage PFA-enabled and SMART-enabled hard disk drives. A PFA-enabled 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. In addition to the PFA hard disk drives, Netfinity Manager for OS/2 and Windows NT both support hard disk drives that conform to the SMART standard.

SMART stands for self-monitoring analysis and reporting technology and is the successor to the PFA technology that was pioneered by IBM. The PFA technology subsequently became the ANSI-standard SMART SCSI protocol and lead to the setting up of the SMART working Group (SWG). The SMART standard has now been extended to IDE/ATA 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 SMART standard. Support for SMART hard disk drives is available only on systems running Netfinity Manager or Client Services for OS/2 or Windows NT.

All disks in the current server range are either PFA or SMART enabled.

2.3.10 Process Manager

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 Manager alerts if a process starts, stops, or fails to start within a specified amount of time after system startup. See 2.4, “Alerts” on page 24 for full description and examples.

You can list, stop and start processes on local or remote systems from the command line using the NFPROCCL command. See Chapter 4 of *Netfinity Manager Command Reference* for details.

2.3.11 RAID Manager

RAID Manager

The RAID Manager service enables you to monitor, manage, and configure an assortment of 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 failed drives, add (or remove) physical 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.

All IBM SCSI RAID adapters are supported by Netfinity Manager.

2.3.12 Remote Session

Remote Session

You can use Remote Session to establish a text-based command-line session with any remote Netfinity Manager system.

2.3.13 Remote System Manager

Remote System Manager

As a system administrator, this will probably be the function you'll use the most. You can use Remote System Manager to access and manage any Netfinity Manager function on any Netfinity Manager system in your network.

Netfinity Manager Remote System Manager organizes all Netfinity Manager remote systems into groups. Three types of groups are available for your use:

1. A *system group* is a group of individual, network-attached systems that can be accessed, managed, and monitored by the Remote System Manager.

2. A *rack group* is a group of systems that are installed in an IBM Netfinity 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.

   Other than that, systems included in a rack group behave exactly like systems included in a system group. You can use the *Netfinity Rack Configurator* to define a configuration for a rack, then save it to be imported into Netfinity Manager. The Rack Configurator software can be found at URL

   ```
   http://www.pc.ibm.com/us/products/netfinity/download.html
   ```

   in the “Configurator Tools” section. See 2.6, “Netfinity Rack Configurator” on page 44 for details on how to use exported data from the configurator for use with Netfinity Manager.

3. A *cluster group* is special type of system group intended to let you manage the nodes of a Microsoft Cluster Server installation as a group. You define the group by entering the cluster name. This feature is available in Netfinity Manager 5.1 or higher.

2.3.13.1 Adding Members to Groups

There are three ways to add members to a group:

1. Manual discovery
2. Auto-discovery at a regular interval
3. Manual entry

Netfinity Manager has the ability to discover LAN-attached client workstations automatically. For example, if a new machine with Client Services or Netfinity Manager appears on the LAN, the next time a broadcast is made from the group within Netfinity Manager, the new LAN-attached machine will respond and a new icon will appear in that group.

The time between auto-discovers is defined when the group is created and can be edited along with keywords and the group name. By default, it is disabled, but the discovery interval can be set from 1 to 164 hours.

If you do not want Netfinity Manager to auto-discover at regular intervals, you can either select a manual discovery or add individual machines manually. You can perform both these actions from the **System** menu once you open the group.

2.3.13.2 TCP/IP Auto-Discover

If you are using the TCP/IP protocol driver, Remote System Manager will discover other Netfinity Manager systems using TCP/IP in your *local* subnet. Your system sends a UDP broadcast message to systems in your local subnet on port 13991 and waits for all Netfinity Manager systems to reply. It then builds the group based on the filters you specify.

If you also want to access Netfinity Manager systems in other TCP/IP subnets, you can either add them manually or you can create a text file named

```
TCPADDR.DSC
```

in your Netfinity directory (C:\NETFIN by default). This file must contain the following information:

```
tcpipaddress subnetmask
```

where *tcpipaddress* is the numeric TCP/IP address of any system in the remote subnet, and *subnetmask* is the TCP/IP subnet mask for the remote subnet. The specified system does not have to be running Netfinity Manager. For example:

```
9.24.104.31 255.255.255.0
9.37.104.248 255.255.248.0
```

By specifying one machine in a remote subnet (it does not have to be running Netfinity Manager), the Remote Systems Manager will be able to detect all machines in that subnet. The TCPADDR.DSC may contain entries for multiple subnets.

Netfinity Manager uses the address/mask combination to determine the broadcast address of for that subnet. It then sends a UDP packet to the broadcast address on port 13991 to direct all Netfinity Manager (and Client Services) systems to repond to your local machine.

Notes:

1. The routers in your network must be configured to allow UDP broadcasts for this auto-discover process to work.
2. There must be a CRLF at the end of the file otherwise the last line in the file will be ignored.
3. These two examples are valid definitions within the IBM Intranet only.

2.3.13.3 Auto-Discover Keywords

Netfinity Manager uses keywords to determine if a remote Netfinity Manager system should be included in a group. When you first installed Netfinity Manager or Client Services, you specified a group of user-defined keywords (you can change these keywords later by running the **Network Driver Configuration** program). These user-defined keywords might include physical location information or departmental information.

When you define a group, you specify what keywords should be present in each machine for it to be included in the group. You can specify either user-defined keywords, or, with Netfinity Manager Version 5.0 or later, system-defined keywords.

System-defined keywords are automatically assigned to a remote system, if they have certain hardware or software characteristics. Table 1 contains the list of system-defined keywords available for group creation. These allow an administrator to group machines of similar configuration.

Table 1 (Page 1 of 2). System-Defined Keywords. (See Notes)

Keyword	Explanation
NF:WAKEUP	Has Wake-on-LAN feature enabled
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

Table 1 (Page 2 of 2). System-Defined Keywords. (See Notes)

Keyword	Explanation
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:PartitonBase	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
APP:appkey	Has an application with Application Keyword appkey present (See Note 3)

Note:

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 services 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.

3. For information on Application Keywords, see “Using Application Keywords” in Chapter 22 of the *Netfinity Manager User's Guide*
4. These keywords are only available on systems running Netfinity Manager Version 5.0 or later.

You can perform many Remote System Manager functions from the command line using the NFRSYSCL command. See Chapter 7 of *Netfinity Manager Command Reference* for details.

2.3.14 Remote Workstation Control

Remote Workstation Control

This feature in Netfinity Manager 5.0 or higher enables you to monitor or control the screen display of a remote Netfinity Manager system. Once you initiate a Remote Workstation Control (RWC) session with another Netfinity Manager 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 RWC session, all mouse clicks and keystrokes entered on your system are automatically passed through to the remote system except for specific keystrokes like Ctrl-Esc or Ctrl-Alt-Del, which can be issued remotely through menu action. With RWC, you can remotely start programs, open and close windows, enter commands, and much more.

> **Tip!**
>
> To make it easier to work with a remote system, if you set the remote screen resolution slightly lower than the system you are working on then the whole desktop of the remote machine can be displayed on your screen.
>
> Also if you set the number of colors displayed to 16 or 256, then the responsiveness of the remote session will increase as less bandwidth is taken up with transferring color information.

Although the RWC function is capable of taking over a system's console, you must take into account that all the actions taken have to be transferred over the network. This means that there is a difference in response time when working remotely, compared to working at the system itself. This performance difference is accentuated when using slow data links, like serial connections through a modem. We recommend that you use at least a 14.4 Kbps modem.

Note: The use of Remote Workstation Control is *not officially supported* through a modem.

2.3.15 Screen View

Screen View

The Screen View service takes a “snapshot” of any remote Netfinity Manager system's graphic display and displays it on your screen. This method, although not interactive, is faster than using Remote Workstation Control, if you only want to see the screen of the remote machine. It also has less impact on the remote workstation and creates less network overhead.

2.3.16 Security Manager

The Security Manager can prevent unauthorized access to some or all of your Netfinity Manager services. It uses incoming user ID and password combinations, and only allows authorized remote users to access the specified Netfinity Manager functions.

The Security Manager only applies to network use. It does not prevent unauthorized users from accessing Netfinity Manager functions while they are working locally. You should implement other local security measures to prevent this. For further details please see 2.7, “Netfinity Manager Security Implications” on page 48

Warning: Security Not Enabled

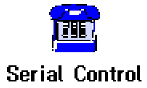
After installation, one user ID will be defined in the security manager, with all accesses granted. This user ID is the <PUBLIC> user ID and it means that everyone has access to your system.

The first step after installation should be to open the Security Manager, and revoke all disallowed actions to <PUBLIC>. Don't forget to uncheck the box that authorizes security manager access. If this is box remains checked, <PUBLIC> will still have the ability to change the security access, regardless of whether or not they have that access now.

See 2.7, “Netfinity Manager Security Implications” on page 48 for more discussion on the security implications of Netfinity Manager.

You can also perform many Security Manager functions from the command line using the NFSECCL command. See Chapter 8 of *Netfinity Manager Command Reference* for details.

2.3.17 Serial Connection Control



The Serial Connection Control function enables remote Netfinity Manager managers to access your system through either a phone line and modem or a null modem cable.

Tip

If you are having problems with either the null modem connection or the modem connection ensure you have a fully wired cable.

Your system must have a properly installed and configured modem that supports at least 9600 bps for the Serial Connection Control function to function.

2.3.18 Service Processor Manager

Service Processor

The Service Processor Manager was renamed to Advanced System Manager in Netfinity Manager Version 5.10.4. See 2.3.1, “Advanced System Managment” on page 11 for more information.

2.3.19 System Diagnostics Manager

System Diagnostics

The System Diagnostics Manager lets you initiate a variety of diagnostic tasks on systems that support ROM based diagnostics.

Note: This function is only supported under OS/2 and NetWare. The function is not available when the server is running Windows NT.

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 (second) CPU
- Parallel
- Serial
- Ethernet
- SCSI
- RAID
- Mouse

Currently, the only servers supporting this feature are

- IBM PC Server 325 (Pentium II models)
- IBM PC Server 330 (Pentium II models and the 8640-PM0 model)

See 4.3.1.2, “Diagnostics with Netfinity Manager” on page 107 for details on this function in the Server 325 and Server 330.

2.3.20 System Information Tool

System Information

The System Information Tool enables you to quickly and conveniently access detailed information on the hardware and software configurations of your system.

The System Information tool can also be run from the command line using the SINFG30 command. See Appendix G, “Netfinity Command Line Operations” of *Netfinity Manager User's Guide* for details.

You can also perform many System Informaiton Tool functions from the command line using the NFSYSICL command. See Chapter 11 of *Netfinity Manager Command Reference* for details.

2.3.21 System Monitor

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 network usage. These convenient monitors are detachable and sizable, 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.

In Netfinity Manager, extra monitors are included to monitor operating system specific features. For example, under Windows NT we can monitor Sessions and Opens as this is an NT function. There are also extra monitors to monitor some specific hardware values such as system board temperature and fan speed.

The open architecture of Netfinity Manager also allows other manufacturers to include their own specific monitors. Examples of these are UPS systems from APC, where voltage and temperature monitors are available. See 2.5, “UPS Support” on page 34 for more information on the UPS extentions. Also see Chapter 4, “Management Functions in Netfinity Servers” on page 89 for information about specific monitors available to specific servers.

You can also perform many System Monitor functions from the command line using the NFSMONCL command. See Chapter 10 of *Netfinity Manager Command Reference* for details.

2.3.22 Web Manager Configuration

Web Manager

Netfinity Manager functions can be accessed through the Internet or an Intranet via a Netfinity Manager with the Web Manager functions enabled. Once enabled, you can use any Web browser to perform a subset of the Netfinity Manager functions.

You can use the Web Manager Configuration service to limit access to the to specific TCP/IP addresses or ranges of addresses. When enabled, all authorized systems running a Web browser, can access a subset of the Netfinity Manager manager functions. This enables you to do remote system management over the internet, without having to install Netfinity Manager.

Note: The Remote Workstation Control and any of the RAID actions are not accessible from a browser. You can view the RAID configuration, but you cannot perform any actions on the RAID arrays such as RAID synchronization, stop and restart drive functions. The synchronization through the Event Scheduler is available, however.

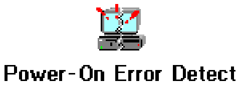
2.3.23 Other Functions

The following is a brief description of the functions that are primarily for use on a workstation or client machine or are not supported by our current range of Netfinity or PC Servers.

- DMI Browser

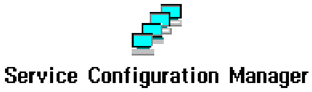
  DMI Browser enables you to examine information about the DMI-compliant hardware and software products installed in or attached to your system. The Desktop Management Interface (DMI) is an industry standard that simplifies management of hardware and software products attached to, or installed in, a computer system.

- Power-On Error Detect

  The Power-On Error Detect service is only available on Micro Channel machines. It will install a shrieker system on the system partition, which will broadcast any POST alert. This alert will be received by all Netfinity Managers.

- Service Configuration Manager

  This function enables you to save the configuration of 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 other similar systems you choose.

  An example can be the System Monitor function. If you define thresholds and alerts on one system, you can save these in a file using the Service Configuration Manager. Later, you can distribute this file to other systems, that then will use these settings for their own system monitor.

  You can also perform many Service Configuration Manager functions from the command line using the NFREPLCL command. See Chapter 6 of *Netfinity Manager Command Reference* for details.

- Software Inventory

Software Inventory

This Software Inventory enables you to make an inventory of software products installed on the system. You can also manage software product dictionaries, to define products that are not in the default dictionary. You can define these products based on the SYSLEVEL, or on one or more required files. These files can be matched on file date and size.

You can also perform many Software Inventory functions from the command line using the NFSINVCL command. See Chapter 9 of *Netfinity Manager Command Reference* for details.

- System Partition Access

System Partition Access

The System Partition Access is only available on Micro Channel systems which have a system partition. It allows you to back up and restore system partitions, and to manage files located on the system partition (diagnostic files and adapter definition files).

- System Profile

System Profile

The System Profile function enables you to record system specific information that is not directly related to the hardware or software. Examples are user name, location, telephone and so forth. Also a lot of system-specific fields are available, like serial number and purchase date. The appearance is that of a notebook, which makes it easy to use.

You can list, view, and modify the system profile of a machine from the command line using the NFPROFCL command. See Chapter 5 of *Netfinity Manager Command Reference* for details.

2.4 Alerts

The Alert Manager is an extendable facility that allows receiving and processing of application-generated alerts. These alerts can be the result of informational, warning or error messages and can originate from a variety of hardware and software sources both within and outside of Netfinity Manager.

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, generating an SNMP alert message, dialing out to a digital pager service, or taking an application-defined action.

The base service that is at the hub of the alerting in is Alert Manager — all alerts that are generated by Netfinity base services are sent to it. Alert Manager matches an incoming alert against one of its default and user definable filters (called profiles) and then if matching, carry out the appropriate action.

To start Alert Manager, double-click on its icon in the Netfinity Manager Main Window. You will then see Figure 3 on page 25 which also doubles as the alert log.

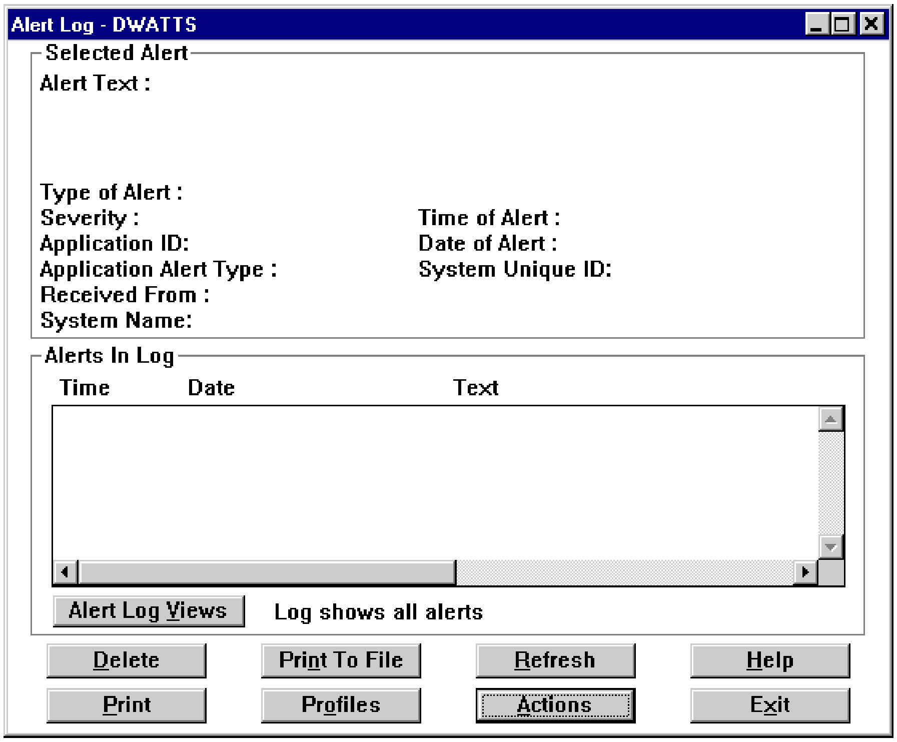


Figure 3. Alert Manager: Main Window

As stated above, alerts can be the result of informational, warning or error messages and can originate from a variety of sources. In fact, there are a constant stream of these messages being generated. You would normally only want to be made aware of a subset of these. You do this by defining an alert action.

2.4.1 Two Methods to Define Alerts

There are two ways to defining a Alert/Action combination:

1. Define a filter (called a *profile*) which specifies the criteria as to when an alert will be generated, followed by defining an action to perform as a result of that profile being met (called *binding the action to a profile*); *or*

2. Simply define the action by specifying the criteria directly. (called *binding the action to an alert condition*)

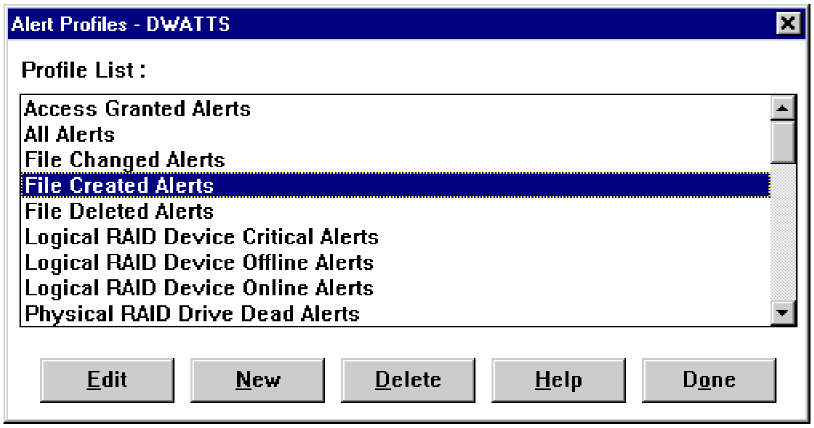
There is no significant difference between these two methods except that defining a profile before binding it to an action gives you a little more control over the alerts and allows you to give each action a name. If you plan to have multiple actions as a result of a single alert, it will be easier if you use the first method.

We now describe how to use both these methods to define an alert/action combination. The first method is described in 2.4.2, “Defining an Action from an Alert Using a Profile” on page 26. The second is described in 2.4.3, “Defining an Action from an Alert Using a Condition” on page 31.

2.4.2 Defining an Action from an Alert Using a Profile

From the main window, click on the **Profiles** button. You will then see Figure 4. This window shows all the currently defined profiles. The ones shown here were all predefined when Netfinity Manager was installed. Any other profiles you define will also appear here.

See "Predefined Alert Profiles" in Chapter 2 of *Netfinity Manager User's Guide* for a description of the other predefined profiles.



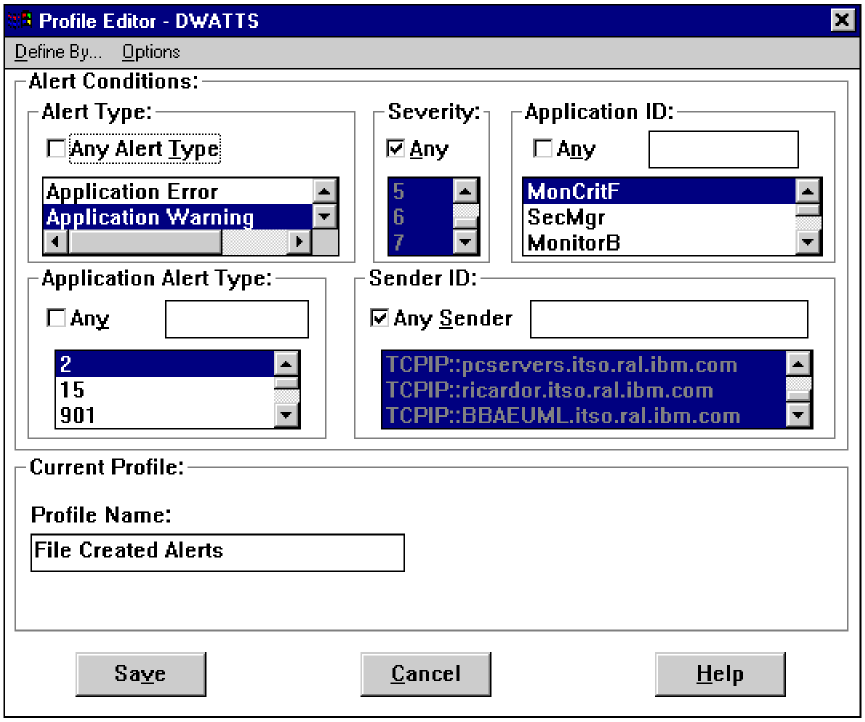
Alert Profiles - DWATTS

Profile List :

- Access Granted Alerts
- All Alerts
- File Changed Alerts
- File Created Alerts
- File Deleted Alerts
- Logical RAID Device Critical Alerts
- Logical RAID Device Offline Alerts
- Logical RAID Device Online Alerts
- Physical RAID Drive Dead Alerts

Figure 4. Alert Manager: List of Defined Profile

Here you can work with existing profile or create new ones. Select the **File Created Alerts** profile and click on **Edit**. The Profile Editor window, shown in Figure 5 now appears.



Profile Editor - DWATTS

Alert Conditions:

Alert Type: □ Any Alert Type
- Application Error
- Application Warning

Severity: ☑ Any
- 5
- 6
- 7

Application ID: □ Any
- MonCritF
- SecMgr
- MonitorB

Application Alert Type: □ Any
- 2
- 15
- 901

Sender ID: ☑ Any Sender
- TCPIP::pcservers.itso.ral.ibm.com
- TCPIP::ricardor.itso.ral.ibm.com
- TCPIP::BBAEUML.itso.ral.ibm.com

Current Profile:

Profile Name: File Created Alerts

Figure 5. Alert Manager: Profile Editor by Alert Conditions

This particular profile is designed to capture alerts from the Critical File Monitor of alert type “Application Warning” and of application alert type 2 from any other Netfinity Manager machine at any severity level. These conditions are specific to an alert generated when one of the nominated critical files gets created. You can see that this profile is useful because it saves the user from having to determine all these values and set up the profile.

The fields in the window are explained in the next section, 2.4.2.1, “Profile Editor.”

2.4.2.1 Profile Editor

The profile editor shown in Figure 5 on page 26 is displayed. It contains the following components:

Alert Type: This is the layer and type of alert generated by Netfinity. All alerts that Netfinity Manager handles will have a type. Select the tick box to select all Alert types.

Severity: These have value 0 to 7 where 0 is the most serious. The severity is usually set by you when setting up a threshold. If the alert has been routed from another alerting system or from a part of Netfinity Manager that does not allow you to set severities then you need to find out these value to trap alerts correctly.

Alert Tip

If you do not know what values will be received when an alert is generated, configure the alert so that it occurs under under normal conditions.

For example, if you want to know what the alert values are when a system exceeds a temperature threshold, set the alert up to trigger at a normal operating value. This way, you can see all of the details of the alert without stressing your machine.

Application ID: This is a case-sensitive alphanumeric identifier that identifies the source application of the alert. Each application will provide an ID and new IDs can be added. See Table 2 for a list of the Netfinity Manager IDs and Table 3 on page 28 for a list of some of the IDs from other Netfinity-aware applications.

You may select one or more currently available Application IDs from the window or you can also enter a new application ID by entering the new Application ID, and pressing Enter. If the **Any** check box is selected, any Application ID received by the Alert Manager will be considered a valid alert condition.

Table 2 (Page 1 of 2). Standard Application IDs for Netfinity Manager Applications

Application ID	**Application**
MonCritF	Critical File Monitor
MonitorB	System Monitor
NetMgr	Remote System Manager
PFA	Predictive Failure Analysis
POED	Power-on Error Detect
ProcMgr	Process Manager
SecMgr	Security Manager

Table 2 (Page 2 of 2). Standard Application IDs for Netfinity Manager Applications

Application ID	Application
SvcMgr	Service Manager

Table 3. Application IDs for Other Netfinity-aware Applications

Application ID	Application
CommMgr	IBM Communication Manager
DB2	IBM Database Server
LNM	IBM LAN Network Manager
LanSrv	IBM LAN Server
ipsraid	IBM ServeRAID Adapter
PwrChute	APC Power Chute software extension for UPSs
SysMgt	IBM Advanced Systems Management Adapter extension

Application Alert Type: This is probably the most important value you need to consider. It is the type of problem that the application has and is assigned by the application that generated the alert. You may select one or more currently available Application Alert Types from the window or you can also enter a new type by entering the new Application Alert Type in the box provided, and pressing Enter. If the **Any** check box above the Application Alert Type window is selected, then any application alert type received will be considered a valid Alert Condition.

Sender ID: The Sender ID is the network address of the system that generated the alert. You may select one or more currently available Sender IDs from the window or you may also enter a new Sender ID by entering the new Sender ID, and pressing Enter. If the **Any Sender** check box is selected, any sender ID received by the Alert Manager will be considered a valid Alert Condition.

The entries in the Sender ID field have a particular format. They contain the name of the network containing the sending system, followed by two colons (::), followed by the network address of the sender. Table 4 shows the various ways of structuring the address:

Table 4. Sender ID Format for Different Protocols

Network Type	Network Address	Example
TCPIP	TCPIP::Hostname.Domain	TCPIP::nf7000.raleigh.ibm.com
IPX	IPX::Network Number.Machine Number	IPX::9.10005AC3B420
NETBIOS	NETBIOS::NetBIOS Name	NETBIOS::NF7000
SERIPC	SERIPC::Serial Name set in Network Driver Configuration	SERIPC::NF_7000
SNA/APPC	APPC::Network Name.XID	APPC::IBMUSNR.NRIMJ600

If you are unsure of the workstations network type or network address, you can use Remote System Manager's Edit System action or system group Detail View to check this information.

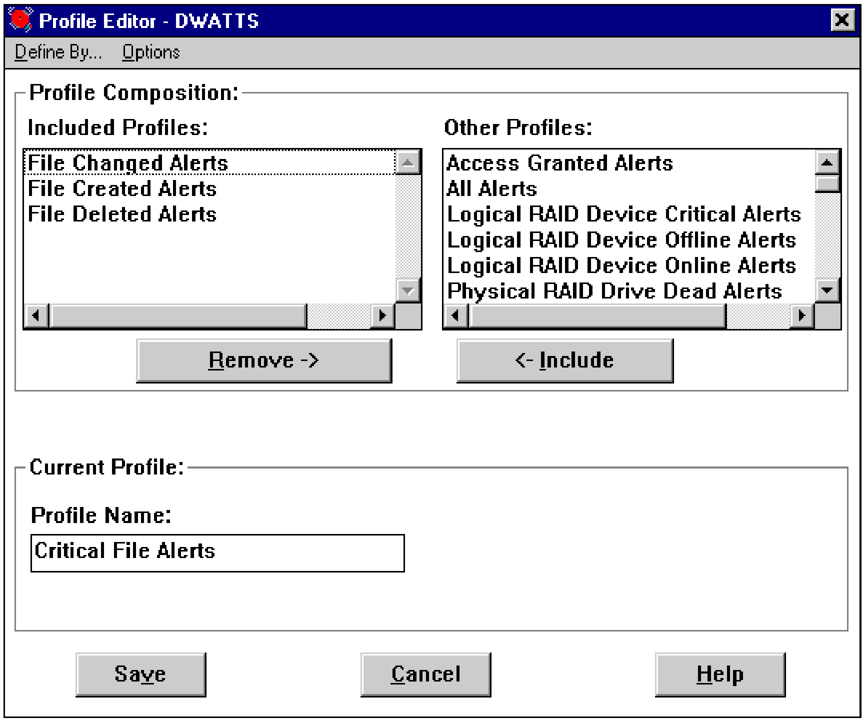
Profile Name: This is the name of the profile. This can be up to 64 characters in length. We advise that you make this name meaningful and describe the alert profile you have just setup.

2.4.2.2 Multiple Profiles

As well as being able to create a profile based on a set of conditions as we described in 2.4.2.1, “Profile Editor” on page 27, you can also use the Profile Editor to create a profile based on *multiple profiles*. This has the affect of funnelling the alerts generated by many profiles into one profile to allow you to set up an alert on just that one profile.

Once this kind of profile is set up, any alert matching *any* of the profiles included in the new “master” profile will trigger the alert.

To do this, from the Profile Editor window, click **Define By...** → **Profile Composition**. Figure 6 appears.



Profile Composition:

Included Profiles:
File Changed Alerts
File Created Alerts
File Deleted Alerts

Other Profiles:
Access Granted Alerts
All Alerts
Logical RAID Device Critical Alerts
Logical RAID Device Offline Alerts
Logical RAID Device Online Alerts
Physical RAID Drive Dead Alerts

Current Profile:

Profile Name: Critical File Alerts

Figure 6. Alert Manager: Profile Editor by Profile Composition

Select the profiles you want to include, then click on the **Include** button. Give the new profile a name of up to 64 characters, the click on **Save** to save the profile, then **Yes** to confirm the save. You new profile will then appear in with the other profiles in the Profile List window.

2.4.2.3 Defining the Action Based on a Profile

Now that we have found an existing profile that generates the alerts we wanted, or we have created a new profile, we now need to bind an action to that profile.

From the Alert Manager Main Window (the Alert Log window), click on the **Actions** button and Figure 7 on page 30 will appear.

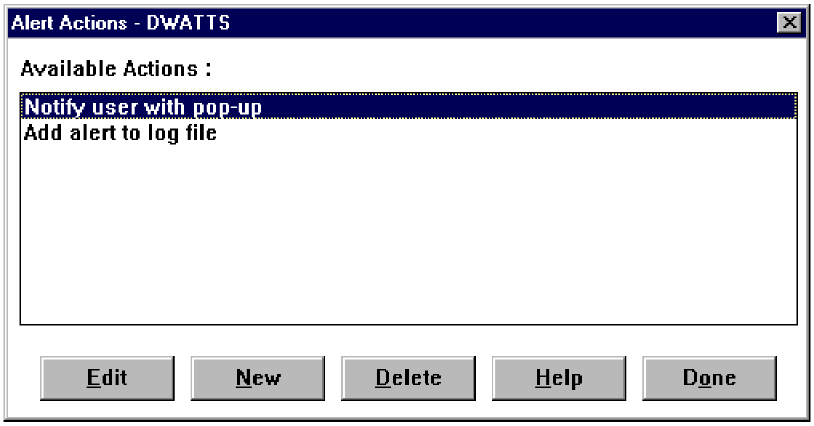
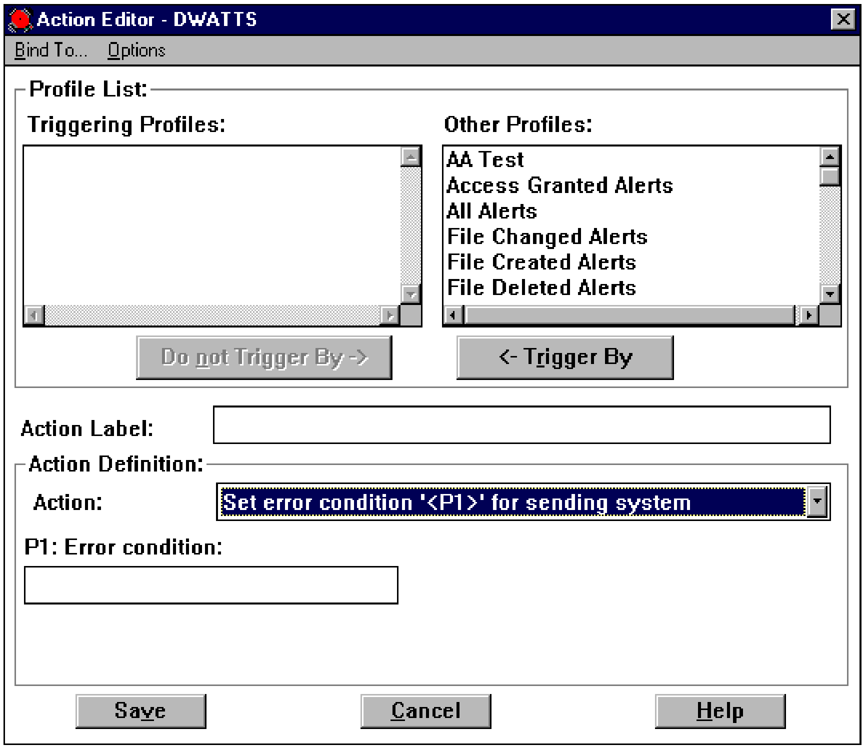


Figure 7. Alert Manager: Alert Actions

You will see that two actions are defined. These two (as shown in Figure 7) are set up when Netfinity Manager is first installed. We will describe these in 2.4.3, “Defining an Action from an Alert Using a Condition” on page 31. For now, click on the **New** button.

The Action Editor window now appears. Click on **Bind To...** → **Profiles**. Figure 8 appears.



Action: Set error condition '<P1>' for sending system

Figure 8. Alert Manager: Action Editor Using Profiles

In the **Other Profile** listbox, select the profile (or profiles) that you want to use to specify the alert, then click on the **<- Trigger By** button. This moves the profiles you selected into the **Triggering Profiles** listbox.

Now, specify a name for the action you are about to set (up to 22 characters), the specify the action you wish to perform from the **Action** pull-down menu. Enter any parameters as needed.

Each of the possible actions is described in 2.4.4, “Alert Actions” on page 32.

Save the action by clicking on **Save**, then confirm the save by clicking on **Yes**. Your new action to be performed based on a profile will then appear in the list of available actions.

2.4.3 Defining an Action from an Alert Using a Condition

As we described in 2.4.1, “Two Methods to Define Alerts” on page 25, a second a quicker method to define an alert/action combination is to simply define the alert with a set of conditions directly, rather than first defining a profile as described in 2.4.2, “Defining an Action from an Alert Using a Profile” on page 26.

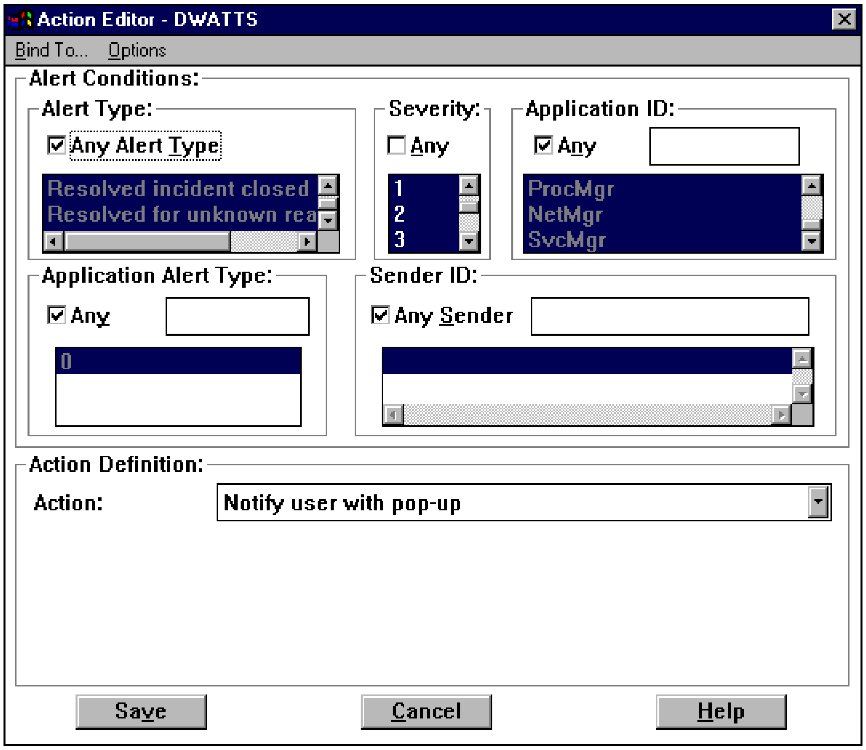
Even though this method is quicker, it does offer some disadvantages:

- You are not able to give the alert a name
- Using profiles is easier to use if you have a single set of conditions generating multiple actions
- Using profiles is easier to manage when you have a complex alert configuration

From the Alert Manager main window (the Alert Log window), click on the **Actions** button. You will be presented with the list of currently defined actions as shown in Figure 7 on page 30.

Select the action **Notify user with pop-up** and click on the **Edit** button. Figure 9 on page 32 appears.

Note: If you see Figure 8 on page 30 instead, click on **Bind To...** → **Alert Conditions** and the window should appear.



Alert Conditions:

Alert Type: ☑ Any Alert Type
Resolved incident closed
Resolved for unknown rea

Severity: □ Any
1
2
3

Application ID: ☑ Any
ProcMgr
NetMgr
SvcMgr

Application Alert Type: ☑ Any
0

Sender ID: ☑ Any Sender

Action Definition:

Action: Notify user with pop-up

Figure 9. Alert Manager: Action Editor Using Alert Conditions

The fields here are the same as those in the profile editor discussed in 2.4.2.1, “Profile Editor” on page 27 except that instead of specifying a profile name, you specify an alert condition.

In the window in Figure 9, the action is to “Notify user with pop-up” and in this case, no additional parameters are required. See 2.4.4, “Alert Actions” for a complete description of all the actions available.

Once you select the appropriate action, click on **Save**, then confirm the save by clicking on **Yes**. Your new action to be performed based on a specific condition will then appear in the list of available actions. The name given to the action is the action itself and cannot be changed.

2.4.4 Alert Actions

When defining an action to perform on a profile or an alert condition, you can specify one of a number of actions to perform, based on the hardware and software installed at the time Netfinity Manager was installed.

The following tables show you all the actions that Netfinity Manager supports and what the prerequisites are for it to be available on your system. The first table, Table 5 on page 33 lists all actions that can be set to occur on the server itself. The second table, Table 6 on page 33 lists all the actions that involve sending an alert to some other system.

For more details on the alerts and the parameters that are required with some of them, refer to “Netfinity Alert Actions” in Chapter 2 of the *Netfinity Manager User's Guide*.

Table 5. Actions Available with Netfinity Manager — Local

Action	**Description/Prerequisites**
Add alert to log file	Available on all systems
Display alert in a pop-up	Available on all systems
Execute a command	Available on all systems
Execute a minimized command	Available on all systems
Play a WAV file	Requires multimedia support
Export to a Netfinity database	Requires a DB2 or ODBC database
Export to a Lotus Notes database	Requires Lotus Notes client or server and the Notes directory in the path statement.
Display on Server 720 front panel	Requires Server 720
Set an error condition	Places an entry in the sending system's Error Conditions log. (accessible from Remote System Manager and right-clicking on the system's icon then selecting **Error Conditions...**.) Available on all systems.
Clear an error condition	Removes an entry in the sending system's Error Conditions log.
Add event to Windows NT event log	Requires Windows NT with the “Alerter” service installed.

Table 6 (Page 1 of 2). Actions Available with Netfinity Manager — Remote

Action	**Description/Prerequisites**
Forward alert to another Netfinity workstation	Available on all systems
Send SNMP Alerts	Uses an SNMP agent to generate an SNMP version of the alert. Requires: • OS/2: TCP/IP V2.0 or later. Needs DPI32DLL.DLL in LIBPATH. • Windows NT: requires the SNMP service • Not available from Windows 3.1 or Windows 95 systems
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 tools. Requires: • OS/2: TCP/IP V2.0 or later. Needs DPI32DLL.DLL in LIBPATH. • Windows NT: requires the SNMP service • Not available from Windows 3.1 or Windows 95 systems
Activate a numeric pager	Requires a Hayes-compatible modem and digital pager support
Send an alert to an alphanumeric pager	Requires: • Modem • Telocator Alphanumeric Protocol (TAP) compatible paging service

Table 6 (Page 2 of 2). Actions Available with Netfinity Manager — Remote

Action	Description/Prerequisites
Send alert as TCP/IP mail	Sends a text-only email message using SENDMAIL. Requires OS/2 with TCP/IP V2.0 or later. Needs DPI32DLL.DLL in LIBPATH.
Send alert as TCP/IP Web mail using SENDMAIL.	Sends an HTML-formatted email message. Requires OS/2 with TCP/IP V2.0 or later.
Send to email via VIM interface	Uses Vendor Independent Messaging (VIM) to generate an alert. Requires • VIM-compliant system (eg Notes or cc:Mail) • OS/2 or Windows NT or Windows 95
Send alert as email via MAPI	Uses Messaging Application Programming Interface (MAPI) to generate an alert. Requires Windows 95 and MAPI-compliant mailer.
Send DMI event	Requires DMI services
Send alert to a remote Netfinity Manager via serial connection	Uses previously-defined serial connection to send an alert. Available on all systems.
Send alert via APPC	Convert alert to a Network Management Vector Transport (NMVT) alert. Requires: APPC support
Forward alert to FFST/2 (First Failure Support Technology/2)	Requires OS/2
Send alert to service processor error log	Requires an Advanced Systems Management Adapter in the machine. See "System Alerts" on page 81 for information on how the Advanced Systems Management Adapter handles this alert.

2.5 UPS Support

IBM and American Power Conversion (APC) have worked together to develop Netfinity Manager extensions which allow management of a wide range of APC Uninterruptible Power Supplies.

ServerGuide includes the following APC products for UPS management:

- PowerChute *Plus* (referred to here as PowerChute)
- PowerXtend for Netfinity Manager (referred to here as PowerXtend)

Note: PowerXtend is also known as *PowerChute Plus Netfinity Extensions*.

PowerChute is a stand-alone program that provides an interface to control, configure and monitor the UPS. It is available for OS/2, Windows NT and NetWare. It can be used to either control a UPS connected to the system the software is being installed on, or it can control a UPS connected to another machine on the network.

In addition, APC offers PowerXtend as a plug-in module to Netfinity Manager. It provides integration into the following Netfinity Manager components:

- System Information
- System Monitor

- Alert Manager
- Event Scheduler

For more information about APC products, go to their home page:

```
http://www.apcc.com
```

To obtain the latest code version, go to the following URL:

```
http://www.apcc.com/english/prods/sware/upgrd
```

2.5.1 Installing PowerChute

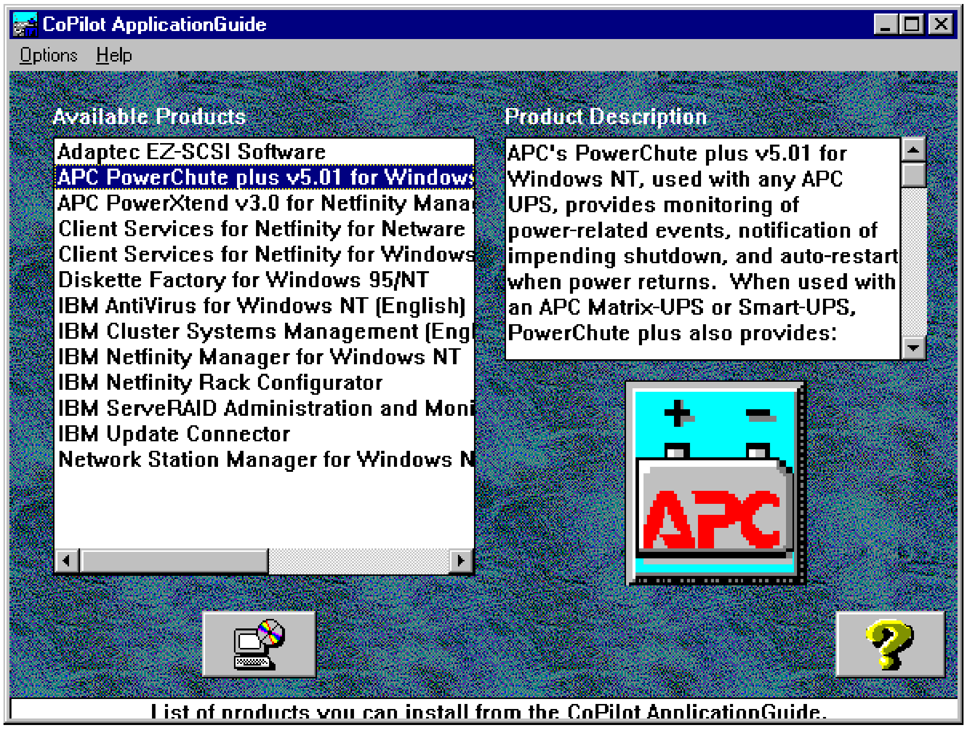
PowerChute and PowerXtend must be installed on both the Netfinity Manager and any machine whose UPS information you want to manage via Netfinity Manager. PowerChute must be installed before installing PowerXtend.

Note: Before starting the installation make sure the UPS is connected to a COM port on the server. If you also have an Advanced Systems Management Adapter installed, ensure there is no conflict over COM port usage.

Administrator Privileges

Ensure you have administrator privileges when installing both products.

Use the ServerGuide CoPilot ApplicationGuide 3A CD-ROM to install both products directly from the CoPilot ApplicationGuide 3A CD-ROM. For Windows NT servers and Windows 95 clients (for NetWare installs), insert the CD-ROM and the installation program should automatically start. For OS/2, insert the CD-ROM and run `OS2SC.CMD`. Figure 10 appears for Windows systems and a similar window appears for OS/2.



Adaptec EZ-SCSI Software
APC PowerChute plus v5.01 for Windows
APC PowerXtend v3.0 for Netfinity Manag
Client Services for Netfinity for Netware
Client Services for Netfinity for Windows
Diskette Factory for Windows 95/NT
IBM AntiVirus for Windows NT (English)
IBM Cluster Systems Management (Engl
IBM Netfinity Manager for Windows NT
IBM Netfinity Rack Configurator
IBM ServeRAID Administration and Moni
IBM Update Connector
Network Station Manager for Windows N

APC's PowerChute plus v5.01 for Windows NT, used with any APC UPS, provides monitoring of power-related events, notification of impending shutdown, and auto-restart when power returns. When used with an APC Matrix-UPS or Smart-UPS, PowerChute plus also provides:

List of products you can install from the CoPilot ApplicationGuide.

Figure 10. ServerGuide Installation of PowerChute

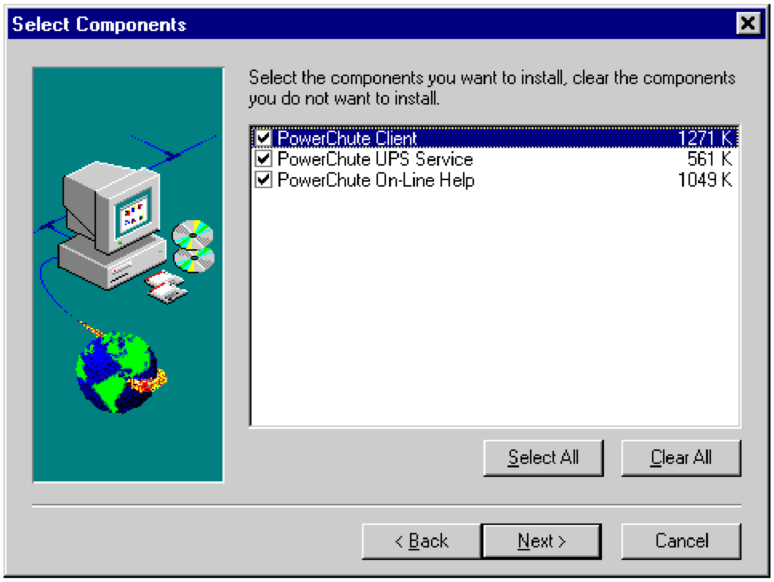
Select PowerChute from the list and click on the install button to begin the installation.

Alternatively, you can start the installation program manually be changing the appropriate directory on the ApplicationGuide 3A CD-ROM as shown in Figure 11.

```
ServerGuide ApplicationGuide 3A CD-ROM
│
├──┬─ Pwrchute
│  ├──┬─ EN
   │  ├─── NTnoext        PowerChute for Windows NT (run SETUP.EXE)
      ├─── OS2noext       PowerChute for OS/2 (run SETUP.EXE)
      └─── NWnoext        PowerChute for NetWare (run SETUP.EXE)
```

Figure 11. PowerChute Directory Tree on the ApplicationGuide 3A CD-ROM

If you are installing the PowerChute software on the server you would normally take the Typical installation path. However, you can chose the Custom installation path which lets you configure PowerChute as shown in Figure 12



Select Components

Select the components you want to install, clear the components you do not want to install.

☑ PowerChute Client	1271 K
☑ PowerChute UPS Service	561 K
☑ PowerChute On-Line Help	1049 K

Figure 12. Selecting Components in a Custom Installation

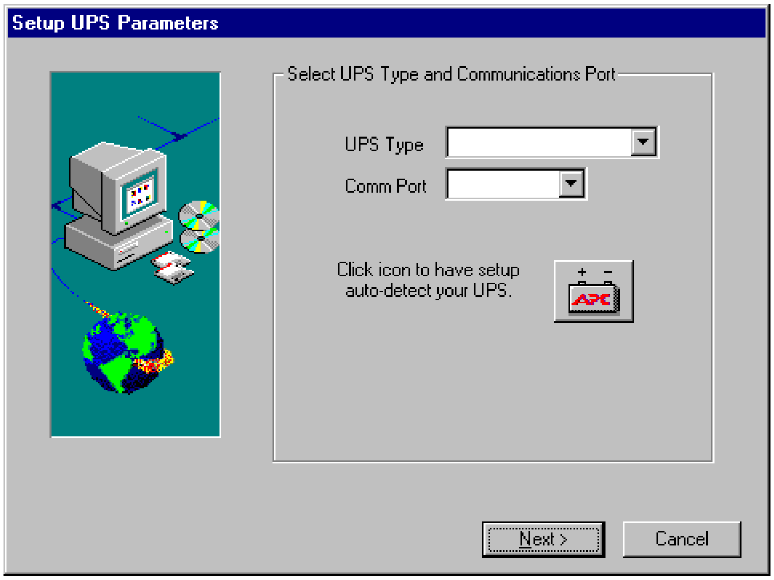
Select the options based only your requirements:

- If you want to manage a locally-attached UPS *or* UPS attached to other systems in your network, select **PowerChute Client** and **PowerChute UPS Service**.
- If you only want to manage a UPS on another system in your network, select **PowerChute Client** only.
- If you don't want to manage the locally-attached UPS but you do want other systems in the network to manage the UPS, select **PowerChute UPS Service** only.

Clicking on **PowerChute On-Line Help** installs an HTML version of the user's guide on your hard disk. There is also a PDF version of the Windows NT version of PowerChute available on the CD-ROM:

```
\PWRCHUTE\EN\NTNOEXT\DOCS\MANUAL.PDF
```

During the installation, Figure 13 appears, prompting you to specify what type of UPS you have and which COM port you have it attached to.



Click icon to have setup auto-detect your UPS.

Figure 13. Selecting Components in a Custom Installation

You can either manually specify these or click on the **APC** button and let the software detect the UPS.

2.5.2 Installing PowerXtend

Once the installation of PowerChute is complete you can then use ServerGuide to install PowerXtend by selecting it from the CoPilot window in Figure 10 on page 35. Alternatively, you can run the installation program directly from the CD-ROM (Figure 14).

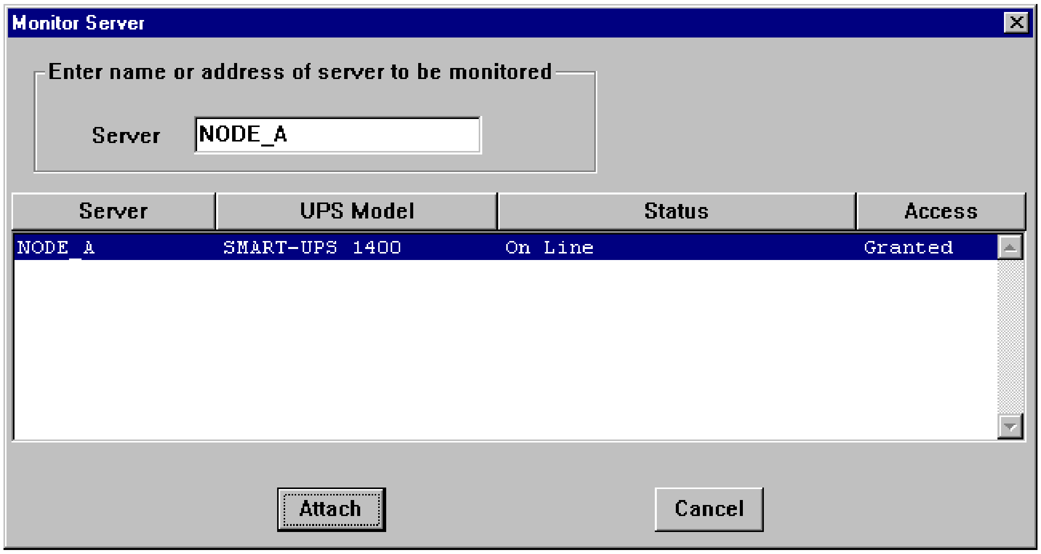
PowerChute and PowerXtend must be installed on both the Netfinity Manager and any machine whose UPS information you want to manage via Netfinity Manager. PowerChute must be installed before installing PowerXtend.

```
ServerGuide ApplicationGuide 3A CD-ROM
│
├── Pwrchute
│   ├── EN
│   │   ├── WinNT      PowerXtend for Windows NT (run NETFINST.EXE)
    │   ├── OS2        PowerXtend for OS/2 (run NETFINST.EXE)
        └── NetWare
            ├── Disk1  PowerXtend for NetWare (run CSETUP.EXE)
            └── Disk2
```

Figure 14. PowerXtend Directory Tree on the ApplicationGuide CD-ROM

2.5.3 PowerChute

Starting PowerChute displays a window, Figure 15, which lets you choose which UPS you wish to connect to. If you wish to connect to a remote UPS, there may be a short delay while it detects it over the network. Select the system you want to access and click on **Attach**

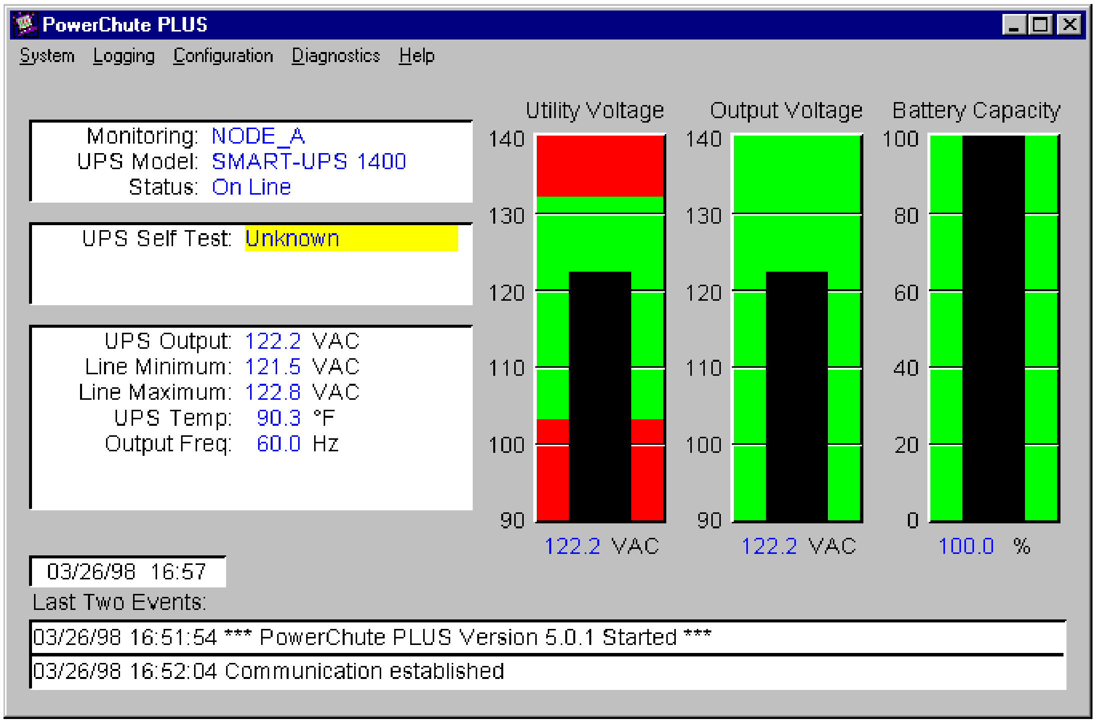


Server: NODE_A

Server	UPS Model	Status	Access
NODE_A	SMART-UPS 1400	On Line	Granted

Figure 15. Selecting a UPS to Access

When you click on **Attach**, Figure 16 appears.



Monitoring: NODE_A
UPS Model: SMART-UPS 1400
Status: On Line

UPS Self Test: Unknown

UPS Output: 122.2 VAC
Line Minimum: 121.5 VAC
Line Maximum: 122.8 VAC
UPS Temp: 90.3 °F
Output Freq: 60.0 Hz

Utility Voltage: 122.2 VAC
Output Voltage: 122.2 VAC
Battery Capacity: 100.0 %

03/26/98 16:57

Last Two Events:

```
03/26/98 16:51:54 *** PowerChute PLUS Version 5.0.1 Started ***
03/26/98 16:52:04 Communication established
```

Figure 16. PowerChute Main Window

From here you can directly control the UPS and perform such actions as shutting down the server, and performing self tests on the UPS. See the *PowerChute User's Guide* for more information.

2.5.4 Measure-UPS

The Measure-UPS is an accessory to the APC UPS that performs temperature and humidity sensing of the environment around the server, as well as contact monitoring. This can be useful as it can give an early warning if the temperature in the server room increases.

It supports up to four contact sensors, each of which supports both normally open and normally closed contacts. Measure-UPS II reports temperatures from 0 to 60°C (32 to 140°F) and relative humidity from 10 to 90%.

The device is a card that is inserted into the “SmartSlot” connector at the rear of the UPS. You can install the Measure-UPS either before you install PowerChute and PowerXtend or after. If you do install it after, you will need to reboot your system before the software will recognize the device.

As well as a temperature or combination temperature-humidity probe, the Measure-UPS device also supports up to four dry-contact-closure type sensors. The Measure-UPS sensor inputs are designed to monitor circuits that have no voltage potential of their own. In general, any normally open (NO) or normally closed (NC) dry contact sensor may be used with Measure-UPS II. Such sensors include:

- Magnetic contact switches
- Window foil
- Tamper switches
- Heat detectors
- Water sensors
- Pressure sensors

Additionally, Measure-UPS provides a source of power for those detectors that need power. These types include:

- Passive infrared (body heat) detectors
- Smoke sensors
- Photo relay detectors

Measure-UPS II provides 12 Vdc at up to 60 mA on the connnection block for sensors that require power.

For more information about the Measure-UPS device, see Appendix B of the *PowerChute plus User's Guide*.

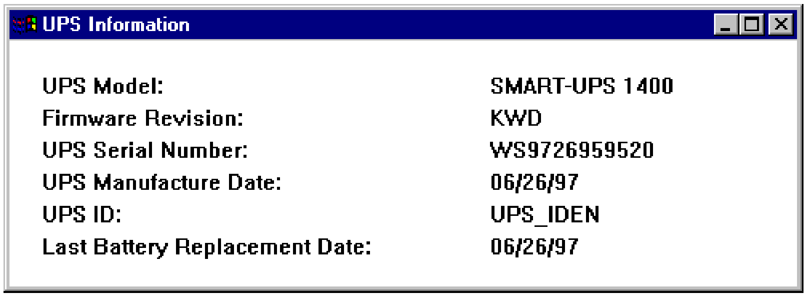
2.5.5 Integration with Netfinity Manager

Once you install PowerXtend the following additional functions are available in Netfinity Manager.

2.5.5.1 UPS Information

UPS Information

PowerXtend supplies another icon on the Netfinity Manager main window. which you can use to display information about the UPS. When you double-click on the icon, Figure 17 appears showing details about the UPS connected to this system.



UPS Information

UPS Model:	SMART-UPS 1400
Firmware Revision:	KWD
UPS Serial Number:	WS9726959520
UPS Manufacture Date:	06/26/97
UPS ID:	UPS_IDEN
Last Battery Replacement Date:	06/26/97

Figure 17. UPS Information Window

2.5.5.2 System Monitor Enhancements

The current release of PowerXtend supports the following monitors for displaying UPS monitoring information:

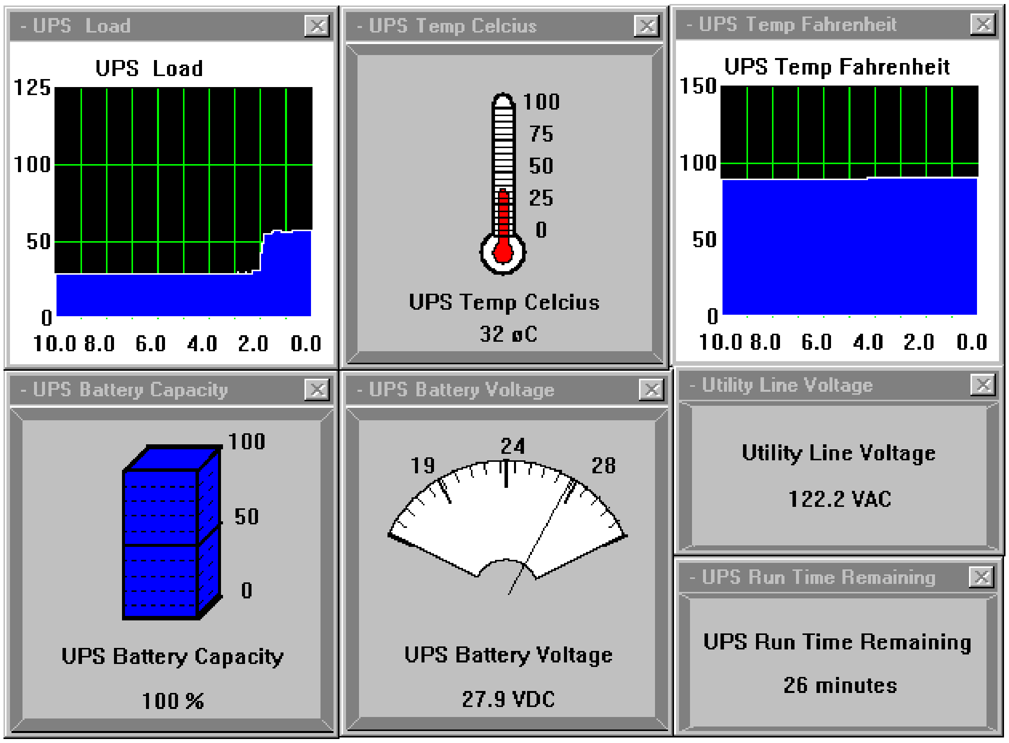


Figure 18. UPS Monitoring Data Displayed by System Monitor

- UPS Run Time Remaining — The maximum number of minutes that your UPS can run on battery before turning off its outlets and going into "sleep" mode.
- Utility Line Voltage — The utility power line voltage in Volts AC. (VAC)

- UPS Battery Voltage — The charge level of the UPS battery in Volts DC. (VDC)
- UPS Load — The equipment load supported by the UPS, as a percentage of the maximum sustainable UPS load.
- UPS Battery Capacity — The charge level of the UPS battery, as a percentage of the maximum charge level.
- UPS Temperature Fahrenheit — The internal temperature of the UPS, reported in Fahrenheit.
- UPS Temperature Celsius — The internal temperature of the UPS, reported in Celsius.

As you can see from Figure 18 on page 40, you can display the information as a gauge, as text or as a line graph over the last 10 minutes. As with other monitors, you can set thresholds that can generate Netfinity Manager alerts.

With the addition of Measure-UPS, a device you connect to the UPS, you can get the following additional monitors through Netfinity Manager as shown in Figure 19.

- Humidity — The relative humidity of the environment in which the UPS is operating.
- Ambient Temperature Fahrenheit — The temperature of the environment in which the UPS is operating, reported in Fahrenheit.
- Ambient Temperature Celsius — The temperature of the environment in which the UPS is operating, reported in Celsius.

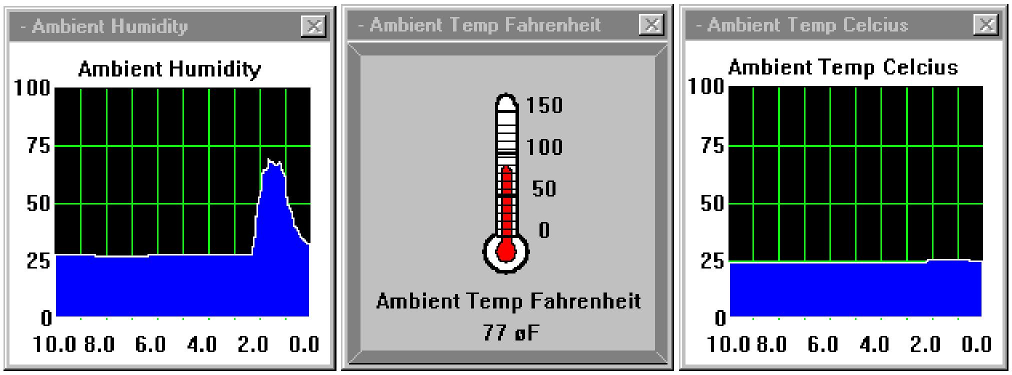


Figure 19. Additional Monitors Using the Measure-UPS Device

2.5.5.3 Alert Manager Enhancements

PowerXtend adds the following to Alert Manager:

- Additional action: “Shutdown with UPS turn off”
- Additional Application ID: “PwrChute”

Table 7 on page 42 shows all the alert types generated by the application ID “PwrChute”:

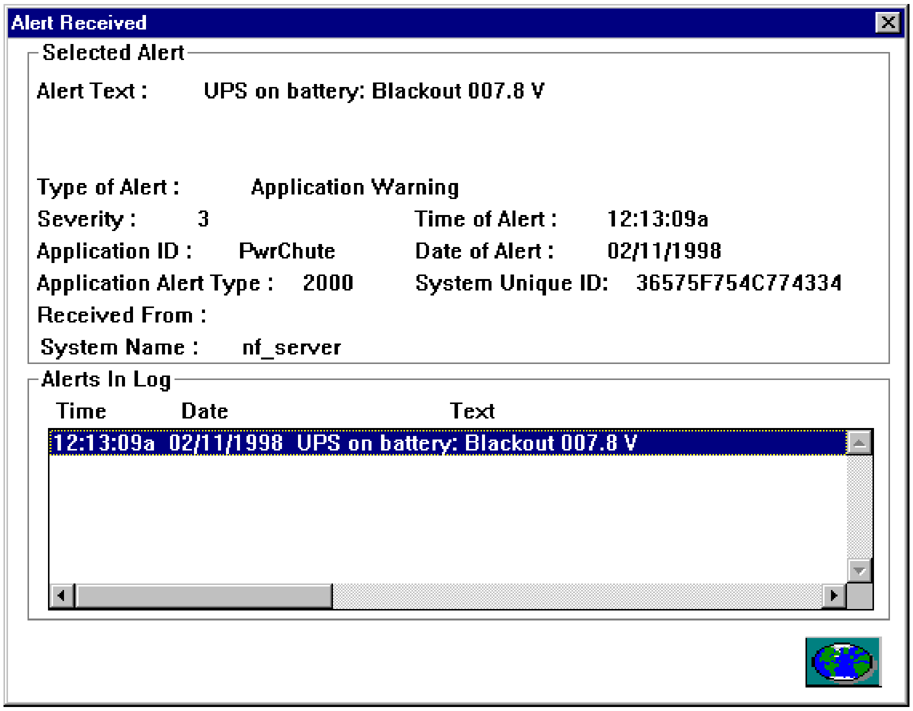
Table 7. Application Alert Types Generated by PowerChute and PowerXtend

Type	Description
1000	PowerChute Started
1001	PowerChute Stopped
1002	Communication Established
1003	Power Restored
1004	UPS Self-Test Passed
1005	Administrative Shutdown
1006	Shutdown Cancelled
1007	UPS Return From Low Battery
1009	UPS Battery No Longer Needs Replacing
1010*	Contact Normal
1013	UPS Overload Condition Solved
1014	UPS Run Time Calibration Initiated
1015	UPS Run Time Calibration Completed
1016	System Shutdown Started
1017	Return From Bypass
1100*	Ambient Temp In Range
1101*	Humidity In Range
2000	UPS On Battery
2001	System Shutdown Complete
2002	UPS Enabling Smart Boost
2003	Low Battery Condition
2004	UPS Run Time Calibration Cancelled
2013	UPS On Bypass: Maintenance
3000	Unable To Communicate With UPS
3001	UPS Output Overload
3002	UPS Self-Test Failed
3003	UPS Battery Is Discharged
3006*	Abnormal Contact Position
3010	Check Smart Cell Signal
3013	UPS On Bypass: Failure
3014	Base Module Fan Failure
3015	Base Module Power Supply Failure
3016	UPS Battery Needs Replacing
3100*	Ambient Temp Out Of Range
3101*	Humidity Out Of Range

Note: The alert types listed with (*) only occur when the Measure-UPS device is installed.

You can configure Alert Manager to react to these alert types from application id “PwrChute” as you would any other event.

Alerts from the UPS appear as they would any other alert, such as shown in Figure 20.



Alert Text : UPS on battery: Blackout 007.8 V

Type of Alert : Application Warning
Severity : 3
Time of Alert : 12:13:09a
Application ID : PwrChute
Date of Alert : 02/11/1998
Application Alert Type : 2000
System Unique ID: 36575F754C774334
Received From :
System Name : nf_server

```
Time      Date        Text
12:13:09a 02/11/1998  UPS on battery: Blackout 007.8 V
```

Figure 20. UPS Alert Displayed by Netfinity Alert Manager

The “Shutdown with UPS turn off” action can be used to shutdown the operating system and turn off the UPS.

Warning: Do not configure Netfinity Manager to issue this action if PowerChute is already configured to automaticaly perform the shutdown. If Netfinity Manager and PowerChute are both configured to initiate a shutdown in response to the same event, the shutdown delay that occurs may not be the one you expect, especially if you change the delay through one of the interfaces but are not aware of the configuration in the other interface.

The “UPS On Battery” and “Low Battery Condition” FlexEvents in PowerChute have the “Shutdown with UPS Turn Off” If you wish to have Netfinity Manager issue this action as a result of these conditions, we recommend you modify these events in PowerChute so that the shutdown only occurs via Netfinity Manager.

2.5.5.4 Event Scheduler Enhancements

PowerXtend supplies two additional events which can be scheduled through Event Scheduler:

- UPS battery calibration
- UPS self test

The UPS self-test verifies how the UPS would function in the event of a power failure. When schedule, it generates the following alert (ID=1004):

```
User initiated UPS self-test passed
```

APC recommends you perform a self test on the UPS every month, especially after the warranty period expires.

A battery calibration determines the UPS battery run time. It deeply discharges the UPS battery and temporarily reduces UPS run time until the battery recharges. During the calibration, the battery capacity shown on the Battery Capacity bar graph on the Main Screen decreases.

When the calibration is started, the following alert (ID=1014) is generated:

```
UPS run time calibration initiated
```

When the calibration completes, the alert 1015 is generated:

```
UPS run time calibration completed
```

APC recommends a UPS battery calibration be performed monthly.

Note: If any server in the group does not have PowerXtend installed, Netfinity Manager issue a message that the requested service is not available on that server.

2.6 Netfinity Rack Configurator

This stand-alone utility lets you simulate and then validate IBM Netfinity rack configurations. You can then use the configuration in Netfinity Manager to create a group based on servers installed in the rack.

You can create your configuration by selecting components from a catalog and then placing them in a picture to create a graphical representation of your rack configuration. You can also simulate connecting to other components and select the correct cables needed for the connection. You can either create a single rack or a suite of racks.

The utility is included with ServerGuide. To obtain the latest version, go to the following URL:

```
http://www.pc.ibm.com/us/products/netfinity/download
```

then click on **IBM Netfinity and IBM PC Server Configuration Tools**. At the time of publication, the latest version was 1.4a.

2.6.1 Installation

This software is included in ServerGuide and can be installed on:

- Windows 3.x (or WINOS2 under OS/2)
- Windows 95
- Windows NT 3.51 and 4.0

Use the ServerGuide ApplicationGuide 3A CD-ROM to install the product. Under Windows 95 or Windows NT 4.0, you can simply insert the CD-ROM and the installation program should start automatically. Under OS/2, run the command SCOS2.CMD. Under Windows 3.x, run command SCW31.EXE. From the Co-Pilot window, select **IBM Netfinity Rack Configurator** and click on the install button.

Alternatively, you can start the configurator installation program manually by running SETUP.EXE from the \RACKCFG\EN directory on the CD-ROM.

Note: Netfinity Manager is not required for this product installation.

2.6.2 Integrating with Netfinity Manager

The Netfinity Rack Configurator can create a set of files that describe your rack configuration suitable for use by Netfinity Manager. These files provide rack-position information during the discovery process, to identify where in the rack your server is installed, and so on.

2.6.2.1 Creating the Netfinity Manager Files

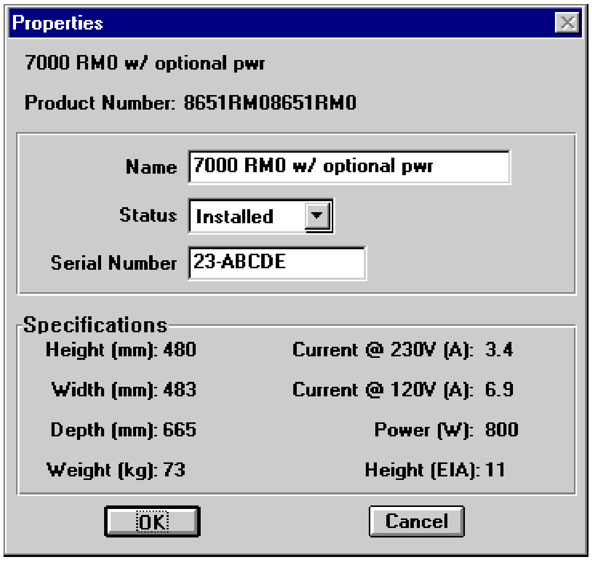
Note: Before creating the Netfinity files, you *must* have a rack configuration that has been created, validated, and built. See the program documentation for more information.

To create the Netfinity files, perform the following steps:

1. Ensure your server component has these settings: (see Figure 21)

   - Set **Status** to Installed.
   - The **Serial Number** field is filled in..

   Netfinity Rack Configurator can *only* generate Netfinity files for those servers with the above settings.



Properties

7000 RM0 w/ optional pwr

Product Number: 8651RM08651RM0

Name: 7000 RM0 w/ optional pwr

Status: Installed

Serial Number: 23-ABCDE

Specifications

Height (mm):	480	Current @ 230V (A):	3.4
Width (mm):	483	Current @ 120V (A):	6.9
Depth (mm):	665	Power (W):	800
Weight (kg):	73	Height (EIA):	11

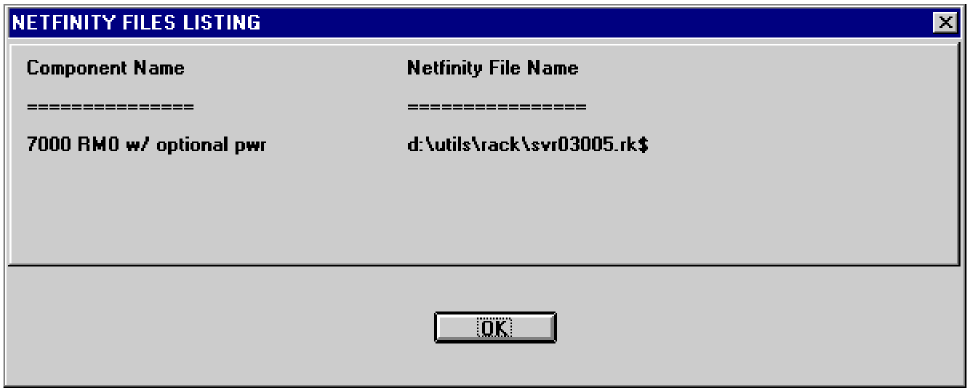
Figure 21. Server Properties Window

2. To improve the quality of the information passed to Netfinity Manager, we recommend you set the following properties:

   - Suite Name — This option allows you to set the name of your suite of racks. Use **Suite** → **Name** in main window.

   - Summary Info — This option allows you to set different properties of your rack configuration, such as: collection name, customer name, etc. Use **Files** → **Summary Info** in add this information.

3. Create the Netfinity files by selecting **Tools** → **Create Netfinity Files** in main window. A separate file is created for each server defined in the rack configuration. (see Figure 22 on page 46)



NETFINITY FILES LISTING

Component Name	Netfinity File Name
===============	================
7000 RM0 w/ optional pwr	d:\utils\rack\svr03005.rk$

Figure 22. Sample Export File Created

As an example, Figure 23 shows the export file created for a Netfinity 7000.

```
#=========================SVR03005.RK$=========================#
#
# Rack Interface File for:
#
#       COLLECTION:    "Server Room Building A"
#       RACK SUITE:    "Rack A"
#       RACK:          "A"
#       COMPONENT:     "7000 RM0 w/ optional pwr"
#       COMPONENT SN:  23-ABCDE
#
# Please copy this file into the root directory
# on the boot drive of the target machine
#
#==============================================================#

SuiteCollection=0
CollectionName="Server Room Building A"
RackSuite=82955752
SuiteName="Rack A"
RackPosition=A01
RackID=
RackType=9306900
RackWidthCapacity=483
RackHeightCapacity=1867
RackDepthCapacity=717
RackName="A"
ComponentPositionX=0
ComponentPositionY=1
ComponentPositionZ=0
ComponentType=8651RM0
ComponentSerialNumber=23-ABCDE
ComponentWidth=483
ComponentHeight=480
ComponentDepth=665
ComponentName="7000 RM0 w/ optional pwr"
```

Figure 23. Netfinity File Sample

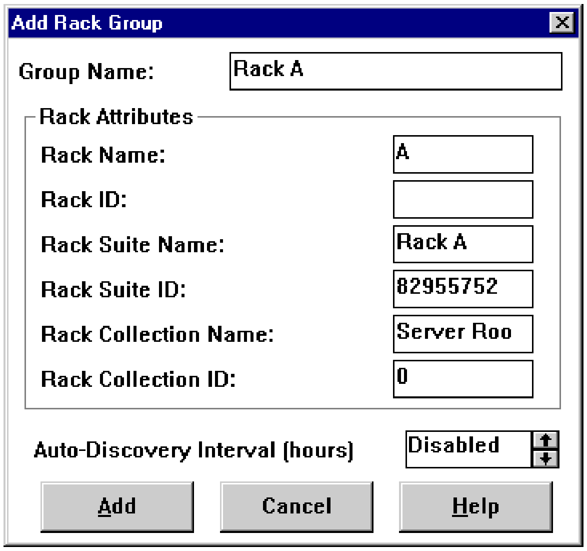
2.6.2.2 Using the Files in Netfinity Manager

Once the Rack Configurator has created the files, you can use them in Remote System Manager to allow Netfinity Manager to manage the rack or suite of racks. To use Netfinity files, perform the following steps:

1. Run **Remote System Manager** from the Netfinity Manager main window.

2. Add a rack group by clicking on **Group** → **Add Rack Group** in the Remote System Manager window.

3. Figure 24 appears.



Group Name: Rack A

Rack Name: A

Rack ID:

Rack Suite Name: Rack A

Rack Suite ID: 82955752

Rack Collection Name: Server Roo

Rack Collection ID: 0

Auto-Discovery Interval (hours) Disabled

Figure 24. Adding a Rack Group in Netfinity

4. Use the entries in the export file (Figure 23 on page 46) to fill in the required fields in Figure 24.

   - Enter a suitable name of the group in **Group Name**.
   - Fill in the other fields as shown in Table 8.

Table 8. What to Use to Fill in the Rack Group Fields

Field in Figure 24	**Entry in Export File (Figure 23 on page 46)**
Rack Name	RackName
Rack ID	RackID
Rack Suite Name	SuiteName
Rack Suite ID	RackSuite
Rack Collection Name	CollectionName
Rack Collection ID	SuiteCollection

   - Set the **Auto-Discovery Interval** time.

5. Press **Add** to complete the process.

You can then use the normal Remote Systems Manager functions to work on systems in the rack individually, or as a single group.

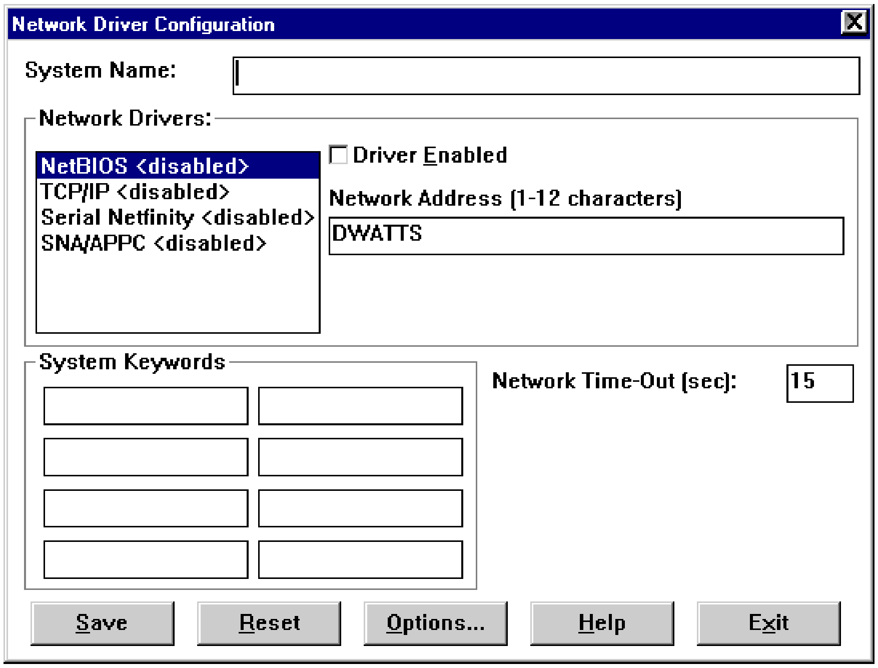
2.7 Netfinity Manager Security Implications

This section describes what security implications there are in using IBM Netfinity Manager.

As with any product that allows remote access to your filing system, the security implications must be examined before implementing a systems management solution. Failure to enforce suitable security could result in damage, either intentional or unintentional.

2.7.1 Network Driver Configuration

During installation, Figure 25 appears, giving you the opportunity to select and configure the Netfinity Manager the network protocols. You can also go back to this configuration by selecting the **Network Driver Configuration** from the program group. The network driver window allows you to select the supported network protocols that will allow access to Netfinity Manager.



System Name:

NetBIOS <disabled>
TCP/IP <disabled>
Serial Netfinity <disabled>
SNA/APPC <disabled>

□ Driver Enabled

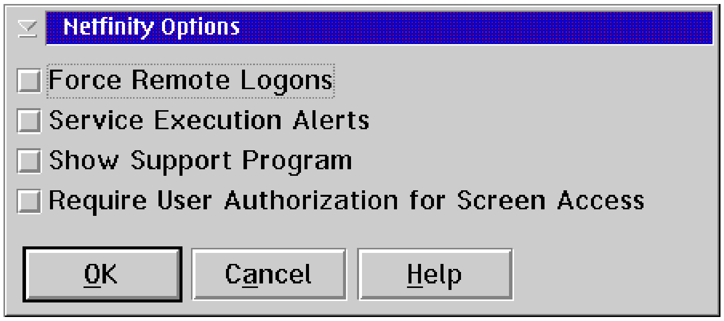
Network Address (1-12 characters): DWATTS

Network Time-Out (sec): 15

Figure 25. Netfinity Network Driver Options

The first consideration is whether you will require your machines to be accessed by more than one protocol. You may not want some machines allow access via the serial protocol, for example. The advantage of having more than one protocol per machine is that if you have a network problem with one protocol then the other may still be available.

The driver configuration window also contains a set of options accessible by clicking on **Options...** This windows can be seen in Figure 26 on page 49.



□ Force Remote Logons
□ Service Execution Alerts
□ Show Support Program
□ Require User Authorization for Screen Access

Figure 26. Netfinity Driver Options

The Netfinity Options window contains four special options that affect Netfinity Manager's network operations. These options are:

- Force Remote Logons

  After enabling this option, your system will not save the user ID/password combinations that you use to access remote systems. This means you will have to manually log on each time to any remote system that you want to access to. This is a distinct advantage if your Netfinity Manager is not physically secure, for example in an open office environment. The big disadvantage with this method is your administrator will have to remember the logons for many machines.

- Service Execution Alerts

  After enabling this option, Netfinity Manager will generate an alert whenever one of your Netfinity services is started by a remote user that is accessing your system. The alert includes the name of the service that was run and information about the user that started the service and gives you a degree of audibility.

- Show Support Program

  After enabling this option, the Netfinity Network Interface will be visible as a minimized icon or as a minimized process depending on the operating system you are running. This enables the user to shutdown the Netfinity Network Interface via a GUI. (You can also use `NETFBASE SHUTDOWN` from the command-line, regardless of this setting). This option is not available on systems that are running NetWare.

- Require User Authorization for Screen Access

  After enabling this option, a message will be displayed requesting approval when a remote user attempts to access the Screen View or Remote Workstation Control services on your system.

2.7.2 Security Manager

Security Manager is designed to restrict remote access to your machine through the Netfinity Manager services.

Security Manager uses a userid/password combinations to give access to your system to authorized users. Each userid can have access to one or more Netfinity Manager functions. You can also use Security Manager to configure pre-set userids for your access to other Netfinity Manager systems.

Authentication is split in to two parts:

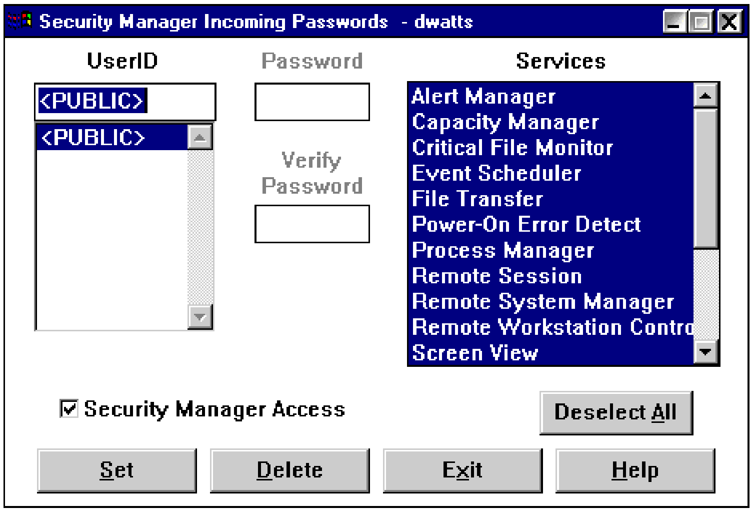
- Incoming userid/password combinations
- Outgoing userid/password combinations

Netfinity Manager Scheduler

The scheduler function is treated as an external system by Netfinity Manager. Consequently you need to define incoming and outgoing passwords on the same system. See 2.8, "Scheduling Regular Events" on page 56 for details.

2.7.2.1 Incoming Userids

These determine which of your services are available to a user accessing your system remotely. For each userid, you can specify which services can be accessed.



<PUBLIC>

<PUBLIC>

Alert Manager
Capacity Manager
Critical File Monitor
Event Scheduler
File Transfer
Power-On Error Detect
Process Manager
Remote Session
Remote System Manager
Remote Workstation Contro
Screen View

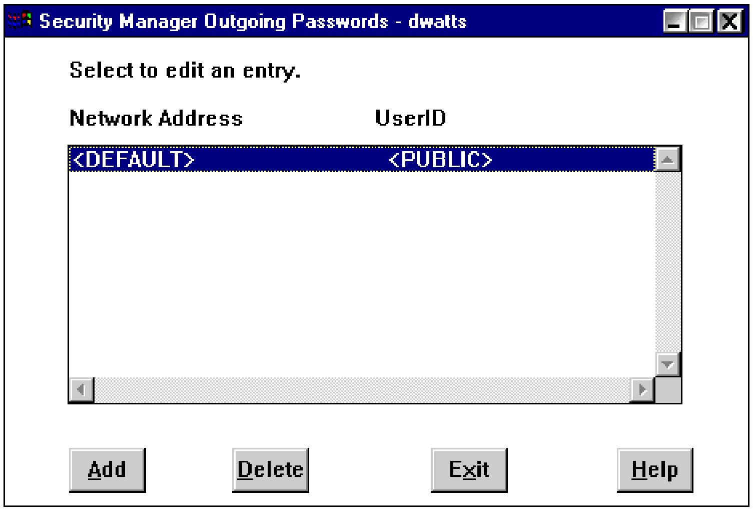
☑ Security Manager Access

Figure 27. Incoming Passwords

After installing Netfinity Manager, the <PUBLIC> userid will have full access to all services, as shown in Figure 27. It is *strongly* recommended that you remove all but the most harmless services, such as **System Information** and **System Profile**. You should deselect all other services, including removing the check mark from **Security Manager Access**, then click on **Set**. Failure to do so will make you system susceptible to intentional or unintentional damage.

2.7.2.2 Outgoing Userids

This is where you set userid/password combinations to access other Netfinity Manager systems. Initially, only the default userid exists and is set to <PUBLIC> as shown in Figure 28 on page 51.



Security Manager Outgoing Passwords - dwatts

Select to edit an entry.

Network Address	UserID
<DEFAULT>	<PUBLIC>

Figure 28. Initial Outgoing Passwords

This enables you to access other systems using the <PUBLIC> userid. If you wish to change the default to access remote systems with a userid other than <PUBLIC>, then double-click on the <DEFAULT> item and modify the userid and password values. This is useful if you access all or most remote systems using the same userid and password.

If you wish to access a system using a userid other than the default, you can do it in one of two ways:

1. Logging in via Remote Systems Manager

   From Remote System Manager, open the desired group and right-click on the desired remote system. A pop-up window as shown in Figure 29 appears.

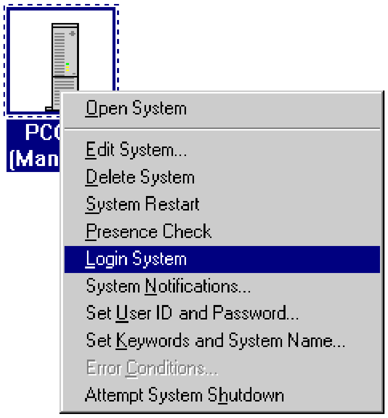


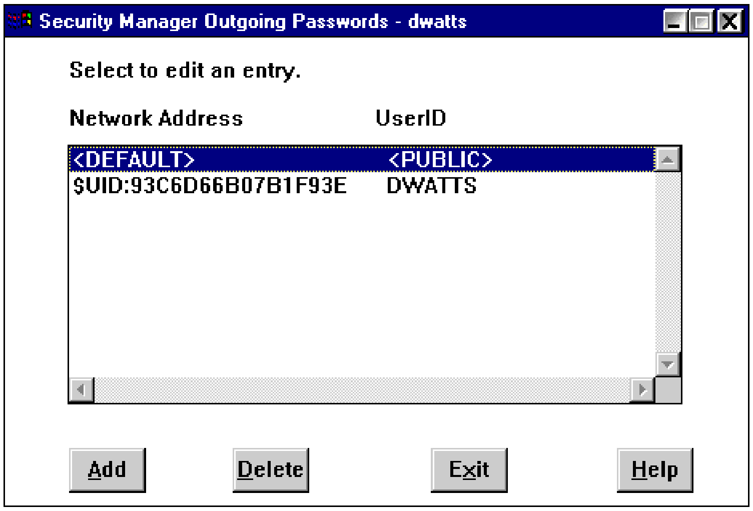
Figure 29. Logging On To a Remote System

   Click on **Login System** and you will be prompted to enter a userid and password. This values you enter will be compared with those listed in the Incoming Password list on the remote system and access will be granted to those services specified there.

   If you have not set **Force Remote Logons** as per 2.7.1, “Network Driver Configuration” on page 48, then you will also be prompted:

   ```
   Do you want this to be your default?
   ```

If you click on **Yes** then an entry will be added to your Outgoing Passwords list, as in Figure 30 on page 52.



Network Address	UserID
<DEFAULT>	<PUBLIC>
$UID:93C6D66B07B1F93E	DWATTS

Figure 30. Outgoing Password Added During a Manual Logon

This will mean that future accesses to that system will not require you to type in your userid and password.

2. Adding an Entry to the Outgoing Password List

   From the Outgoing Passwords window (Figure 30), click on **Add** You will then see Figure 31.

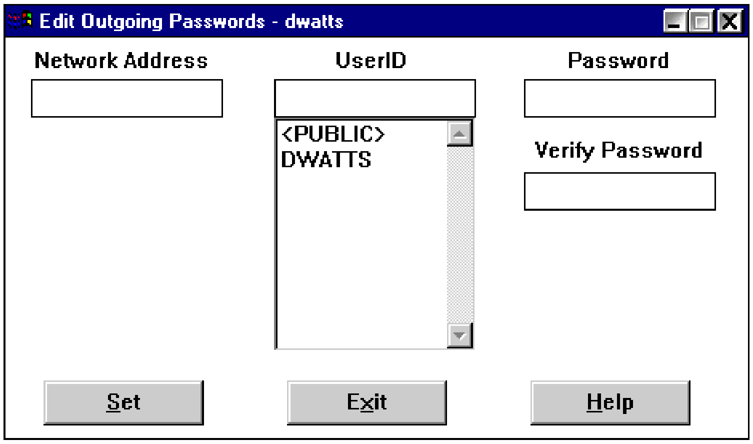


Figure 31. Adding an Outgoing Password Manually

From here you can type in the address of the system you want to access, and a userid and password that match an incoming userid on the remote system. The network address is the NetBIOS name or TCP/IP address or other suitable network address.

Note: The network address does not include the protocol used (for example, “TCP::”)

To save, click on **Set** then **Exit**.

2.7.2.3 Password Storage and Transmission

Check This

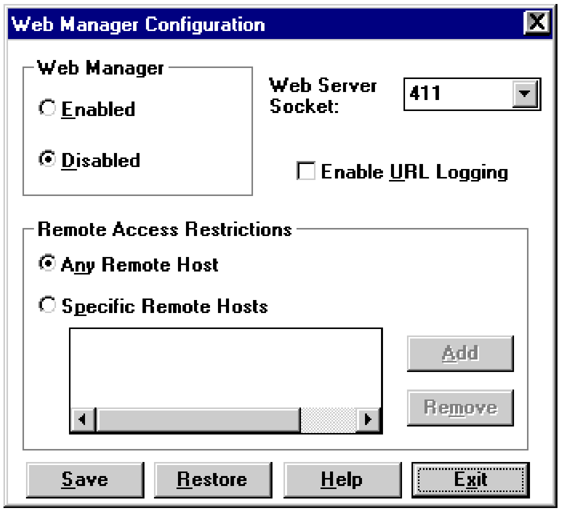
Incoming and outgoing passwords are stored in files in the Netfinity Manager directory. They are SECIN.INI and SECOUT.INI respectively. These files have the userids and machine IDs in plain text but the passwords are scrambled.

When passwords are set from one Netfinity machine to another, the passwords are kept in their scrambled state and only restored at the other end.

Note: Even though the passwords are encrypted on the hard disk, we recommend you limit access to the Netfinity Manager directory to prevent unauthorized access.

2.7.3 Web Manager

The Web Manager enables and disables access to Netfinity Manager on the local system via a Web browser. The configuration window is shown in Figure 32.



Web Manager
○ Enabled
● Disabled

Web Server Socket: 411

□ Enable URL Logging

Remote Access Restrictions
● Any Remote Host
○ Specific Remote Hosts

Figure 32. Web Manager Security

When enabled, all authorized systems running a Web browser, can access the Netfinity Manager manager functions. This enables you to do remote system management over the internet, without having to install Netfinity Manager on your machine.

You can use the Web Manager Configuration service to limit access to the to specific TCP/IP addresses or ranges of addresses. If specify the TCP/IP addresses, click on **Specific Remote Hosts** and Figure 33 on page 54 appears.

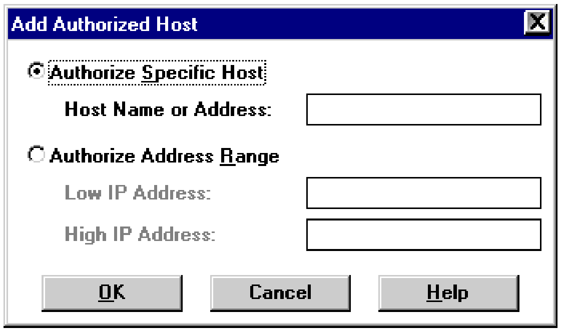


Figure 33. Giving Access to Specific TCP/IP addresses

Here you can specify either an individual IP address, or a range of IP addresses. They should be IP addresses in dotted form and not TCP/IP names. Click on **OK** to add the entry.

Note: If you wish to access a Netfinity Manager system via a Web browser through a Socks server, the IP address of the socks server must be one of the ones authorized to gain access.

You can also log all accesses from browsers by clicking on **Enable URL Logging**. Selecting this checkbox will enable logging to WEBFIN.LOG in your Netfinity directory (default C:\NETFIN). Each request made to the Web server will be recorded in the following form:

```
[date-time-stamp] [byte-order-address] [request]
```

The byte-order address can be converted to a normal dotted address. Consider a byte-order address of `94681809`:

1. break the address into four 2-digit hex numbers: 94-68-18-09
2. convert each of these into decimal: 148-104-24-9
3. reverse the order and this is the dotted address: 9.24.104.148

Note: Since many parameters are sent, sensitive data could potentially be logged (such as passwords), so you should ensure only authorized people can have access to the directory.

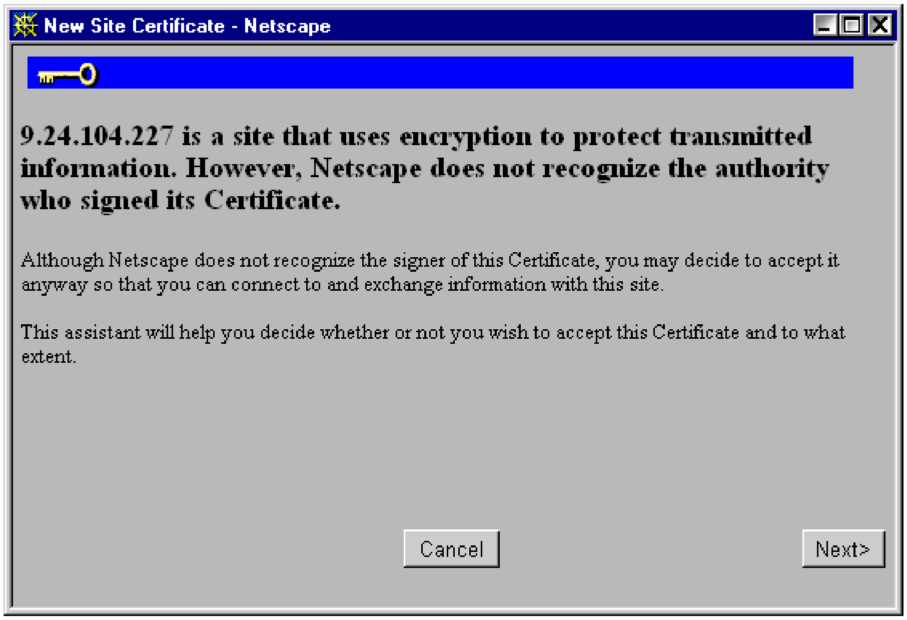
The logging action takes care to remove passwords from the log that are entered through the security service. However this does not prevent user from entering a password and having it logged by other services, such as while setting up an alert action to export alerts to a database.

2.7.3.1 Secure User Access

Normally, users would access the Netfinity system via the un-secured http:// protocol. However, if you are concerned about transmitting passwords as unprotected text, you can connect to the Netfinity Manager Web interface using SSL (https://). For example, using URL:

```
https://9.24.104.227:411/main
```

The first time you attempt this from your workstation, you will be prompted to verify the host you are connecting to. If you are using Netscape Navigator, the following window will appear


New Site Certificate - Netscape

9.24.104.227 is a site that uses encryption to protect transmitted information. However, Netscape does not recognize the authority who signed its Certificate.

Although Netscape does not recognize the signer of this Certificate, you may decide to accept it anyway so that you can connect to and exchange information with this site.

This assistant will help you decide whether or not you wish to accept this Certificate and to what extent.

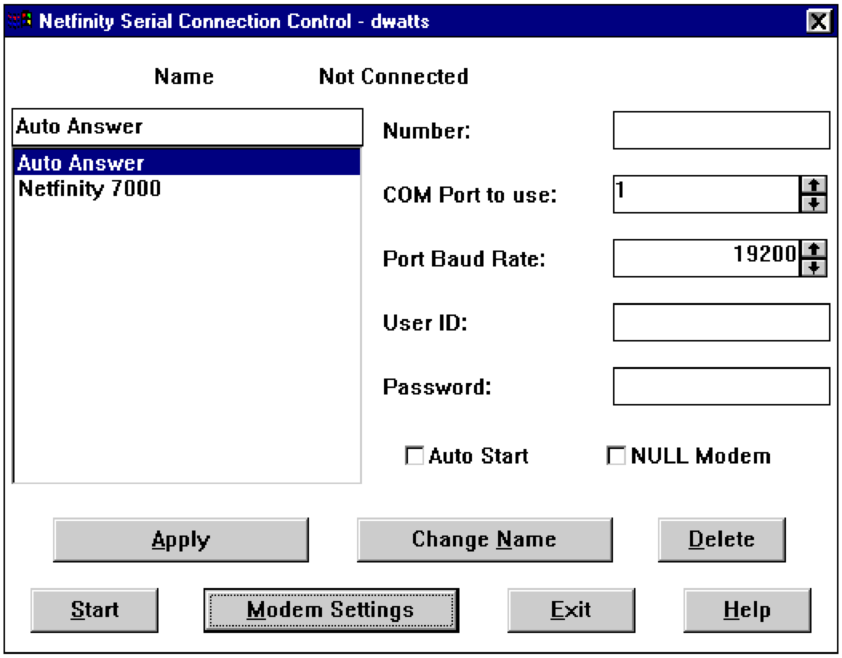
Figure 34. Setting up an SSL Encryption Certificate

The encryption used is of Export Grade (that is, using a 40-bit encryption key). Follow the instructions on the screen to complete the security certificate issuance.

2.7.4 Serial Access

The serial control function allows you to set up userids which can be used to dial out to other Netfinity Manager systems. It also enables you to configure the local system to let other system dial into it. Here we discuss the latter, that is how to configure the local machine to allow authorized access from other Netfinity Manager machines.

By default, external access via a modem is disabled. To enable it, open the Serial Control function. You will see Figure 35 on page 56.



Netfinity Serial Connection Control - dwatts

Name: Auto Answer

Not Connected

Auto Answer
Netfinity 7000

Number:

COM Port to use: 1

Port Baud Rate: 19200

User ID:

Password:

□ Auto Start □ NULL Modem

Figure 35. Netfinity Manager Serial Control

Select **AutoAnswer** if it isn't selected already. Select the COM port where your modem is that will answer any incoming calls and port speed at which it operates. Enter a userid and password into the appropriate fields then click on **Apply** to save the settings then **Start** If Serial Control can successfully connect to the modem, it sets the status at the top of the window to `Waiting for Call`.

Note: If you wish to have AutoAnswer always started and available, click on **Auto Start** in Figure 35. However, this will prevent the modem being used for any other purpose, including dial-out requests.

At this point your system is ready to receive calls from other Netfinity Manager systems. Any incoming user will have to user the userid/password combination you just entered. All users will have to share this userid/password.

Once a remote user is connected, they would use Remote Systems Manager to access other Netfinity Manager systems. The remote user will still need a valid userid and password that is in the Incoming Password list of any of the systems they want to access. This includes the system they dial into in the first place.

2.8 Scheduling Regular Events

Netfinity Manager's Scheduler function lets you configure events to run at regular intervals. In this section we describe how to use the Scheduler to regularly scrub (synchronize) the RAID array.

2.8.1 Scheduling a RAID Scrub

It is recommended you scrub (synchronize) your ServeRAID logical drives regularly. The easiest way to do this is to set up Netfinity Manager's scheduler to perform the scrub at regular intervals (for example every Tuesday night at midnight).

Note: The ability to schedule RAID scrubs is only available with Netfinity Manager Version 5.0 or later and is only necessary when using the IBM ServeRAID SCSI Adapter. It is not required when using the IBM ServeRAID II Ultra SCSI Adapter.

When you only have a small number of servers to scrub, we recommend you configure the schedule for each server individually, either locally on the server or through the Remote Systems Manager. This will ensure the scrub will occur as scheduled regardless of any network problems that may occur. If you have many servers, however, it would make sense to configure the schedule for all servers at once. In this case, ensure you have **Retry for offline systems** checked in Figure 39 on page 59.

To schedule an event to scrub all RAID arrays in a server, perform the following:

1. Double click on **Event Scheduler**. Figure 36 appears.

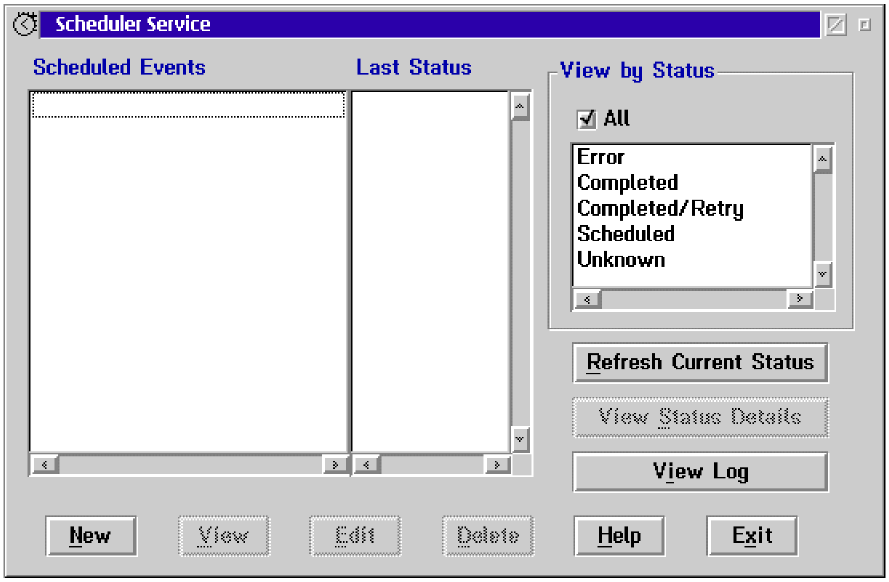
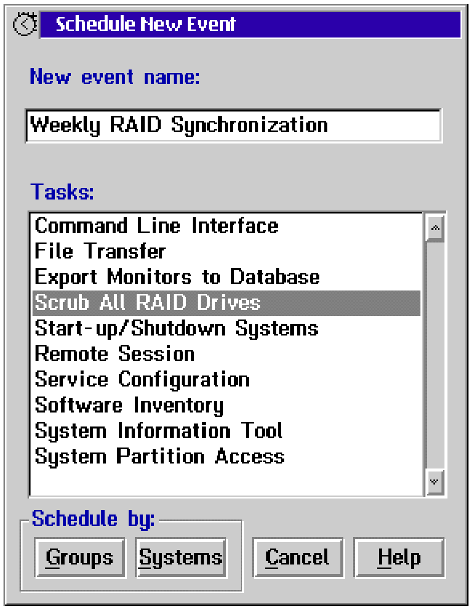


Figure 36. Event Scheduler Main Window

2. Click on **New**. Figure 37 on page 58 appears.



Schedule New Event

New event name: Weekly RAID Synchronization

Tasks:

Command Line Interface
File Transfer
Export Monitors to Database
Scrub All RAID Drives
Start-up/Shutdown Systems
Remote Session
Service Configuration
Software Inventory
System Information Tool
System Partition Access

Figure 37. Creating a New Scheduled Event

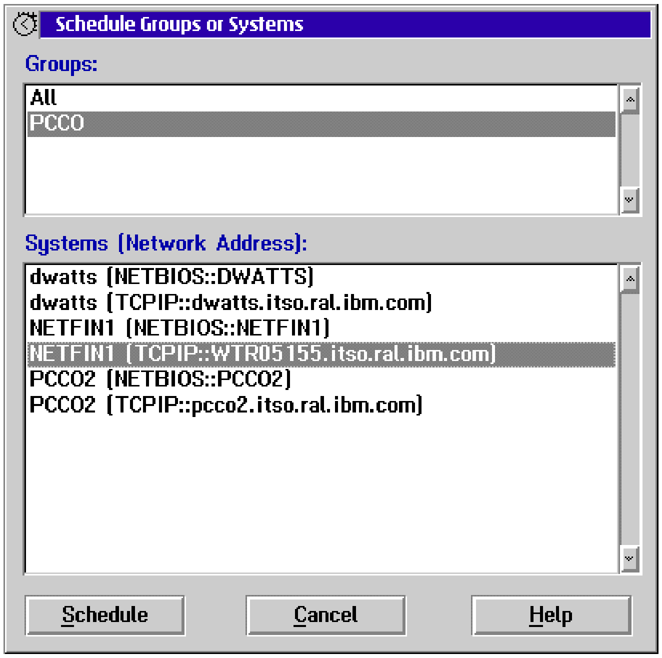
We recommend you perform a RAID scrub every week.

3. Type in an event name and select **Scrub All RAID Drives**.

4. Click on **Systems** to select individual systems or **Groups** for whole groups of systems.

   Note: You must have groups predefined via Remote System Manager otherwise you will receive an error message at this point.

   We clicked on **Systems** and Figure 38 appears.



Schedule Groups or Systems

Groups:

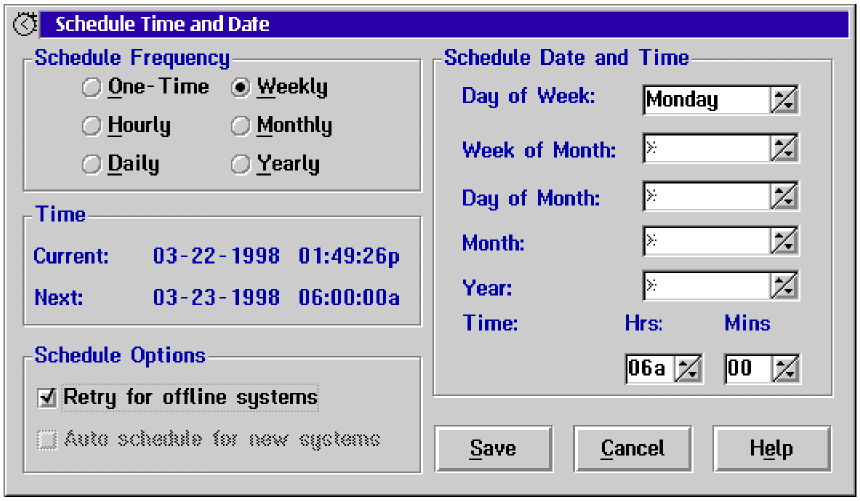
All
PCCO

Systems (Network Address):

dwatts (NETBIOS::DWATTS)
dwatts (TCPIP::dwatts.itso.ral.ibm.com)
NETFIN1 (NETBIOS::NETFIN1)
NETFIN1 (TCPIP::WTR05155.itso.ral.ibm.com)
PCCO2 (NETBIOS::PCCO2)
PCCO2 (TCPIP::pcco2.itso.ral.ibm.com)

Figure 38. Selecting the System to Schedule

5. Select the system or systems you want to schedule and click on the **Schedule** button. In this case this is the local server we are working on. Figure 39 on page 59 appears.



Schedule Frequency: ○ One-Time ● Weekly ○ Hourly ○ Monthly ○ Daily ○ Yearly

Current: 03-22-1998 01:49:26p

Next: 03-23-1998 06:00:00a

☑ Retry for offline systems

□ Auto schedule for new systems

Day of Week: Monday

Week of Month:

Day of Month:

Month:

Year:

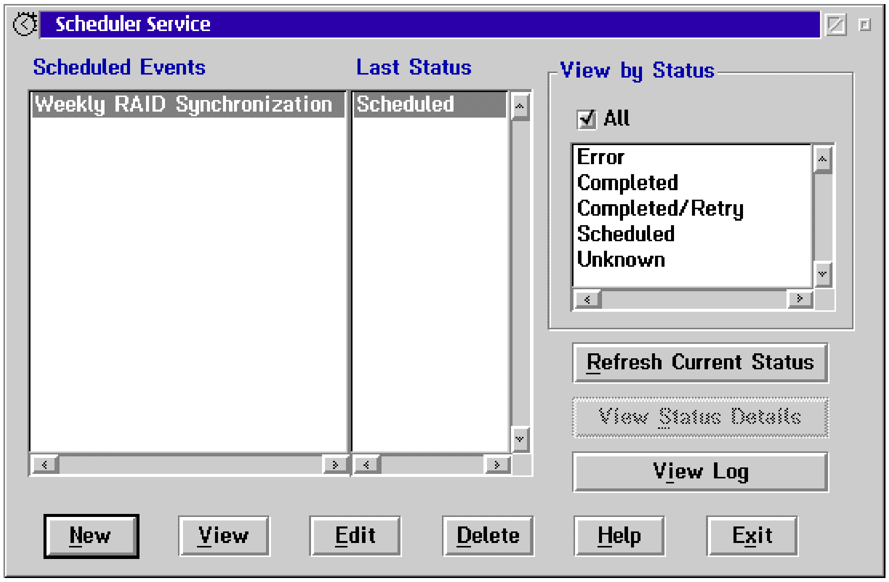
Time: Hrs: 06a Mins: 00

Figure 39. Configuring the Schedule

6. Specify the frequency, day and time you wish to start the scrub.

   If you are configuring the schedule on a remote system (that is, not the server you selected in Figure 38 on page 58) you should also click on **Retry for offline systems** to ensure network failures do not impact your RAID scrub schedule.

7. Click on **Save**. Figure 40 appears.



Scheduled Events	Last Status
Weekly RAID Synchronization	Scheduled

View by Status: ☑ All

Error
Completed
Completed/Retry
Scheduled
Unknown

Figure 40. Scheduled Events

At this point, the schedule has been configured. Now you need to ensure the appropriate security has been set as per 2.8.2, “Configuring Security” on page 60.

If you wish to view that status of previously run scrubs, click on **View Log**.

2.8.2 Configuring Security

If you have removed <PUBLIC> access to the RAID Manager on your server (which we recommend you do), you must set up an outgoing user ID and password on the system you are defining the schedule on. This also applies when you are defining the schedule at the server, as the Event Scheduler is always considered a remote user.

At the server (either locally or through the Remote Systems Manager), double-click on **Security Manager**. Figure 41 appears.

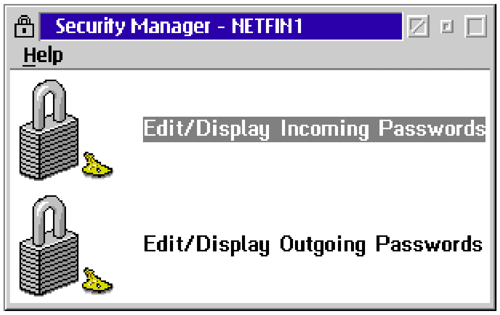
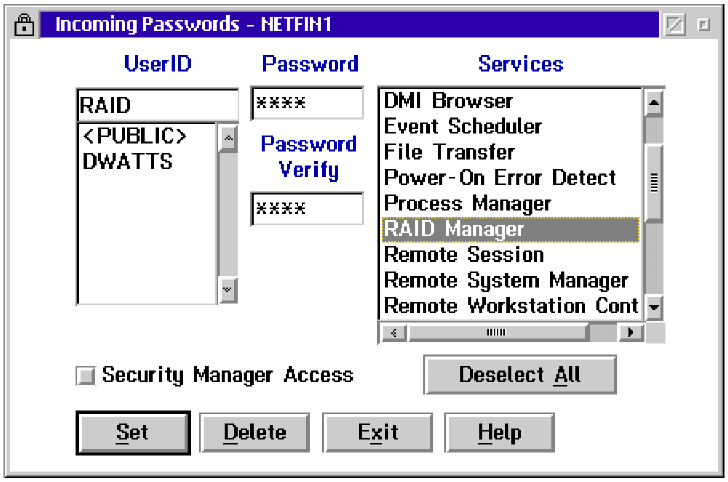

Security Manager - NETFIN1
Help
Edit/Display Incoming Passwords
Edit/Display Outgoing Passwords

Figure 41. Security Manager Main Window

Incoming passwords are those that allow access to this system from other systems in the network. Outgoing passwords are those that this system uses to gain access to other servers. The schedule service is actually considered to be an external user with respect to the security manager. As a result, you have to set both an incoming and an outgoing password to allow access to the scheduler.

To configure the incoming and outgoing passwords, do the following:

1. Double-click on **Edit/Display Incoming Passwords**. Figure 42 appears.



UserID: RAID

<PUBLIC>
DWATTS

Password: ****

Password Verify: ****

Services:

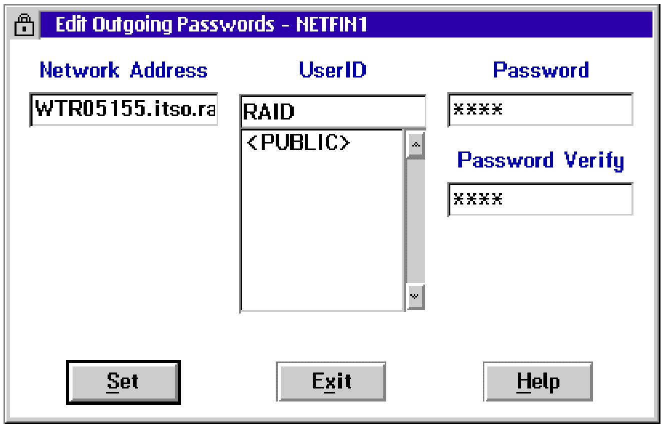
DMI Browser
Event Scheduler
File Transfer
Power-On Error Detect
Process Manager
RAID Manager
Remote Session
Remote System Manager
Remote Workstation Cont

□ Security Manager Access

Figure 42. Defining Incoming Passwords

2. Set up a userid and password to allow access to the RAID Manager as shown in Figure 42. This is the service that performs the RAID scrub. Click on **Set**.

3. Double-click on **Edit/Display Outgoing Passwords** then click on **Add**. Figure 43 on page 61 appears.



Edit Outgoing Passwords - NETFIN1

Network Address: WTR05155.itso.ra

UserID: RAID

<PUBLIC>

Password: ****

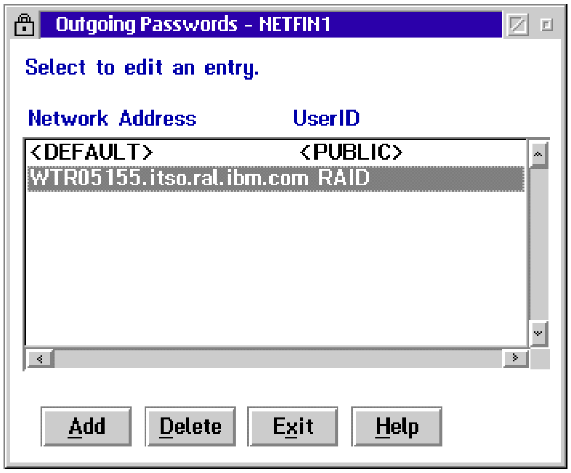
Password Verify: ****

Figure 43. Defining Outgoing Passwords

4. Specify the network address of the server. Ensure the address you type in matches the network address of the server you selected in Figure 38 on page 58. The userid and password you type in must match those in Figure 42 on page 60.

   Note: The network address does not include the protocol used (for example, “TCP::”)

5. Click on **Set**. A window similar to Figure 44 appears.



Outgoing Passwords - NETFIN1

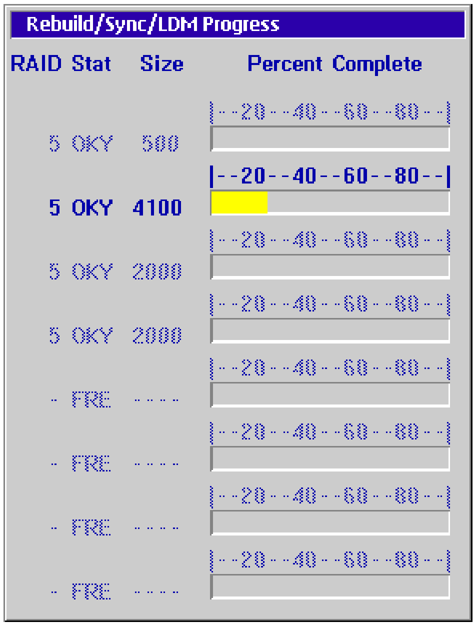
Select to edit an entry.

Network Address	UserID
<DEFAULT>	<PUBLIC>
WTR05155.itso.ral.ibm.com	RAID

Figure 44. Outgoing Passwords Set

6. Click on **Exit**. This concludes the configuration of Security Manager to allow scheduler access to the RAID subsystem.

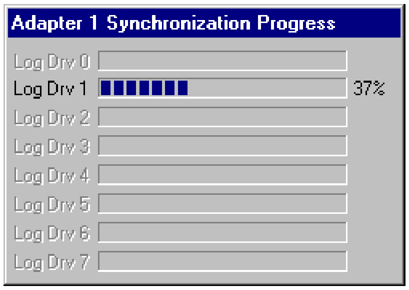
When the scheduled time arrives, the scrub will begin. If you wish you can view the progress of the scrub using the ServeRAID Administration Utility either locally (on Windows NT, OS/2 or NetWare servers) or remotely (using a Windows NT or Windows 95 client).



Rebuild/Sync/LDM Progress

RAID	Stat	Size	Percent Complete
5	OKY	500	|--20--40--60--80--|
5	OKY	4100	|--20--40--60--80--|
5	OKY	2000	|--20--40--60--80--|
5	OKY	2000	|--20--40--60--80--|
-	FRE	-----	|--20--40--60--80--|
-	FRE	-----	|--20--40--60--80--|
-	FRE	-----	|--20--40--60--80--|
-	FRE	-----	|--20--40--60--80--|

Figure 45. Progress Indicator — OS/2 Warp



Adapter 1 Synchronization Progress

Log Drv 0

Log Drv 1 37%

Log Drv 2

Log Drv 3

Log Drv 4

Log Drv 5

Log Drv 6

Log Drv 7

Figure 46. Progress Indicator — Windows NT

Chapter 3. Advanced Systems Management Adapter

The IBM Advanced Systems Management Adapter (part #94G5570) is an full-length ISA card designed to provide comprehensive systems management capability to IBM Netfinity and PC Servers.

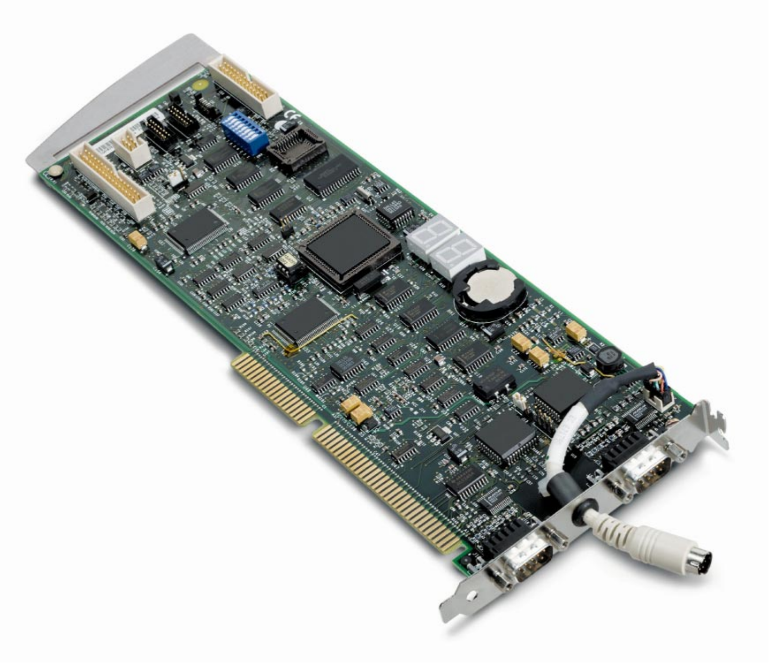


Figure 47. The Advanced Systems Management Adapter. The top connector is COM B and the bottom connector is COM A. A connector for an external power supply is in between the two COM ports.

Two Versions

There are currently two versions of the Advanced Systems Management Adapter: the current version, known as the “Pass 5” card as shown in Figure 47, and an earlier model, known as the “Pass 4” adapter. The two versions perform the same functions and can both be upgraded to the latest version of the firmware and configuration code. Only the Pass 5 card is currently available from IBM.

The major difference between the two cards is a change in the components on the end-plate of the adapter. The Pass 4 card has the power connector integrate with the end-plate rather than extending beyond it. The Pass 4 card also does not have plastic or metal guide at the other end of the adapter.

The Advanced Systems Management Adapter integrates fully with Netfinity Manager to provide both local and remote management of the server:

- Dial in to the systems management card even when the system is down to reset the server, browse a log of events detected by the service processor, check voltages and temperature, and control system power.
- Dial out to a pager or Netfinity Manager, via an external modem, to alert the system administrator if an error is detected.

- Full exploitation of the I²C bus of the Netfinity 7000, Server 325, Server 330 and other servers for additional systems management functions such as power control, fan, power, security and temperature monitoring.
- Remote POST Console support on the Server 325, 330 and Netfinity 7000 which echoes text data during system start-up to Netfinity Manager or a remote ANSI terminal.
- Additional remote diagnostics on some models of the PC Server 325 and 330 that feature ROM-based diagnostics.

The adapter has two DB9 serial ports, one of which (COM B) supports attachment of a modem for dial-in/dial-out functions. The other serial port (COM A) can be used as an additional system serial port by standard communications packages. The use of COM A, however, is not officially supported. We therefore recommend not to use COM A as serial port at all.

A connector is also provided to connect an external power supply option (#94G5571). This power supply is required for servers that do not have an internal continuous power feature and it provides continuous power even if the system is powered off or is down due to a mechanical malfunction. The following table lists the servers that require this option:

Table 9. External Power Supply Requirements

Server	**External Power Supply Required**
Netfinity 3000	Yes
Server 310	Yes
Server 315	Yes
Netfinity 3500	Yes
Server 325	No[1,2]
Server 330	No[1,3]
Netfinity 5500	No[1]
Server 704	Yes
Netfinity 7000	No[1]

Note:

1. The servers that do not require the external power supply also do not support the external power supply. For example, the external power supply is not required and is not supported on the Netfinity 7000.
2. The current Server 325 models 8639-xTx and 8639-xBx do not require the external power supply unit. The other, older models 8639-xJx and 8639-xSx *do* require the external power supply.
3. The current Server 330 models 8640-Pxx do not require the external power supply unit. The other, older models 8640-Exx *do* require the external power supply.

Note: The PC Server 704 requires both the external power supply option (#94G5571) and the Advanced Systems Management Adapter cable option (#94G6970) to be installed for proper operation. Installation of the cable without the use of the external power supply will cause the server to not power on.

The Advanced Systems Management Adapter can generate the following alerts:

- Operating system hung

- POST sequence timeout (325 and 330 only)
- Loader timeout (325 and 330 only)
- Non-critical temperature threshold exceeded
- Critical temperature threshold exceeded (automatic operating system shutdown)
- Temperature near Advanced Systems Management Adapter exceeded threshold
- Temperature near CPUs exceeded threshold (325, 330 and 7000 only)
- Temperature on planar exceeded threshold (325 and 330 only)
- Voltage thresholds exceeded
- Six incorrect attempts to enter Advanced Systems Management Adapter dial-in password
- Single fan failure
- Multiple fan failure (automatic operating system shutdown)
- Power on
- Power off
- Power supply failure (for redundant power supplies)
- Hard disk failure

This chapter explains how to configure the Advanced Systems Management Adapter using the configuration utility and Netfinity Manager.

Note: The terms “Advanced Systems Management Adapter” and “Service Processor” are used interchangeably to refer to the Advanced Systems Management Adapter.

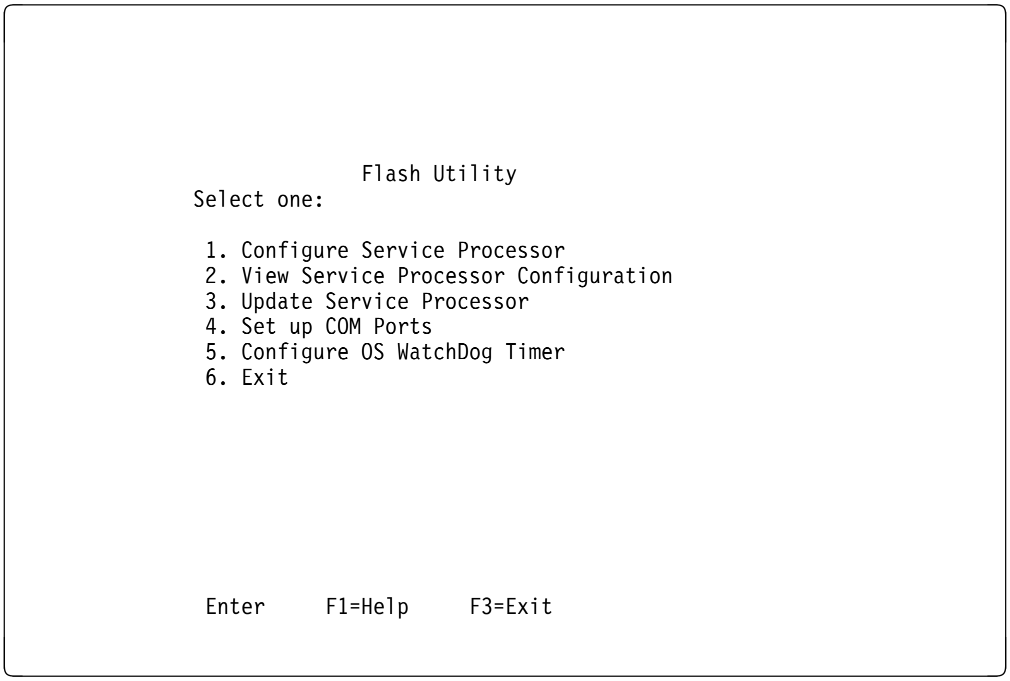
3.1 Configuration

The configuration utility is supplied on diskette with your Advanced Systems Management Adapter. For the latest version go to the following URL and search on “Management Adapter”:

```
http://www.pc.ibm.com/us/searchfiles.html
```

At the time of publication, the latest version is V2.20. We recommend you use this version or later.

To start the configuration utility insert the floppy disk and restart the server. After the welcome screen showing the version number of the utility, you will see Figure 48 on page 66, the utility's main menu.



```
                    Flash Utility
      Select one:

       1. Configure Service Processor
       2. View Service Processor Configuration
       3. Update Service Processor
       4. Set up COM Ports
       5. Configure OS WatchDog Timer
       6. Exit





       Enter     F1=Help     F3=Exit
```

Figure 48. Advanced Systems Management Adapter Utility Main Menu

Select different options by highlighting them using the cursor keys and pressing Enter. These options are:

1. Configure Service Processor

   This option changes the interrupt and I/O address used by the Advanced Systems Management Adapter card. You can assign any combination of IRQ and I/O address listed in Table 10 as long as it is not being used by other devices. We recommend you use the settings of IRQ 5 and I/O address 200-207.

Table 10. Valid I/O Addresses and Interrupts

I/O Address	Interrupt (IRQ)
100-107	3
120-127	4
140-147	5
168-16F	9
188-18F	10
200-207	11
220-227	14
240-247	15[1]
268-26F	
300-307	

Note:

[1] You should not use IRQ 15 under NetWare as it uses the IRQ to process lost interrupts.

2. View Service Processor Configuration

   Shows you IRQ and I/O address just configured.

3. Update Service Processor

   This option updates the microcode level of the Advanced Systems Management Adapter. To update the card highlight and press Enter. Follow the instruction on the screen.

4. Set up COM Ports

   This option leads you to the COM port configuration menu, as described in 3.1.1, “COM Ports.”

5. Configure OS WatchDog Timer

   This option enables or disables the operating system watchdog timer. If enabled, the system will reboot if a preset value for OS timeout is exceeded. Once the timer is enabled, you configure it in the Service Processor Manager in Netfinity Manager. See 3.2.2.6, “O/S Timeout” on page 75 for details.

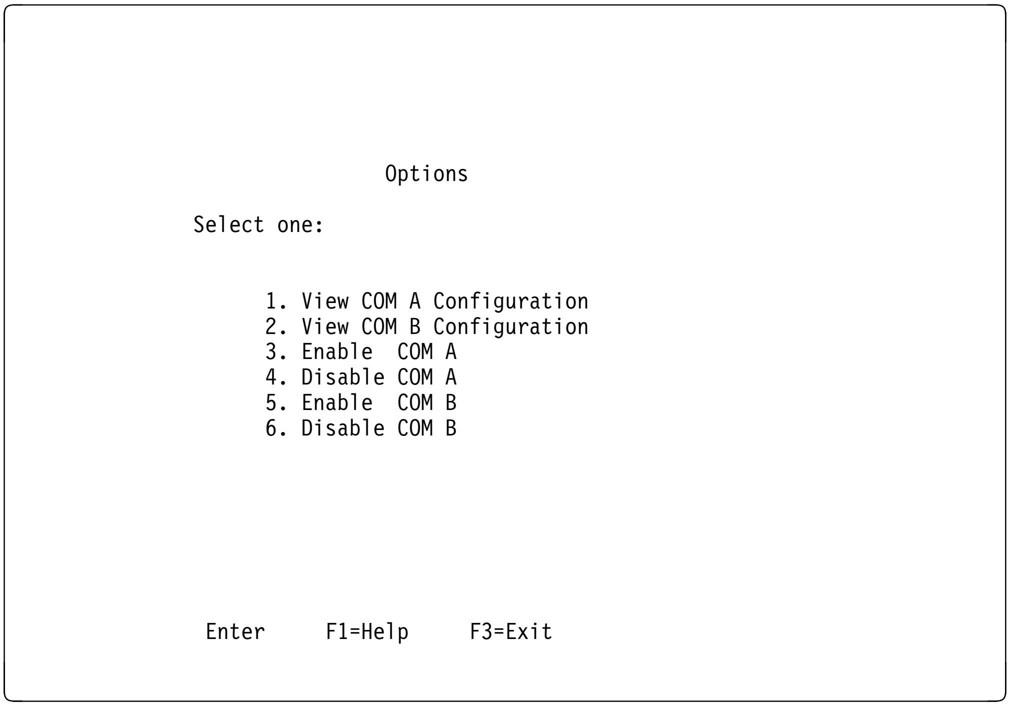
6. Exit

   Save the configuration and exit the utility.

Note: You must power off the server in order to apply the changes.

3.1.1 COM Ports

Selecting Option 4, **Set up COM Ports** from the main menu results in Figure 49 appearing.



```
                    Options

      Select one:


            1. View COM A Configuration
            2. View COM B Configuration
            3. Enable  COM A
            4. Disable COM A
            5. Enable  COM B
            6. Disable COM B





       Enter     F1=Help     F3=Exit
```

Figure 49. COM Port Configuration Utility

The options from this menu are:

- View Configuration (options 1, 2)

  Display resources currently used for the each COM port.

- Enable COM Ports (options 3, 5)

Enabling a COM port means the port is available to the operating system once it boots as well as the Advanced Systems Management Adapter. Disabling a COM port means only the adapter can use the port. By default, both COM ports are disabled.

Enabled Not Supported

At the time of writing, the ability to enable COM ports was still available. However, various problems have been occurring with this option set, so there are plans to remove the option and make them permanently disabled (that is, only available for use by the Advanced Systems Management Adapter card).

For the sake of completeness, we describe what enabling a COM port achieves but this is for informational purposes only. IBM will soon not be supporting the option so we recommend you do not enable it.

The **Enable COM Ports** option lets you assign IRQ and I/O Address for COM A and COM B. COM A is not used by the Advanced Systems Management Adapter, so can you assign resources to the port to be used as an additional COM port, such as COM 3. However, due to problems with the setup of the Advanced Systems Management Adapter COM ports at customer sites, sharing the the card's COM ports with the operating system is not supported anymore. We therefore recommend you do not enable COM A and do not use COM A at all.

COM B is used by the Advanced Systems Management Adapter to communicate via modem to another machine. Enabling COM B means the port is shared between the Advanced Systems Management Adapter card and the operating system. While the server is off, the COM B port is owned by the Advanced Systems Management Adapter. After the operating system boots, the COM port acts as a normal serial port.

When an operating system starts, it load its serial port driver for each COM port, but only for those ports that are *not in use*. Sharing the COM ports only really works if, at the time the operating system start, no active serial connection (dial-in or dial-out) exist. If a connection is active, the operating system will ignore the Advanced Systems Management Adapter COM port, however you will still be able to dial-in to the Advanced Systems Management Adapter using that port.

If you enable COM B and assign resources, make sure the resources are not use by any other device.

For example, if you assign IRQ 4 and I/O 3F8, you need to disable COM 1 in your server's setup as these values are used for COM 1.

- Disable COM Ports (options 4, 6)

  Disables the usage of the COM A and COM B. Disable means the COM ports are exclusively used by the Advanced Systems Management Adapter. In this mode, the attached modem will be unavailable to the operating system and to Netfinity Manager serial control. You will only by able to dial into the Advanced Systems Management Adapter. The Advanced Systems Management Adapter can dial out when one of the 14 selectable dial-out alerts occur or when an event log entry is made by Netfinity Manager (requires **Application** be checked in &servrpo. Automatic Dialout Settings as per Figure 57 on page 79).

If you want alerts being forwarded by Netfinity Manager via serial connection, you need a second modem or a null modem connection. For how to set up alerts see 2.4, “Alerts” on page 24.

COM A and COM B are disabled by default.

Note: Dial-in connection to Netfinity Manager via the Service Processor port does not work when the port is disabled.

To exit this menu, press F3. The configuration settings are automatically save in SM.INI on the utility diskette. This file provides setup information used during the device driver installation process.

3.1.2 Advanced Systems Management Adapter LEDs

The Advanced Systems Management Adapter has two 7-segment LEDs on board. These display different numbers depending on the status of the server. At boot up the LEDs display the POST Check Points. After operating system startup, the LEDs display different numbers depending on operating system and server type.

In the power-off status, the LEDs have two dashes in the middle and a slow blinking dot in the bottom right corner of one of them. The slow blinking dot in the bottom right corner indicates the adapter is properly configured and functional.

In addition, if the LEDs display “H1” or “H2” the server experienced an error:

- H1: The server experienced a voltage (spike or brown-out) that exceeded the threshold in either direction
- H2: The server experienced a temperature that exceeded the threshold

H1 and H2 will stay lit after the Advanced Systems Management Adapter has powered off the system.

3.1.3 Device Drivers

In order to install your Advanced Systems Management Adapter device driver correctly you must use the diskette you used to configure the adapter in the step above. The setup programs are located in subdirectories named corresponding to the operation system:

- In Windows NT run `A:\NT\SETUP.EXE`
- In NetWare from the server console run `LOAD A:\NETWARE\SETUP.NLM`
- In OS/2 run `A:\OS2\SETUP.EXE`

3.2 Adapter Configuration in Netfinity Manager

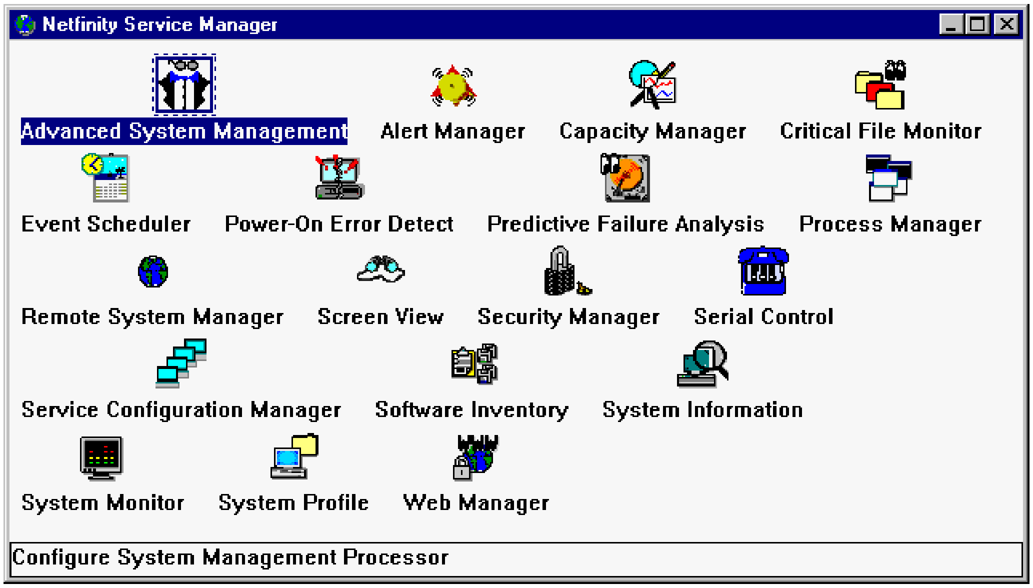
This section describes how to configure and enable the functions of the Advanced Systems Management Adapter and the Netfinity Advanced Remote Management processor in Netfinity Manager and how to enable dial-out alerts. Before you use the adapter for the first time you need to configure it. The Advanced Remote Management processor is preconfigured and will not normally need configuring.

Note: In the Netfinity Manager user guides, the Advanced Systems Management Adapter is often referred to as the Service Processor. In this book, when describing functions related to both the Advanced Systems Management Adapter and the Netfinity Advanced Remote Management processor, we will refer to them as Management Processors.

You can configure your Management Processor locally or remotely connected through the network or serial link, however you need to use Netfinity Manager or an "Active Client" installation of Client Services for Netfinity Manager.

In OS/2 and Windows NT, you can use Netfinity Manager or an active client installed on the server, but in NetWare, you need to connect to the server through Remote System Manager. Client Services for NetWare does not have a NLM to configure the Service Processor at the server console.

To start Netfinity Manager in Windows NT click on **Start** → **Programs** → **Netfinity** → **Netfinity Manager**.



Configure System Management Processor

Figure 50. Netfinity Manager Main Window

To start the Management Processor service, double-click on the **Advanced System Management** icon highlighted in Figure 50.

Notes:

1. Versions of Netfinity Manager prior to 5.10.4 named this icon Service Processor.
2. If your Netfinity Manager Main Window does not have the Service Processor icon or Advanced System Management icon, you will need to uninstall Netfinity Manager on your machine and install it again. When prompted for installation options, ensure that you select **Advanced System Management Support**.

The Advanced System Management window, shown in Figure 51 on page 71, contains program icons that are used to configure and operate your Management Processor. If you are connected to a remote Management Processor, the remote system name is displayed in the title bar of the Advanced System Management window.

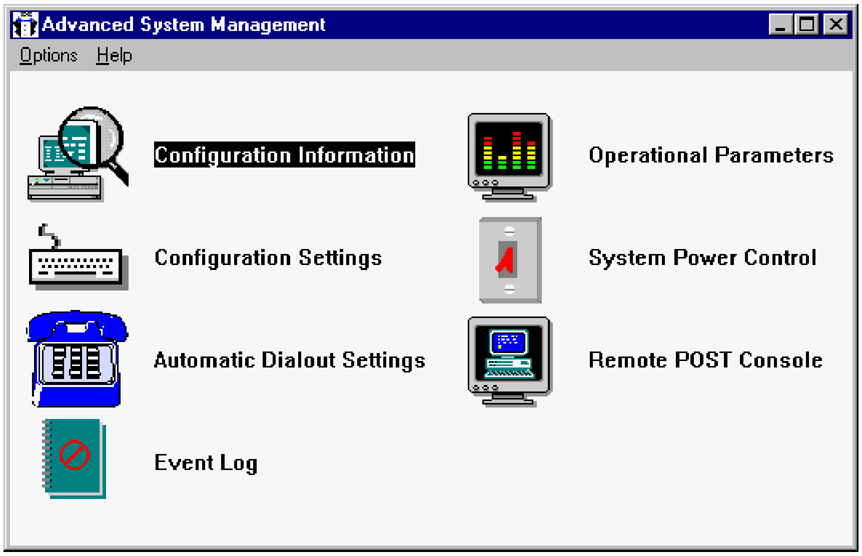


Figure 51. Advanced System Management Window

The **Options** → **Update Microcode** → **System Management Processor** pull-down menu option lets you update the firmware of the Management Processor When using the Advanced Systems Management Adapter either locally or via a LAN connection, this option will be grayed out. This is because the Advanced Systems Management Adapter can only have it's firmware updated when dialed into the adapter through its COM port. The Advanced Remote Management processor does not have this restriction.

The next section explains each of the program icons.

3.2.1 Configuration Information

Double-click on **Configuration Information** displays Figure 52 for the Advanced Systems Management Adapter and Figure 53 on page 72 for the Advanced Remote Management processor

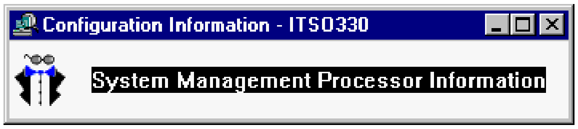

Configuration Information - ITSO330
System Management Processor Information

Figure 52. Configuration Information Options for Advanced Systems Management Adapter

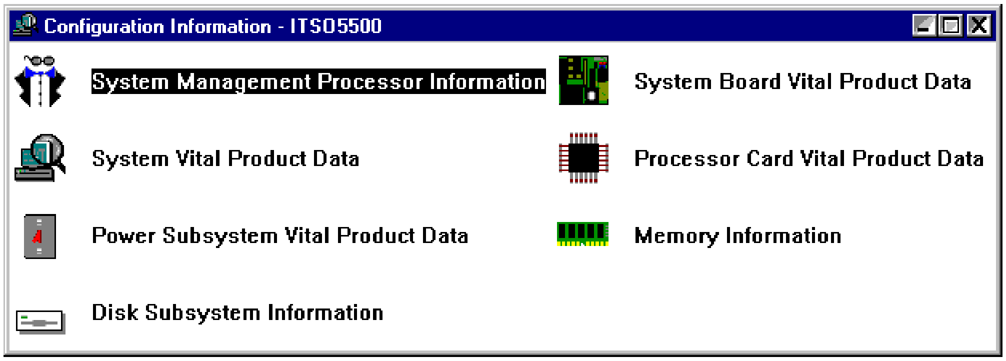
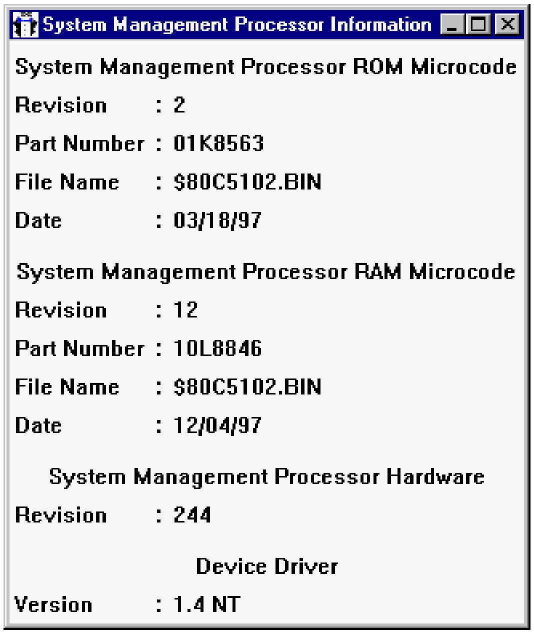

Configuration Information - ITSO5500
System Management Processor Information
System Board Vital Product Data
System Vital Product Data
Processor Card Vital Product Data
Power Subsystem Vital Product Data
Memory Information
Disk Subsystem Information

Figure 53. Configuration Information Options for Advanced Remote Management Processor

Double-clicking on **System Management Processor Information** shows the firmware levels of the Management Processor as shown in Figure 54.



System Management Processor Information

System Management Processor ROM Microcode

Revision : 2
Part Number : 01K8563
File Name : $80C5102.BIN
Date : 03/18/97

System Management Processor RAM Microcode

Revision : 12
Part Number : 10L8846
File Name : $80C5102.BIN
Date : 12/04/97

System Management Processor Hardware

Revision : 244

Device Driver

Version : 1.4 NT

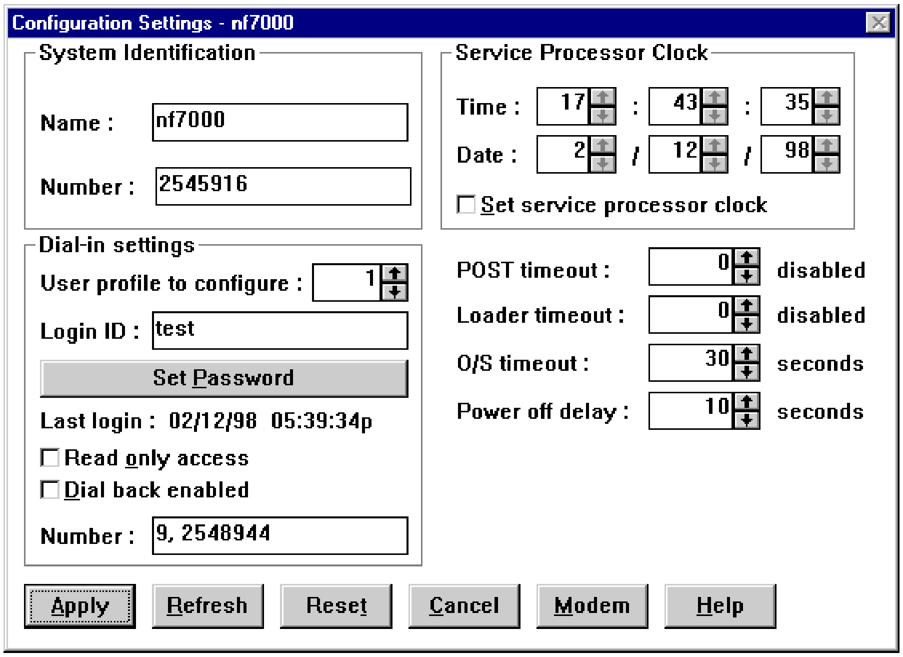
Figure 54. Management Processor Information

When accessing the Advanced Remote Management processor, the remaining options display information on the following components: information:

- System Vital Product Data: BIOS level, model, serial number, etc
- Power Subsystem Vital Product Data: Power supplies and power backplane
- Disk Subsystem Information: Internal hot-swap backplane
- System board
- Processor board
- Memory Information: Each memory DIMM size, speed, serial number, etc

3.2.2 Configuration Settings

The Configuration Settings window (Figure 55) is used to configure dial-in settings, system identification, processor clock and timer watchdogs for POST hangs, operating system loader hangs and operating system hangs. You also configure the modem here.



Configuration Settings - nf7000

System Identification

Name : nf7000

Number : 2545916

Service Processor Clock

Time : 17 : 43 : 35

Date : 2 / 12 / 98

□ Set service processor clock

Dial-in settings

User profile to configure : 1

Login ID : test

Last login : 02/12/98 05:39:34p

□ Read only access

□ Dial back enabled

Number : 9, 2548944

POST timeout : 0 disabled

Loader timeout : 0 disabled

O/S timeout : 30 seconds

Power off delay : 10 seconds

Figure 55. Service Processor Configuration Settings

Each of the items in this window are described below:

3.2.2.1 System Identification

These two fields let you enter a name and phone number which will identify the Service Processor. The phone number is for informational purposes only.

3.2.2.2 Service Processor Clock

The Service Processor has it's own independent clock. This clock is used to record the time and date for every operation of Service Processor such as event log or dial-out, regardless of the system status.

To change the time or date, you must first put a check mark in the **Set service processor clock** checkbox. You can then change the time and date using the spin controls, then press **Apply** to save the changes.

3.2.2.3 Dial-in Settings

The dial-in group of properties lets you enable or disable dial-in support, enable users to dial into and access the Service Processor. These properties are now described:

- User Profile to Configure

Use the spin buttons to select the user profile you want to configure. When using the Advanced Systems Management Adapter, you can configure up to six separate user profiles. With the Advanced Remote Management processor, you can configure up to 12 user profiles. Each user profile can have different login IDs and passwords.

- Login ID

  Type in this field the Login ID that will be used by the user wanting to dial into this machine. A Login ID must be specified to enable remote access.

- Set Password button

  If a password is configured, it must be provided along with the Login ID to allow a remote user to access the Service Processor. After providing a Login ID, click on the **Set Password** button to open the Set Password window.

- Last Login field

  This shows the date and time of the last successful login by this particular user.

- Read only access

  If the **Read only access** check box is checked, the currently selected user profile will not be able to alter any of the Service Processor settings when access is granted. The user profile will, however, be able to see all currently configured settings and values.

- Dial back enabled

  If the **Dial back enabled** check box is checked, the Service Processor will automatically terminate the connection as soon as the selected user profile logs in, and will then use the telephone number that is entered in the **Number** field to dial out and attempt to connect with the remote system.

If necessary, click on the **Modem** button to access the Modem Settings window. These settings enable you to specify modem settings and dialing settings. See 3.2.3, “Port and Dialing Settings” on page 76 for details.

Creating a New User: To create a new login ID for a remote user:

1. Use the **User profile to configure** field to select a user profile that is not already in use.
2. Type the ID that will be used by the remote user into the **Login ID** field. This ID can be up to eight characters long.
3. If you want remote users to supply a password in order to gain access to the Service Processor, click on the **Set Password** button and enter a password for them to use.
4. Click on **Apply** to remove the user ID.

Note: We recommend you set a password to prevent unauthorized access to you system. If you do not configure a password, any remote user that knows the configured login ID can use the Service Processor Manager service to access your system's Service Processor. If you configure a password, remote users will have to supply both the correct login ID and the correct password to access the Service Processor. For additional security, use the dial-back setting.

Deleting an Existing User: To delete the currently configured login ID:

1. Select the user you want to delete in the **User profile to configure** field.
2. Select 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.

3.2.2.4 POST Timeout

The **POST timeout** field is used to configure the time the Service Processor will allow the system to complete the POST before it initiates a system restart.

If the POST takes longer than the time specified, the Service Processor will generate a POST time-out event and forward a POST time-out alert to all enabled dial-out entries. See 3.2.4, “Automatic Dialout Settings” on page 79 for details on how to configure dial-out entries.

You should time how long it normally takes to complete the POST. You can then set a POST timeout value greater than this value.

The first time the POST timeout occurs, the system will reboot automatically. It does not reboot on the second successive POST timeout.

Note: This option is only available on the Server 325 and Server 330.

3.2.2.5 Loader Timeout

The **Loader timeout** field is used to configure the time the Service Processor will allow the server to load the operating system before it initiates a system restart. The operating system is considered loaded once the Advanced Systems Management Adapter driver is started.

You should disable this option if you are reinstalling your operating system or whenever you don't boot using the standard boot process which loads the Advanced Systems Management Adapter driver.

If the time between POST and the end of operating system startup exceeds the configured time, the Service Processor will generate a loader time-out event and forward a loader time-out alert to all *enabled* dial-out entries with the Loader time-out field selected in their Automatic Dial-out Settings configuration (see 3.2.4, “Automatic Dialout Settings” on page 79).

The first time the loader timeout occurs, the system will reboot automatically. It does not reboot on the second successive loader timeout.

Note: This option is only available on the Server 325 and Server 330.

3.2.2.6 O/S Timeout

The **OS timeout** field is used to configure the time the Service Processor will wait before it initiates a system restart, in case the operating system stops responding to the Service Processor.

If the responds time exceeds the configured value, the Service Processor will generate a OS timeout event and forward a OS timeout alert to all enabled dial-out entries that have OS timeout selected in their Automatic Dial-out Settings configuration (see 3.2.4, “Automatic Dialout Settings” on page 79). The system will then be rebooted.

Note: This option is available on all Netfinity and PC Server systems.

3.2.2.7 Power Off Delay

When a shutdown is requested via the Advanced Systems Management Adapter, the operating system is either shutdown (Windows NT and NetWare) or effectively rebooted (OS/2) then powered off. If there is a problem with the shutdown, unless a timeout is set, the system may never shutdown.

The **Power off delay** field is used to configure the time the Service Processor will wait for the operating system to shut down before powering off the system, when such problems occur. If the Service Processor initiates a power-down procedure, a Power Off event is generated and a Power Off alert is forwarded to all enabled Dial-out entries that have Power off selected in their Automatic Dial-out Settings configuration (see 3.2.4, “Automatic Dialout Settings” on page 79).

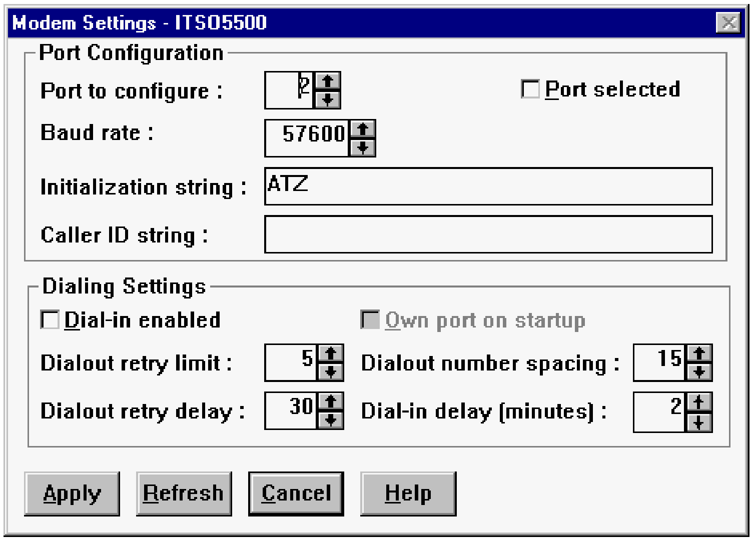
To find out what is a suitable value to put here, we recommend you time how long it takes to shut down your server when no problems occur, then set the power-off delay to a value slightly above this time.

Click on Apply to Save

If you change any option or setting, you must select the **Apply** button to store these changes in the Service Processor.

3.2.3 Port and Dialing Settings

Clicking on the **Modem** button in the window shown in Figure 55 on page 73 brings up the Modem Settings window shown in Figure 56. There are two groups of properties in this window: Port Settings and Dialing Settings.



Modem Settings - ITSO5500

Port Configuration

Port to configure : 2

☐ Port selected

Baud rate : 57600

Initialization string : ATZ

Caller ID string :

Dialing Settings

☐ Dial-in enabled

▨ Own port on startup

Dialout retry limit : 5

Dialout number spacing : 15

Dialout retry delay : 30

Dial-in delay (minutes) : 2

Figure 56. Service Processor Modem Settings

3.2.3.1 Port Settings

Use the Modem Settings group to specify and configure the modem that will be used to forward the alert when a Service Processor Dial-out Event occurs.

- Port to Configure

  This option lets you select the Management Processor port connected to the modem. With the Advanced Systems Management Adapter, there will only be one option, “1” as the Advanced Systems Management Adapter only uses a modem on COM B. The Advanced Remote Management processor lets you separately configure Ports 1 and 2 which correspond to COM B and COM C respectively.

- Baud Rate

  Use the spin buttons to specify the speed you wish to set the modem to. The Advanced Systems Management Adapter can go up to 38400 bps and the Advanced Remote Management processor can be set up to 57600 bps.

  Note: We have found setting the Advanced Systems Management Adapter to values higher than 19200 can cause data corruption.

- Initialization String

  Type in the initialization string that will be used for the specified modem. We found that leaving the field empty was sufficient for our modems.
  If you need to specify an initialization string, you will need enter modem command that perform the following functions:

  – Command echoing OFF
  – On-line 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

Problems?

If you have trouble with your modem configuration, look in the Service Processor Event Log. Messages like

```
Modem configured but not responding
```

indicate the card can not communicate with the modem properly. If you use an initialization string delete it and try again.

- Caller ID String

  This field is currently not implemented and should be left blank. This field is not available with the Advanced Systems Management Adapter.

- Port Selected

  Check this option to enable the use of the COM port. If you want the Management Processor to use the port, it must be enabled here.

- Null Modem check box

Check this check box to use a null modem connection to allow access from a remote Netfinity system.

Note: The null modem connection cannot be used for sending alerts through the Management Processor. It is only for connecting *to* the card.

3.2.3.2 Dialing Settings

Use the Dialing Settings group to specify settings that will be used to forward the alert when a Management Processor Dial-out Event occurs.

- Dial-in Enabled

  Check this check box to enable remote users to dial into and access the Management Processor. If this box is unchecked, remote users will be unable to dial into the Management Processor.

- Own Port On Startup

  With the Advanced Systems Management Adapter, you need to tick this checkbox if you disabled COM B. Configuration Utility (see 3.1.1, “COM Ports” on page 67). If you do not do so, the COM port will be released by the adapter but not taken over by the operating system at boot-up and will be unavailable for both. Disabling the COM port means that it is not available to the operating system once it boots. If you enabled COM B in the adapter configurator, untick this checkbox.

  Note: Enabling the COM port is not supported with the Advanced Systems Management Adapter, so you should ensure this checkbox is ticked.

- Dial-out retry limit

  Use the spin button to select how many times the Management Processor attempts to dial with the modem to forward the alert.

- Dial-out delay

  Select a delay in seconds before the Management Processor retries to forward the alert again.

- Dial-out Number Spacing

  If you have configured more than one dial-out entry to forward alerts, the Management Processor will attempt to contact each of these entries sequentially. Use the spin buttons to specify the number of seconds that the Management Processor should wait between dial-out attempts for separate Dial-out Entries.

- Dial-in delay (minutes)

  This field shows the number of minutes that must pass after an incorrect User ID or Password has been used in a dial-in attempt to the Management Processor, before any valid dial-in access will be permitted.

  Note: If six failed attempts are made to dial into the adapter, the adapter will generate a “Tamper” event, as described in 3.2.4, “Automatic Dialout Settings” on page 79.

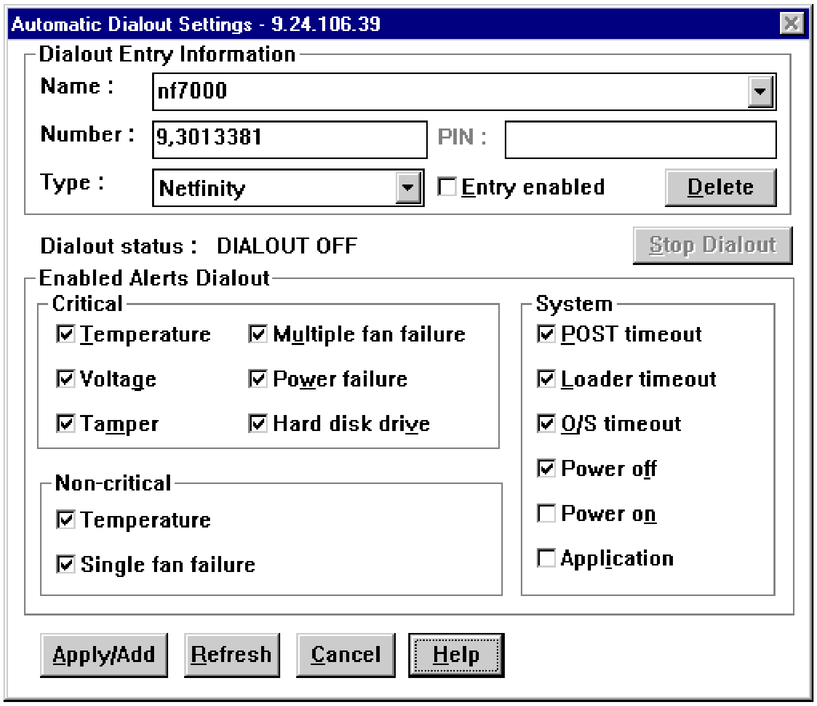
Click on Apply to Save

If you change any option or setting, you must select the **Apply** button to store these changes in the Service Processor.

3.2.4 Automatic Dialout Settings

Double-clicking on the **Automatic Dialout Setting** icon yields Figure 57. This is where you configure when and how the Management Processor dials out to a remote machine. You can configure the card to dial out when particular critical and non-critical alerts occur and these alerts can be sent to three different types of devices:

- A numeric pager
- An alphanumeric pager
- A remote Netfinity Manager system



Automatic Dialout Settings - 9.24.106.39

Dialout Entry Information

Name : nf7000

Number : 9,3013381 PIN :

Type : Netfinity □ Entry enabled

Dialout status : DIALOUT OFF

Enabled Alerts Dialout

Critical

☑ Temperature ☑ Multiple fan failure

☑ Voltage ☑ Power failure

☑ Tamper ☑ Hard disk drive

Non-critical

☑ Temperature

☑ Single fan failure

System

☑ POST timeout

☑ Loader timeout

☑ O/S timeout

☑ Power off

□ Power on

□ Application

Figure 57. Service Processor Automatic Dial-out Settings

You can configure up to six separate entries. If a particular alert is enable for multiple entries, the dial-out phone calls will occur sequentially.

The fields in this windows are as follows:

3.2.4.1 Dial-out Entry Information

- Name

  Enter a name which will identify the dial-out event. You can also select previously added events which you can modify.

- Number

  This is the phone number that will be dialed when a dial-out event occurs.

- Type

This is where you select what sort of device is on the other end of phone line. There are three choices:

1. A numeric pager
2. An alphanumeric pager
3. A remote Netfinity Manager system

- PIN

  If you select “Alpha-numeric” from the **Type** field, the PIN field will become active. You can then enter the PIN number associated with the pager you wish to call.

- Entry enabled

  Check the box if you want to enable this particular dial-out entry. If you do not check the box, the dial-out entry will not be used to transmit alerts.

- Delete button

  Use the Delete button to erase a dial-out entry.

3.2.4.2 Dial-out Status

Displays the present status of the Service Processor. The status will be either `DIALOUT OFF` or `DIALOUT ON`. When it is on, the Service Processor is currently performing a dialout function. You can use the **Stop Dialout** button to interrupt a dial-out process.

Note: Examine the **Dial-out Status** field after you configure your dial-out entries to see whether the dial-out attempt is successful or not. The dial-out status displays an attempt to dial-out — `DIALOUT ON` will appear even when the Service Processor is not connected to a modem.

3.2.4.3 Critical Alerts

These alerts are generated if a system enters a critical status like hard drive failure, power supply failure, high voltage or the system is in danger of being damaged due to overheating. Most of these alerts use hard-coded thresholds.

- **Temperature**: if any of the monitors report that the temperature has exceeded the threshold, the Management Processor will issue an alert and attempt to shutdown the operating system and power off the server.
- **Voltage**: if the monitors power sources are outside of their operational ranges, an alert will be issued and an attempt to shutdown the operating system and power off the server will be made.
- **Tamper**: if checked, the Management Processor will dial out when six consecutive login attempts are made using an invalid password.
- **Multiple fan failure**: if checked, the Management Processor will dial out if two or more of the system's fans fail. The Management Processor will attempt to shutdown the operating system and power off the server.
- **Power failure**: an alert will occur if a redundant power supply fails. The power supply failure alert will only be issued if either of the following are true:
  - There is still another power supply running in the server
  - The external power supply option for the Advanced Systems Management Adapter is used, on servers where it is required and supported. (see Table 9 on page 64)

The battery on the Advanced Systems Management Adapter is not designed to provide sufficient power to dial-out with an alert.

- **Hard disk drive**: an alert will be issued if a hard disk in the system fails.
- **Voltage regulator module failure**: if checked and if you system has a VRM, the Management Processor will dial out if the VRM fails.

  Note: This option is not available with the Advanced Systems Management Adapter.

3.2.4.4 Non-Critical Alerts

The following non-critical alerts are configurable:

- **Temperature**: If checked, the Management Processor will dial out if any monitored temperatures exceed their threshold values. However, unlike the Critical Temperature alert, this alert will not initiate a system shutdown automatically.
- **Single fan failure**: an alert will be issued if one fan fails.
- **Voltage** If checked, the Management Processor will dial out if any monitored voltage exceed their threshold values. However, unlike the Critical Voltage alert, this alert will not initiate a system shutdown automatically. This option is not available on the Advanced Systems Management Adapter.

3.2.4.5 System Alerts

The System group enables dial-out events to cover operational fault such as operating system loader (that is, operating system boot) time-out or power on/off events. For how to configure the timeout WatchDog timers, see 3.2.3, “Port and Dialing Settings” on page 76.

- **POST timeout**: the POST timeout (as configured in 3.2.2.4, “POST Timeout” on page 75) was exceeded.
- **Loader timeout**: the Loader timeout (as configured in 3.2.2.5, “Loader Timeout” on page 75) was exceeded.
- **O/S timeout**: the operating system boot timeout (as configured in 3.2.2.6, “O/S Timeout” on page 75) was exceeded.
- **Power off**: the Management Processor will dial out if server was powered off using the on/off button on the server. Power must still be available to the Management Processor for this alert to be issued. For the Advanced Remote Management processor, the server's power supply must still be receiving mains power. For the Advanced Systems Management Adapter, either the server's power supply must still be receiving mains power or the external power supply option for the adapter (where supported — see Table 9 on page 64) must still have power.
- **Power on**: the Management Processor will dial out when the server is powered on.
- **Application**: This option, when checked, will cause the Management Processor to dial out when it receives an alert from Netfinity Manager when you configure it to the action “Send alert to system management processor error log.” You can then dial into the Management Processor and examine the Event Log to see the alert. See 2.4, “Alerts” on page 24 for details about setting up alerts in Netfinity Manager.

- **PFA**: the Management Processor will dial out if it receives a PFA notification from the server. This is only available on systems that have specially architected PFA hardware, such as the Netfinity 5500. It is not available with the Advanced Systems Management Adapter.

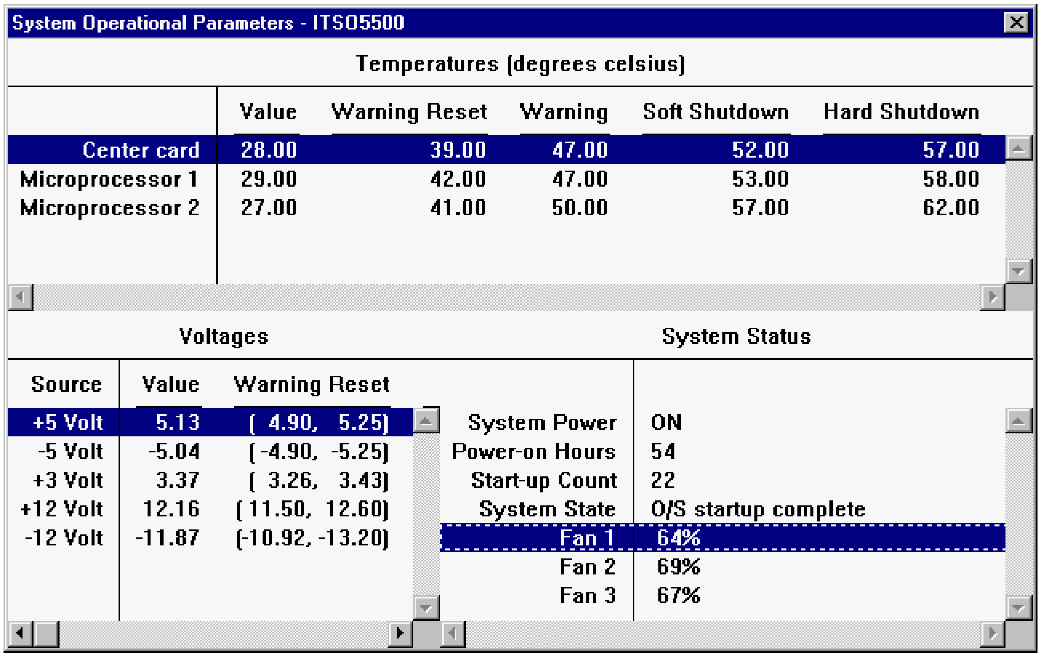
3.2.5 Event Log

The Event Log window enables you to view the contents of the Service Processor Event Log. Information about all remote access attempts and dial-out events that have occurred are recorded in the Service Processor Event Log.

The event log is very useful to troubleshoot problems with the attached modem. It will give you the a first hint to solve problems concerning modem setup.

3.2.6 Operational Parameters

The Operational Parameters window (Figure 58) shows the current values or status of many system components monitored by the Management Processor. The values that are available are dependent upon the hardware configuration of the system.



System Operational Parameters - ITSO5500

Temperatures (degrees celsius)

	Value	Warning Reset	Warning	Soft Shutdown	Hard Shutdown
Center card	28.00	39.00	47.00	52.00	57.00
Microprocessor 1	29.00	42.00	47.00	53.00	58.00
Microprocessor 2	27.00	41.00	50.00	57.00	62.00

Voltages

Source	Value	Warning Reset
+5 Volt	5.13	(4.90, 5.25)
-5 Volt	-5.04	(-4.90, -5.25)
+3 Volt	3.37	(3.26, 3.43)
+12 Volt	12.16	(11.50, 12.60)
-12 Volt	-11.87	(-10.92, -13.20)

System Status

System Power	ON
Power-on Hours	54
Start-up Count	22
System State	O/S startup complete
Fan 1	64%
Fan 2	69%
Fan 3	67%

Figure 58. Service Processor Operational Parameters on Netfinity 5500. Note that the Voltages window is scrollable.

Values that are available, depending on the server model are:

- Current temperatures and threshold levels for the far-end of the adapter card, the center of adapter card (or near the processor), microprocessor area and near the microprocessors themselves.
- Status of system fans and blowers, including % speed of maximum.
- Power supply voltages (for +5V, -5V, +3V, +12V, -12V)
- System state (including O/S restart initiated, O/S restart complete, POST started, POST stopped (error detected), and system powered off/state unknown).
- System power status (on or off).
- Power on hours (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).

For some systems (such as the Netfinity 5500), various thresholds are shown for temperature and voltage values:

- Warning: the first temperature/voltage threshold. This corresponds to the non-critical temperature event as defined in 3.2.4.4, “Non-Critical Alerts” on page 81.
- Warning Reset: the warning threshold was reached but the temperature or voltage decreased back to a “normal” operating range.
- Soft Shutdown: the second threshold where the operating system will be shutdown. This corresponds to the critical temperature event as defined in 3.2.4.3, “Critical Alerts” on page 80.
- Hard Shutdown: the server is immediately powered down.

3.2.7 System Power Control

You can use the System Power Control window to power-on or power-off a remote server.

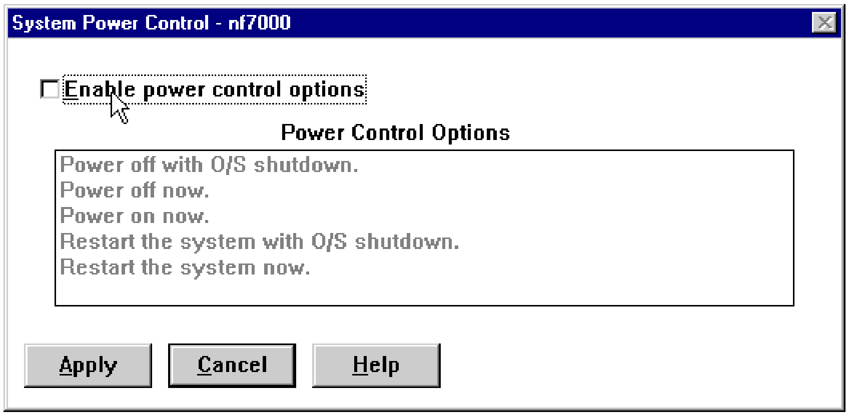

System Power Control - nf7000
□ Enable power control options
Power Control Options
Power off with O/S shutdown.
Power off now.
Power on now.
Restart the system with O/S shutdown.
Restart the system now.
Apply
Cancel
Help

Figure 59. Service Processor System Power Control

Check the **Enable power control option** box and select one option. Click on **Apply** to let your choice take effect.

Note: The option **Power on now** is only available via serial link (modem or null modem connection).

3.2.8 Remote POST Console

The Remote POST Console function of the Advanced System Management service enables you to remotely monitor, record, and replay all textual output generated on a remote system during POST.

Not All Servers

The Remote POST Console function is currently only available on the following systems:

- PC Server 325
- PC Server 330
- Netfinity 5500
- Netfinity 7000

To monitor and record the POST data on a remote system, do the following:

1. Connect to Netfinity Manager on the remote system via a modem or null modem (only serial connections are supported by Remote POST Console)
2. Connect to the remote system's Advanced System Management service through Remote System Manager.
3. Open **Remote POST Console** and leave it open while returning to the Advanced System Management main window
4. Restart the remote system using **System Power Control**

All POST data will be displayed in and recorded by the Remote POST window as the remote system completes POST. The console display will end once the operating system starts loading. This allows you to control other POST functions such as ServeRAID (Ctrl I) and Adaptec (Ctrl A) configurations.

While you are monitoring POST on a remote system all local keystrokes are relayed automatically to the remote system. All other functions of the Service Processor Manager will be disabled as long as the Remote POST console window is opened.

To review this data after POST completes, disconnect from the remote system and use the replay functions from the **Replay** pull down menu in the Remote POST Console window. You can stop and restart the replay as well as adjust the speed of the replay.

Note: Remote POST functions are available only when connecting to a remote system using a serial connection (that is, either a modem or a null modem connection). Remote POST functions are not available when connected to a remote system using a network connection.

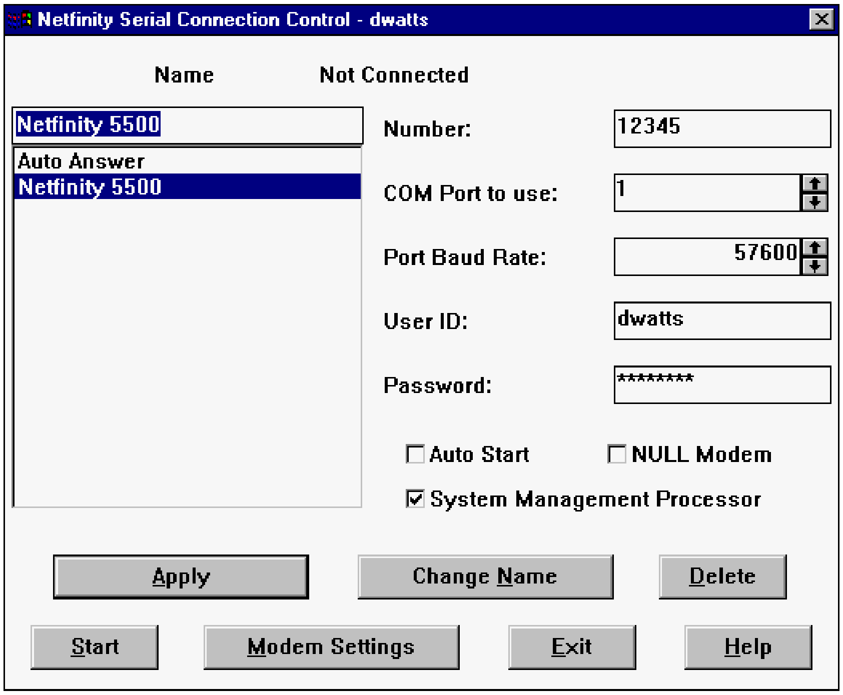
3.3 Dialing Into the Management Processor

As part of your server management strategy, you may need to dial into a server's Advanced Systems Management Adapter or Advanced Remote Management processor while the server is either fully functioning, in a critical state, or powered off. This section describes how to do this.

To dial into a remote server via its Management Processor, from the local machine you need to have Netfinity Manager installed with the **Advanced System Management Support** option installed. You do not have to have an Advanced Systems Management Adapter in the local machine.

The steps are:

1. On your local workstation, configure a dial-out entry using Netfinity Manager's **Serial Control** as per Figure 60



Netfinity 5500

Auto Answer
Netfinity 5500

Number: 12345

COM Port to use: 1

Port Baud Rate: 57600

User ID: dwatts

Password: ********

□ Auto Start □ NULL Modem

☑ System Management Processor

Figure 60. Configuring a Dial-out Entry

If you are using Netfinity Manager Version 5.10.4 or later, you should put a tick in the **System Management Processor** checkbox. Versions prior to 5.10.4 will not have this checkbox.

2. On the server you should have the userid and password used in Step 1 as per 3.2.2, “Configuration Settings” on page 73.

3. Dial the remote server.

   If you are using Netfinity Manager Version 5.10.4 or later, skip to 4.

   If you are using an earlier version of Netfinity Manager do the following:

   a. Start the Service Processor Manager and click on **Connect** from the menu bar, as shown in Figure 61 on page 86.

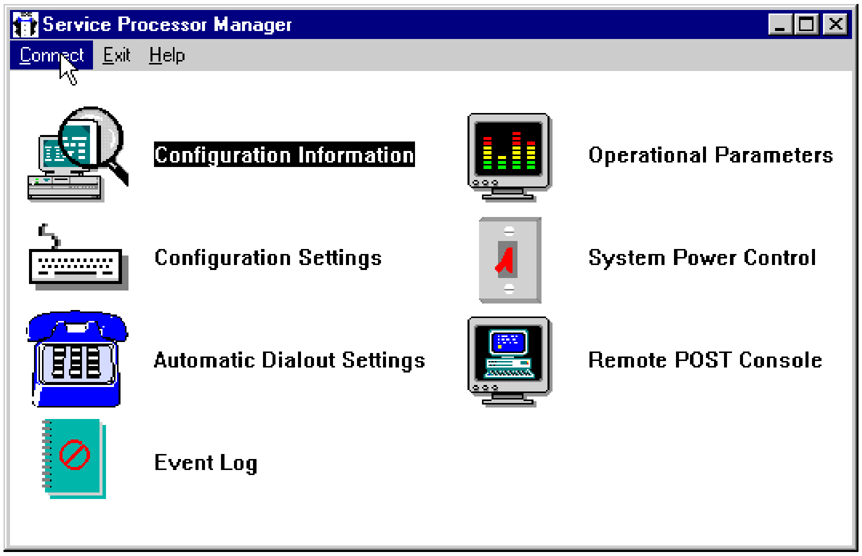
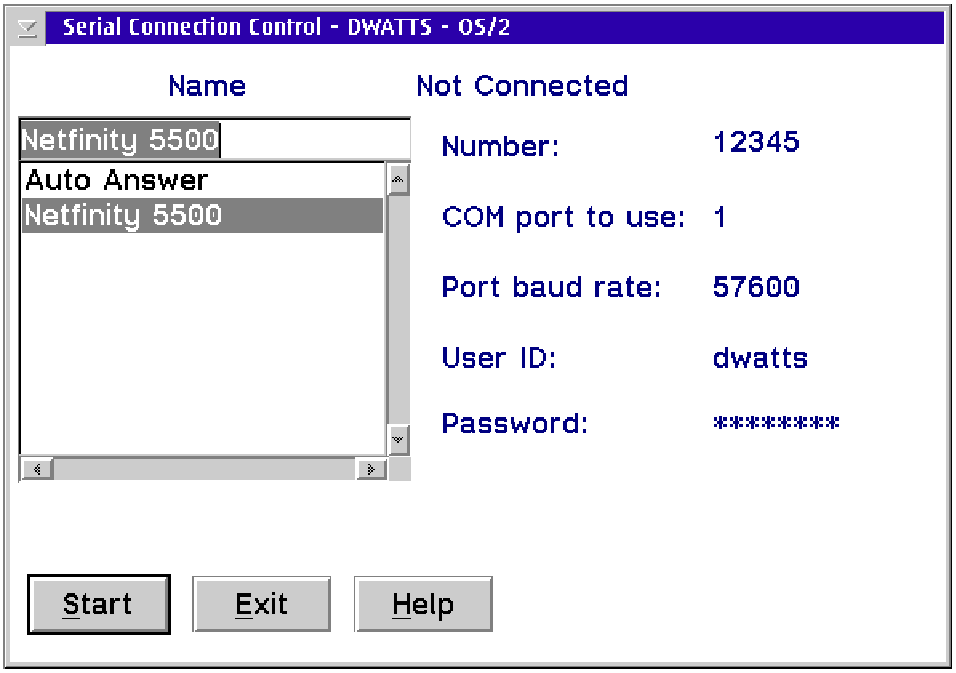


Figure 61. Service Processor Manager Window

b. Figure 62 appears.



Number: 12345

COM port to use: 1

Port baud rate: 57600

User ID: dwatts

Password: ********

Figure 62. Selecting the Dial-out Configuration. (for versions of Netfinity Manager prior to 5.10.4)

c. If you get the following error message instead, then you have not completed Step 1.

```
No serial connection remote access entries are defined.  Use the
Netfinity Serial Control service to define a remote service processor
serial connection entry.
```

d. Select the dial-out entry you defined in Netfinity Manager Serial Control for the remote server.

4. Click on the **Start** button.

Once you are connected to the remote server, you will get the message `Connected` in the Serial Control window.

5. Click on the **Exit** button to leave the dial-out window and go back to the Advanced System Management main window

All seven icons in the window will now be available and will perform operations on the remote server via the serial connection. You will see the name of the remote server as part of the window title. This is a reminder that you are now working remotely.

See 3.2.1, “Configuration Information” on page 71 onwards for details on these icons.

Chapter 4. Management Functions in Netfinity Servers

This chapter describes the management components that are included with servers from the IBM range:

1. IBM Netfinity 7000
2. IBM Netfinity 5500
3. IBM Server 330
4. IBM Server 325
5. IBM Netfinity 3500
6. IBM Netfinity 3000

4.1 IBM Netfinity 7000

The IBM Netfinity 7000 is a highly reliable enterprise server offering 4-way Pentium Pro processing power with up to 4 GB of ECC memory and 12 hot-swap hard disk bays for up to 109 GB of RAID protected storage.

The Netfinity 7000 comes standard with features such as redundant power supplies, redundant fans, ECC memory and RAID protected storage that provide the ability to overcome malfunctions. They avoid server shutdown and provide a reliable network solution.

The Netfinity 7000 has been designed to detect errors and provide alerts prior to system malfunctions. Notification of failures and recoveries of those failures is reported through a combination of LEDs, the LCD display, alerts from Netfinity Manager and the Advanced Systems Management Adapter, standard on all Netfinity 7000 systems.

4.1.1 Status Indicators

The Netfinity 7000 server information panel is on the front of the server as shown in Figure 63 on page 90 It provides information about the status of the machine.

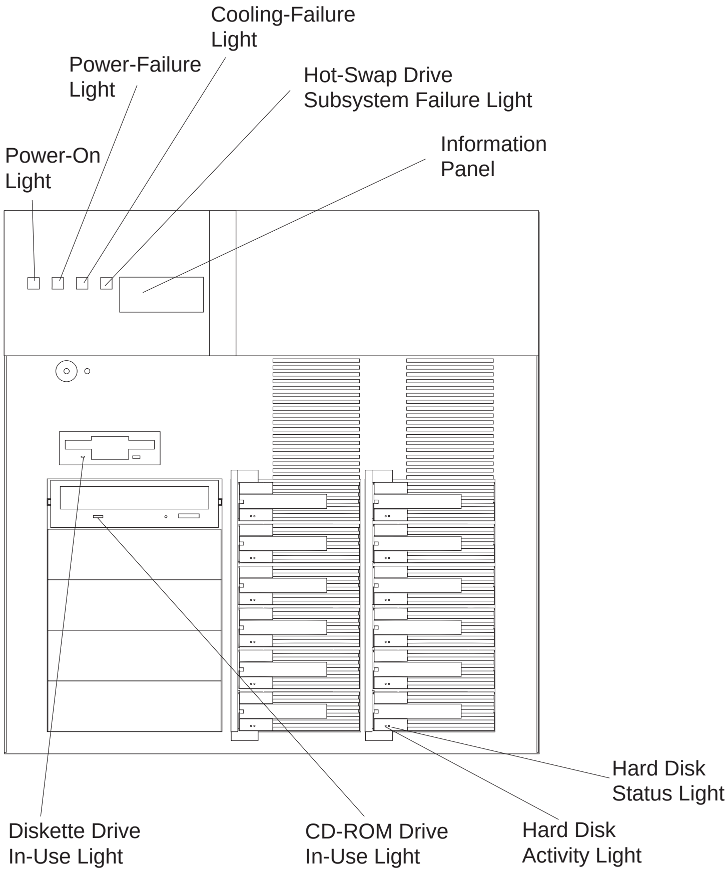


Figure 63. Netfinity 7000 Front View

The information panel displays:

- Checkpoint information on POST
- Boot-up error messages
- Server and BIOS information

The server also has a set of LEDs at the front of the machine and a set of LEDs at the rear of the machine to display the status of the following functions and devices:

4.1.1.1 Power Indicators

The Netfinity 7000 comes standard with two 400 Watt hot-swap power supplies providing power to support full configurations. The optional IBM Netfinity 400W Hot-Swap Redundant Power (#94G7150) can be added to allow the Netfinity 7000 to operate without interruption if one of the two standard power supplies fails. The replacement of the failing power unit (easily removed and re-installed) will be possible without powering down the server.

When three power supplies are installed in the system, the power load is shared across all three sources.

There are four types of LEDs indicating the status of the power to the server. These are shown in Figure 63 and Figure 64 on page 91.

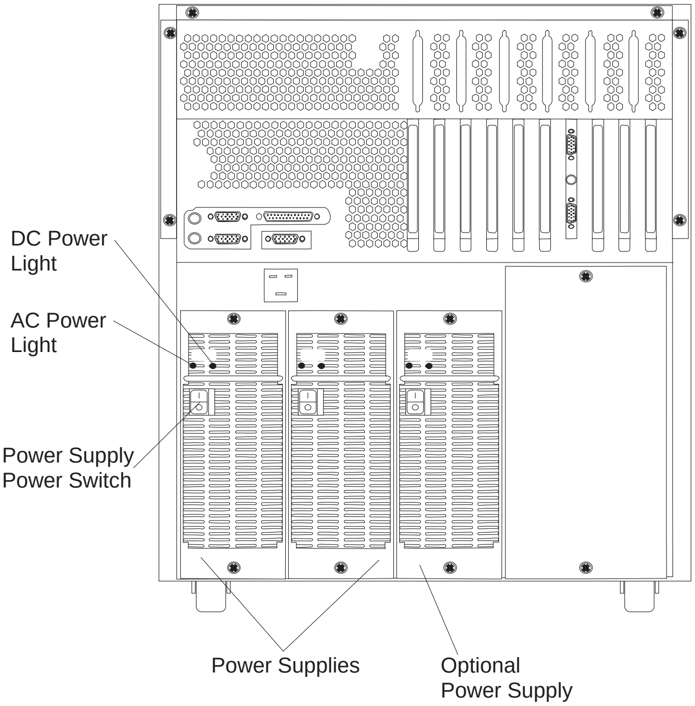


Figure 64. Netfinity 7000 Rear View

1. Green Power-On light, on the front of the server
2. Amber Power-Failure light, on the front of the server
3. Green DC Power light, on each of the two or three power supplies on the back of the server
4. Green AC Power light, on each of the two or three power supplies on the back of the server

Table 11 shows the state of the server's power depending on these LEDs:

Table 11 (Page 1 of 2). Power Indicators and What They Mean

Power On	**Power Failure**	**AC Power**	**DC Power**	**State**
on	off	all on	all on	The server is powered on and no power subsystem problem is detected.
off	off	all off	all off	The server is not connected to a working electrical outlet or all power supplies are in the Off position.
off	off	all on	all off	AC power to the server is functioning properly. The Power On/Off button on the front of the server is in the Off position.
off	blinking		all off	The server was shut off before a power subsystem problem was corrected. After the problem is corrected, you must restart the server before the status lights will be reset.
on	blinking	all on	all on	A non-critical power subsystem error has occurred. The Advanced Systems Management Adapter error log should contain more information.

Table 11 (Page 2 of 2). Power Indicators and What They Mean

Power On	Power Failure	AC Power	DC Power	State
on	blinking	on	1+ on	The power supply with the DC Power Good light off either has the Power switch in the Off position or has failed.
Note: To ensure that the power supply is operational, both lights on the power supply must be on. Make sure that the Power switch on each installed power supply is in the On position.				

4.1.1.2 Cooling Fan Indicators

Three hot-swap cooling fans provide cooling redundancy which means that the server can continue to operate even if a fan fails. Nevertheless, the failing hot-plug fan should be replaced as soon as possible to regain the cooling efficiency and maximum reliability.

The Cooling-Failure light on the front of the server as shown in Figure 63 on page 90 indicates the health of the cooling fans in the server.

The Cooling-Failure light on the front of the server blinks slowly if one of the fans fails or is predicted to fail (for example, starts to slow down).

If the ambient temperature exceeds the warning threshold, Cooling-Failure light will blink rapidly and an error will be logged in the Advanced Systems Management Adapter error log.

If more than one fan fails or if the ambient temperature exceeds the operating system shutdown threshold, the Cooling-Failure light will continue to blink rapidly, the operating system will shutdown and the server will be powered off.

If the ambient temperature exceeds the server shutdown threshold, the Cooling-Failure light will continue to blink rapidly and the server will power off immediately.

4.1.1.3 Hot-Swap Drive Indicators

To show the status of the hot-swap drive subsystem, the The Netfinity 7000 has a LED on the front of the server showing the overall status of the subsystem as well as individual LEDs on each of the hot-swap trays.

The Hot-Swap Drive Subsystem Failure light on the front of the server blinks if the server detects a hot-swap drive failure or if one of the SCSI backplanes gets too hot.

Each of the 12 hot-swap trays has two LEDs as shown in Figure 63 on page 90:

1. Green Activity Light: When it is lit, the drive is in use.
2. Amber Status Light:
   - Continuously on — drive has failed
   - Slow blink — drive is being rebuilt
   - Fast blink — controller is identifying the drive

To aid in the detection of heat-related problems in the drive subsystem, the Netfinity 7000 has four hot-swap drive subsystem temperature thresholds:

1. If one of the SCSI backplanes starts to overheat and the temperature of the backplane reaches the first threshold, the speed of the power supply fans is automatically increased.
2. If the temperature continues to increase and reaches the second threshold, Hot-Swap Drive Subsystem Failure light will blink slowly and an alert will be sent to Netfinity Manager.
3. If the temperature of the SCSI backplane reaches the third threshold, the Hot-Swap Drive Subsystem Failure light will start to blink fast and an operating system shutdown will occur.
4. Finally, if the temperature of the SCSI backplane reaches the fourth threshold, the server will power off immediately.

4.1.2 Advanced Systems Management Adapter

The Netfinity 7000 is shipped with an Advanced Systems Management Adapter installed. This adapter, in conjunction with Netfinity Manager, allows you to manage the functions of the server remotely through a modem. It also provides system monitoring, event recording, and dial-out alert capability.

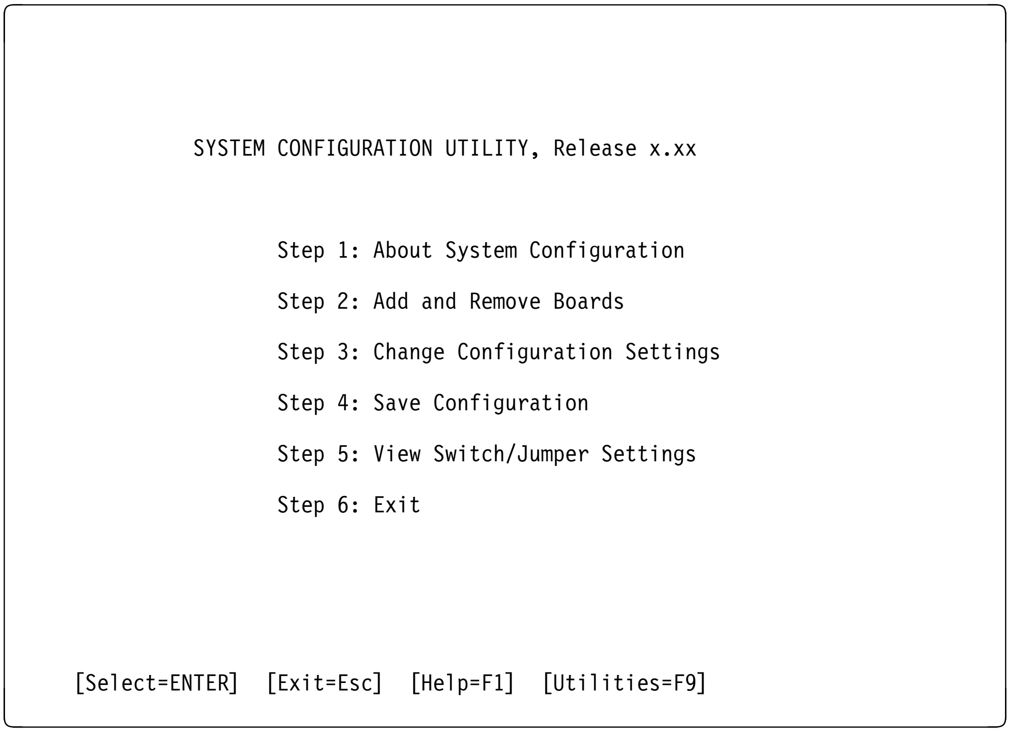
The Advanced Systems Management Adapter comes completely installed and configured. You should only change the default parameters if conflicts arise with other adapters you install.

Note: If you decide to install a replacement Advanced Systems Management Adapter ensure it is a Pass 5 card (as described in Page 63). Pass 4 adapters will not work in the Netfinity 7000.

The following resources are assigned by default.

- IRQ 5
- I/O Address 200

You can check the setting by running the System Configuration Utility (SCU). To start the SCU insert the Netfinity 7000 CD-ROM (or diskette if you download a later version) and reboot the server. You will see a menu with several choices.



```
              SYSTEM CONFIGURATION UTILITY, Release x.xx


                     Step 1: About System Configuration

                     Step 2: Add and Remove Boards

                     Step 3: Change Configuration Settings

                     Step 4: Save Configuration

                     Step 5: View Switch/Jumper Settings

                     Step 6: Exit




     [Select=ENTER]  [Exit=Esc]  [Help=F1]  [Utilities=F9]
```

Figure 65. SCU Menu

Select **Change Configuration Settings** and press Enter. The program will load several configuration files. When you are prompted for the password press the Esc key (no password set). You will see all PCI and ISA/EISA cards listed. Move the highlight bar to the Advanced Systems Management Adapter and press Enter. The next window shows the following:

```
*  Advanced System Management Adapter.
*  ISA Resources
```

Press F6 to display the resources used by the Advanced Systems Management Adapter. You will not be able to change the resources here. If you need to configure these resources, see Chapter 3, “Advanced Systems Management Adapter” on page 63.

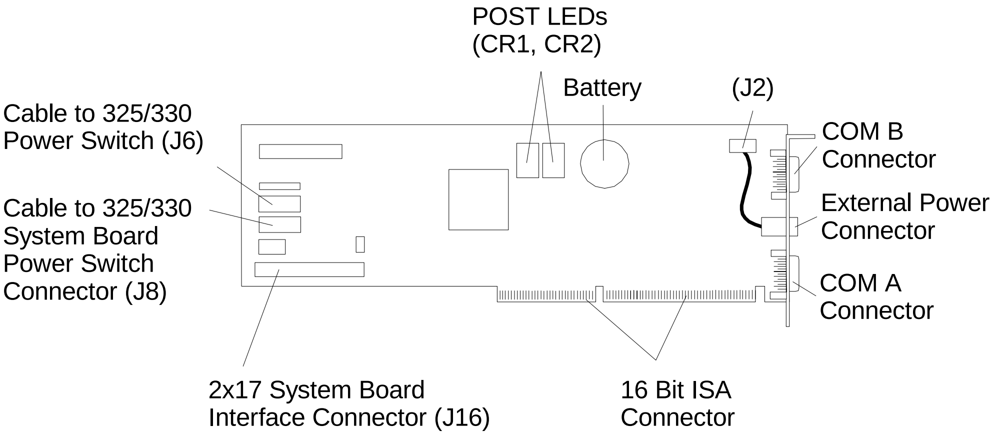

POST LEDs
(CR1, CR2)
Battery
(J2)
Cable to 325/330 Power Switch (J6)
COM B Connector
External Power Connector
Cable to 325/330 System Board Power Switch Connector (J8)
COM A Connector
2x17 System Board Interface Connector (J16)
16 Bit ISA Connector

Figure 66. Advanced Systems Management Adapter

The Advanced Systems Management Adapter is installed in one of the ISA/EISA slots and connected to the planar board via the 34-to-24 pin cable.

4.2 IBM Netfinity 5500

The Netfinity 5500 is IBM's new mid-range server that provides significant levels of performance, fault-tolerance and integrated management capability. It is available in a tower or rack chassis.

Up to two 350 MHz or 400 MHz Pentium II processors with 100 MHz operations to memory are supported. 128 MB of ECC RAM is standard, with up to 1 GB supported. The system has an integrated two-channel Ultra SCSI ServeRAID II RAID controller with six internal hot-swap bays. The tower model also includes the NetBAY3 which lets you install options such as the Netfinity EXP10 internally, to provide an additional 10 hot-swap storage bays.

For fault tolerance and recovery, the Netfinity 5500 has the following features:

- Single CPU failure recovery with two CPUs installed
- Ability to bypass failed memory modules on startup
- ECC memory and L2 cache
- Two Ultra SCSI RAID channels
- Six internal hot-swap drive bays
- Four hot-swap PCI card slots
- Predictive failure analysis (PFA) on processors, memory and disks power supplies and fans
- Hot-swap fixed-speed fans and variable-speed blowers
- Optional Hot-swap redundant power supply
- “Light-Path” Diagnostics as described in 4.2.1.3, “Locating Failures” on page 101
- Backup copy of the BIOS to enable recovery of a corrupted BIOS
- Easy access to system components

Central to management of the Netfinity 5500 is the new Netfinity Advanced Remote Management processor. This integrated subsystem is based on a PowerPC RISC processor and communicates to all other subsystems through five separate I²C busses. The Advanced Remote Management is described in 4.2.2, “Advanced Remote Management Processor” on page 101.

4.2.1 Indicators

The front of the server has a variety of indicators and controls as shown in Figure 68 on page 98.

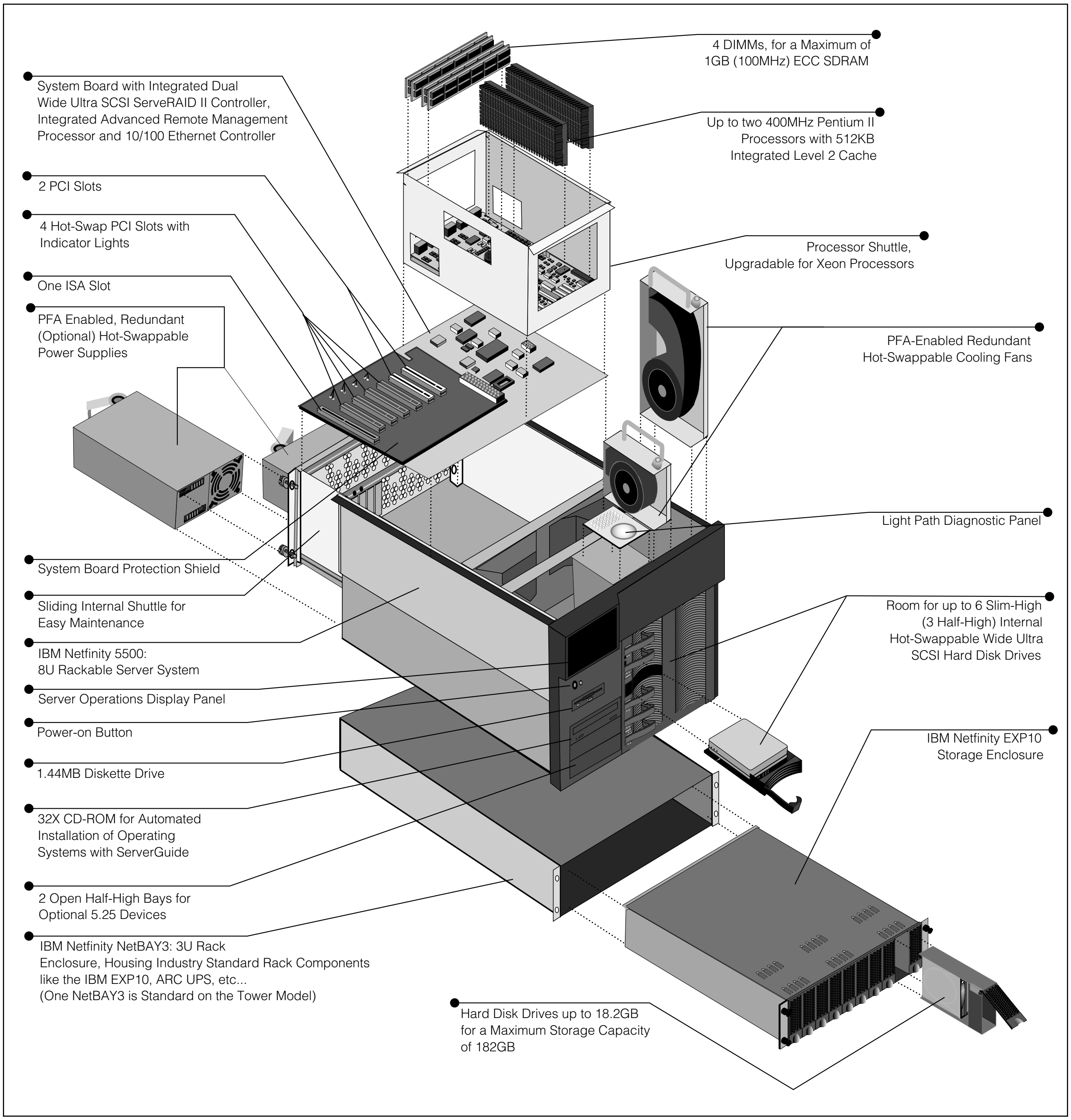

4 DIMMs, for a Maximum of
1GB (100MHz) ECC SDRAM
System Board with Integrated Dual
Wide Ultra SCSI ServeRAID II Controller,
Integrated Advanced Remote Management
Processor and 10/100 Ethernet Controller
Up to two 400MHz Pentium II
Processors with 512KB
Integrated Level 2 Cache
2 PCI Slots
4 Hot-Swap PCI Slots with
Indicator Lights
Processor Shuttle,
Upgradable for Xeon Processors
One ISA Slot
PFA Enabled, Redundant
(Optional) Hot-Swappable
Power Supplies
PFA-Enabled Redundant
Hot-Swappable Cooling Fans
Light Path Diagnostic Panel
System Board Protection Shield
Sliding Internal Shuttle for
Easy Maintenance
Room for up to 6 Slim-High
(3 Half-High) Internal
Hot-Swappable Wide Ultra
SCSI Hard Disk Drives
IBM Netfinity 5500:
8U Rackable Server System
Server Operations Display Panel
Power-on Button
IBM Netfinity EXP10
Storage Enclosure
1.44MB Diskette Drive
32X CD-ROM for Automated
Installation of Operating
Systems with ServerGuide
2 Open Half-High Bays for
Optional 5.25 Devices
IBM Netfinity NetBAY3: 3U Rack
Enclosure, Housing Industry Standard Rack Components
like the IBM EXP10, ARC UPS, etc...
(One NetBAY3 is Standard on the Tower Model)
Hard Disk Drives up to 18.2GB
for a Maximum Storage Capacity
of 182GB

Figure 67. The IBM Netfinity 5500

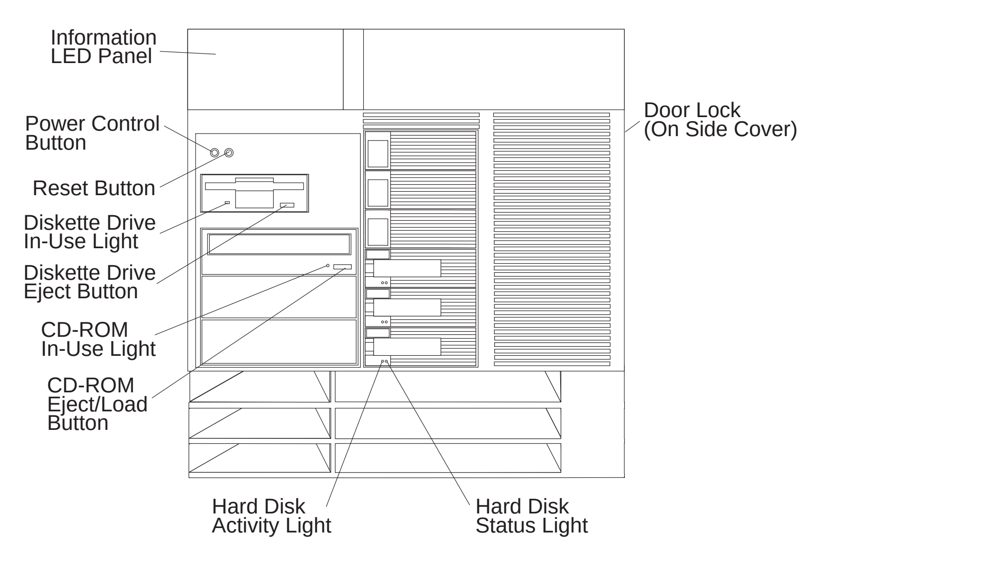


Figure 68. Netfinity 5500 Front Panel

4.2.1.1 Information LED Panel

The Informational LED panel at the top-left corner of the front panel provides information about the current status of server and is also the first place to look when hardware faults occur. The various components of the panel are shown in Figure 69.

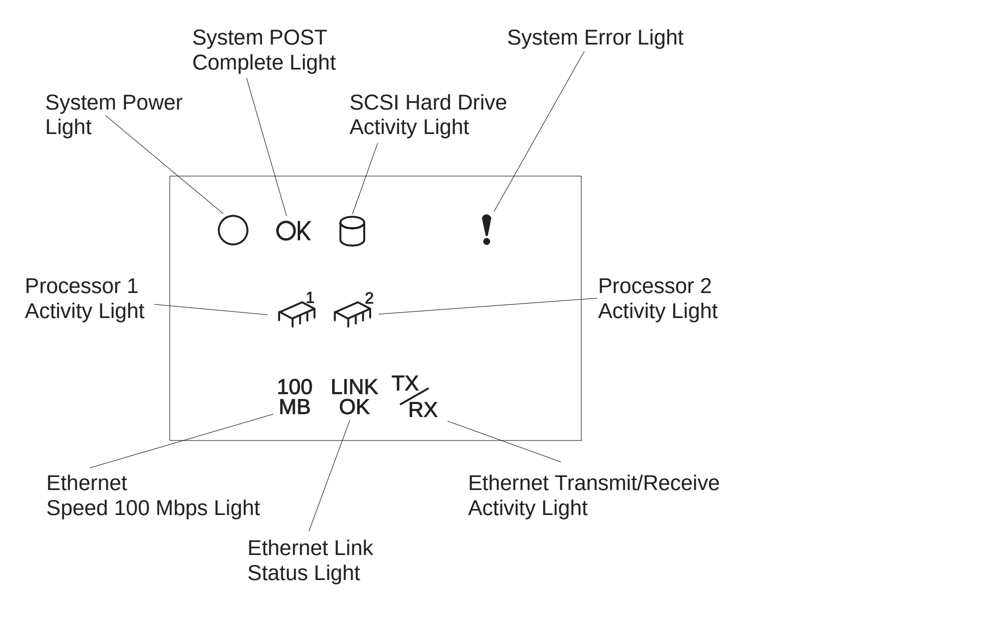

System POST Complete Light
System Error Light
System Power Light
SCSI Hard Drive Activity Light
OK
!
Processor 1 Activity Light
1
2
Processor 2 Activity Light
100 MB
LINK OK
TX/RX
Ethernet Speed 100 Mbps Light
Ethernet Transmit/Receive Activity Light
Ethernet Link Status Light

Figure 69. Netfinity 5500 Information LED Panel

Three of the LEDs warrant special mention:

- **System Power Light**

  When this green lamp is on, the system is powered up. When the light flashes, AC power is present, but the server is off. When the light is off, either there is no power to the server or a failure has occured in the power supply, wall socked or the light itself.

- **System POST Complete Light**

  This green light is lit when the power-on self-test completes without any errors.

- **System Error Light**

  When this amber LED lights up, a system error has occured. Remove the top cover of the server and examine the diagnostics LED panel to determine the cause of the error. See 4.2.1.3, “Locating Failures” on page 101.

4.2.1.2 Indicators on the Planar

The Netfinity 5500 has both a system board and a processor board. Both of these have indicators on them showing status of various components in the server.

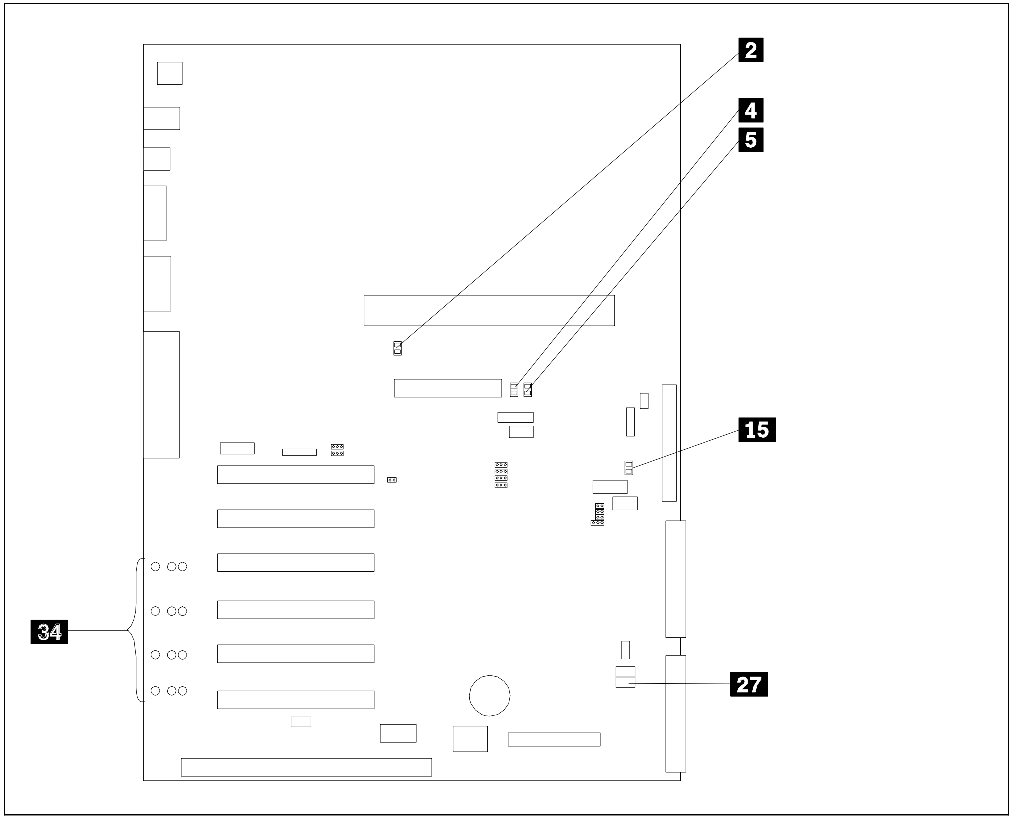


Figure 70. Netfinity 5500 System Board

The following LEDs are on the system board (Figure 70):

2	Advanced Remote Management processor error
4	ServeRAID channel 1 error
5	ServeRAID channel 2 error
15	RAID subsystem error
34	hot-plug PCI slot LEDs: • Power LED on each slot (visable on the inside) • Attendtion LED on each slot (2 LEDs each, one visible from the outside)

Also of note is 27 which is the jumper to switch between primary and backup versions of the system BIOS. This is described in more detail in 6.8, “Example 8: Remote Update of Netfinity 5500 BIOS” on page 177.

Note: Other components on the system board are described in “System Board Component Locations” in Chapter 10 of the *Netfinity 5500 User's Handbook*.

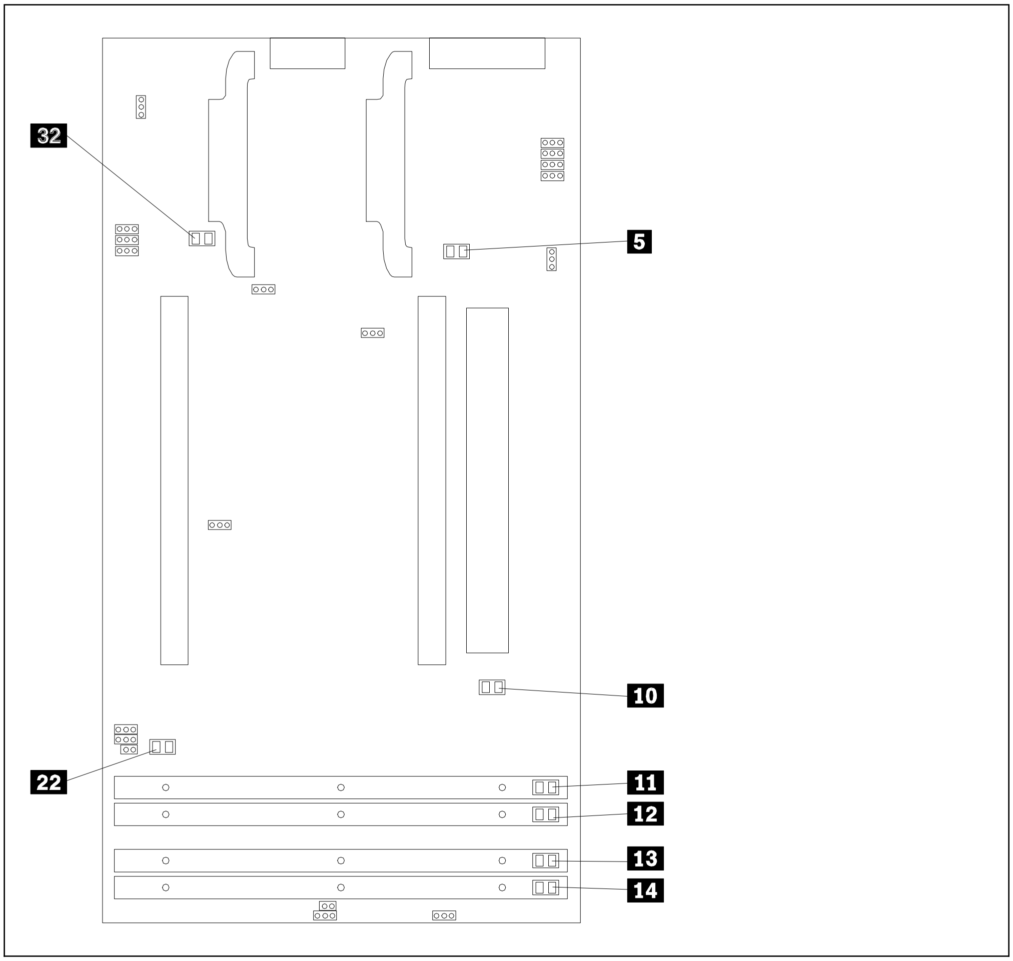


Figure 71. Netfinity 5500 Processor Board

The processor board connects to the system board and accomodates the two Slot 1 CPUs, memory and VRMs. The following LEDs are on the processor board (Figure 71):

5	VRM error on CPU 1
10	CPU 1 error
11	DIMM 1 error
12	DIMM 2 error
13	DIMM 3 error
14	DIMM 4 error
22	CPU 2 error
32	VRM error on CPU 2

Note: Other components on the processor board are described in “Processor Board Component Locations” in Chapter 10 of the *Netfinity 5500 User's Handbook*.

4.2.1.3 Locating Failures

The Netfinity 5500 uses a “light-path” to help you narrow down the specific cause of the failure. In short, the path is:

1. System Error Light on the front panel
2. Diagnostics LED panel inside the server
3. Individual LEDs on various components in the server

The diagnostics LED panel, located inside the top of the server, shows you which subsystem has developed a fault. The panel is shown in Figure 72.

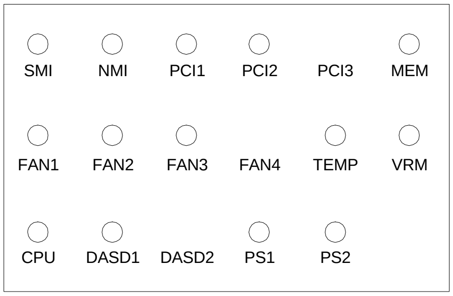


Figure 72. Netfinity 5500 Diagnostics LED Panel

The LEDs on this panel are:

SMI System Management failure
NMI Non-maskable Interrupt failure
PCI1 Failure on the primary PCI bus (bus 0)
PCI2 Failure on the secondary PCI bus (bus 1)
MEM Memory failure. Check LEDs near each DIMM on the procesor board. (Figure 71 on page 100)
FAN1 Fan 1 has failed or developed a fault
FAN2 Fan 2 has failed or developed a fault
FAN3 Fan 3 has failed or developed a fault
TEMP System temperature has exceeded the hard coded threshold
VRM A Voltage Regulator Module has failed. Check LEDs near each VRM on the processor board. (Figure 71 on page 100)
CPU A CPU has failed. Check the LEDs near each CPU on the processor board. (Figure 71 on page 100)
DASD1 A drive connected to the internal hot-swap backplane has failed. Check the individual drive LEDs as per Figure 68 on page 98.
PS1 The primary power supply has failed
PS2 The optional, secondary power supply has failed

Note: For more information about the LEDs and recommended actions, see “Identifying Problems Using Status LEDs” in Chapter 8 of the *Netfinity 5500 User's Handbook*.

4.2.2 Advanced Remote Management Processor

The integrated service processor on the Netfinity 5500, known as the Advanced Remote Management processor, offers strong local and remote management of the server. It has the following specifications:

- Powered by a 403GA Power PC 32-bit RISC microprocessor
- Self-contained SRAM, non-volatile RAM, real-time clock, UART serial port processor and I²C controller

- Interface to LM78 environmental monitoring processor
- Five I²C busses to hot-swap backplane, power backplane, power supplies, processor board, system board and memory DIMMs
- ISA interface with selectable IRQ (hard coded I/O port)
- Upgradeable through flash update
- COM port B, shared with operating system after boot
- COM port C, dedicated managment COM port

The Advanced Remote Management processor offers superior capabilities of that of the Advanced Systems Management Adapter:

- Additional dial-out alerts: VRM failure, PFA alert, non-critical voltage alert
- Remote diagnotics using ROM-based diagnostic utilities
- Remote POST Console to view and manage POST functions remotely
- dial-in functions
- monitoring of temperature, voltage and fan speed
- dial-out functions when alerts occur

4.2.2.1 Installation

To use the features of the Advanced Remote Management processor, you need to use Netfinity Manager 5.10.4 or later. Before installing Netfinity Manager, you must first install the “IBM Netfinity 5500 Device Driver for Advanced Remote Manager.” The driver diskette is available on ServerGuide 4.0.4 or later.

Note: If you installed Netfinity Manager before installing the driver, you must reinstall Netfinity Manager before you can use the features of the Advanced Remote Management processor.

When you install Netfinity Manager ensure you have **Advanced System Management Support** selected as one of the to-be-installed options. You also need to select this option when installing Netfinity Manager on other administration workstations on your network.

4.2.2.2 Management Functions

The Netfinity Manager interface of the Netfinity 5500 Advanced Remote Management processor, shown in Figure 73 on page 103 is similar to that of the Advanced Systems Management Adapter but with extra functions as explained in 3.2, “Adapter Configuration in Netfinity Manager” on page 69. The following is a summary of the enhancements:

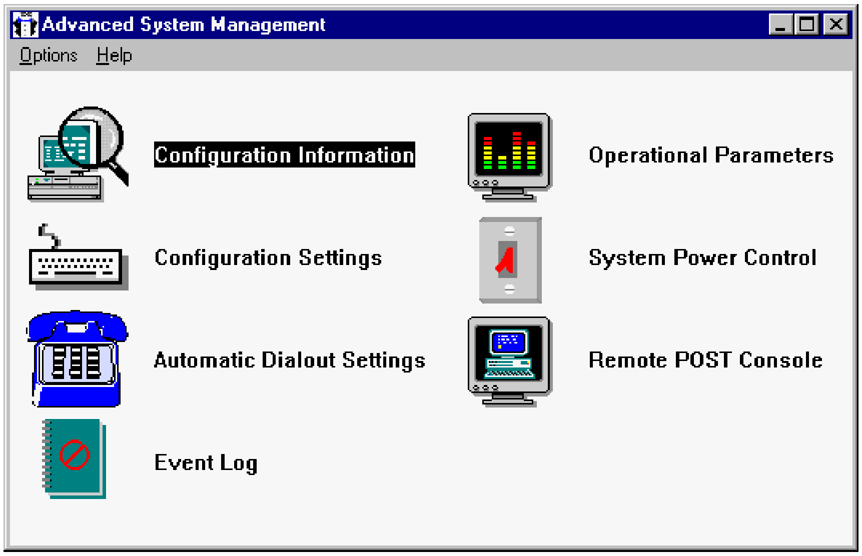


Figure 73. Advanced System Management Window

- **Remote BIOS Flash**

  Through the Advanced System Management service in Netfinity Manager, you can update the system BIOS and the firmware of the Advanced Remote Management processor. From the Advanced System Management service, click on **Options** → **Update Microcode...** and select either **System Management Processor** or **System**.

- **Configuration Information**

  The Advanced Remote Management provides Vital Product Data (VPD) information about the following components as shown in Figure 74:

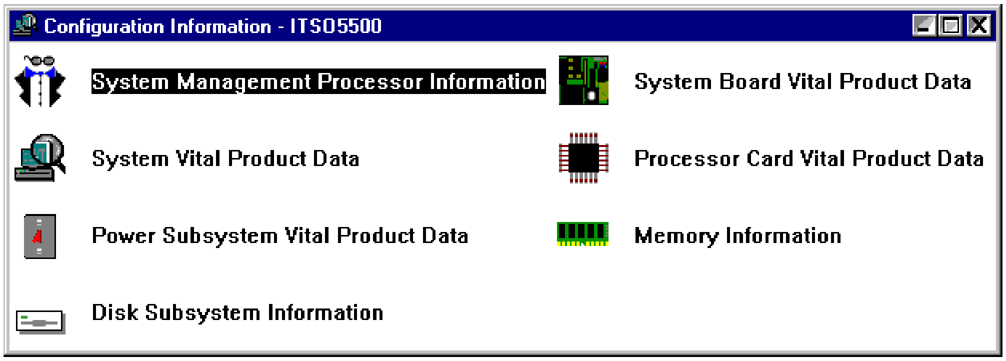

Configuration Information - ITSO5500
System Management Processor Information
System Board Vital Product Data
System Vital Product Data
Processor Card Vital Product Data
Power Subsystem Vital Product Data
Memory Information
Disk Subsystem Information

Figure 74. Netfinity 5500 Advanced Remote Management Configuration Information

  - Advanced Remote Management processor microcode and driver levels
  - System (BIOS level, model, serial number, etc)
  - Power supplies and power backplane
  - Internal hot-swap backplane
  - System board
  - Processor board
  - Each memory DIMM (size, speed, serial number, etc)

  See 3.2.1, “Configuration Information” on page 71 for details.

- **Configuration Settings**

The Advanced Remote Management processor supports up to 12 separate user profiles whereas the Advanced Systems Management Adapter supported only six.

See 3.2.2, “Configuration Settings” on page 73 for details.

- **Automatic Dialout Settings**

  The following events have been added which will, when enabled, cause the Advanced Remote Management processor to dial-out and send an alert:

  – Critical VRM failure
  – PFA alert
  – Non-critical voltage alert

  See 3.2.4, “Automatic Dialout Settings” on page 79 for details.

- **Operational Paremeters**

  The Netfinity 5500 provides much more information about temperature, voltage and fan status that in the Advanced Systems Management Adapter. For temperature monitoring, the Advanced Remote Management processor provides four threshold settings rather than one “hard shutdown” threshold:

  – Warning Reset
  – Warning
  – Soft Shutdown
  – Hard Shutdown

  For voltage monitoring, the Advanced Remote Management processor also supplies these same four thresholds rather than the one “hard shutdown” threshold. A total of five voltage levels are monitored instead of the previous three.

  The three fans in the Netfinity 5500 are also reported using the Advanced Remote Management processor. The percentage of maximum speed is shown for each. The total number of system power-ups is also recorded as is the current status of the server.

  See 3.2.6, “Operational Parameters” on page 82 for details.

- **Remote POST Console**

  Like the Server 325, 330 and Netfinity 7000 with the use of an Advanced Systems Management Adapter, the Netfinity 5500 also provides the ability to monitor and replay the POST messages using the integrated Advanced Remote Management processor.

  See 3.2.8, “Remote POST Console” on page 84 for details.

4.3 PC Server 325 and 330

The IBM PC Server 325 is a powerful tower or rack-drawer system with one or two Pentium II processors. All models contain integrated Ultra SCSI controller, 100/10 Mbps full-duplex PCI Ethernet controller, I²C bus, and ECC EDO DIMM memory.

The IBM PC Server 330 tower uses one or two Pentium Pro or Pentium II processors. Like the Server 325, the Server 330 contains an 100/10 Mbps full-duplex PCI Ethernet controller, I²C bus, and ECC EDO DIMM memory. The Server 330 has an integrated single-channel ServeRAID Ultra SCSI RAID controller and hot-swap drive bays for added performance and protection.

On both the Server 325 and Server 330, LED lights located on the front panel (as shown in Figure 75 for the Server 330) provide visual information about SCSI, Ethernet, power, POST, primary and secondary processor, and security activities. The I²C management bus provides Vital Product Data (VPD) and a connector for an optional Advanced Systems Management Adapter for monitoring temperature and other server functions.

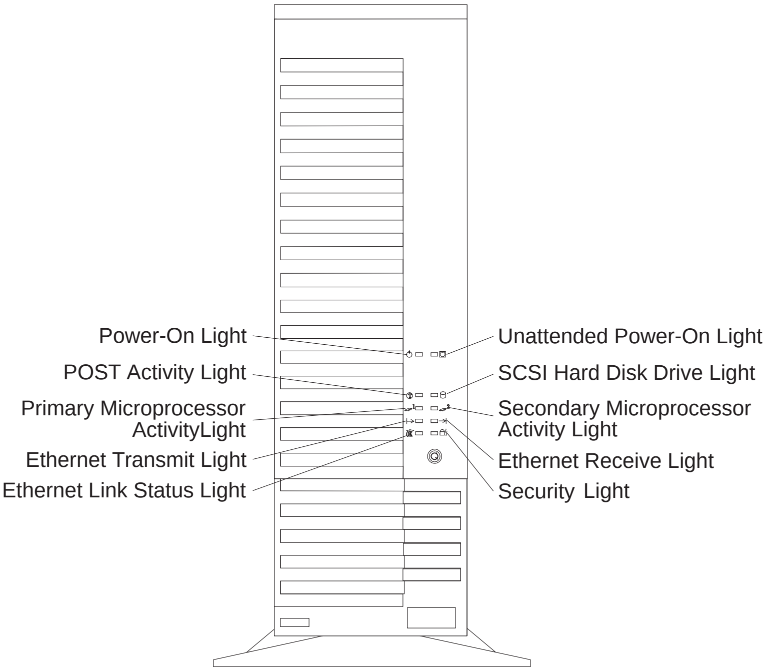

Power-On Light
POST Activity Light
Primary Microprocessor ActivityLight
Ethernet Transmit Light
Ethernet Link Status Light
Unattended Power-On Light
SCSI Hard Disk Drive Light
Secondary Microprocessor Activity Light
Ethernet Receive Light
Security Light

Figure 75. Front Panel of the Server 330

There are eight LEDs located on the front panel. Most of them are self-explanatory but two require further clarification: (see Figure 75)

- **POST Activity Light**

  This amber LED comes on while the POST and the configuration utility programs are running.

- **Security Error Light**

  When tamper-detection software is installed and enabled, this amber LED shows that a security hardware or software alert occurred.

Server 330 SCSI Status

For this server model, the SCSI LED light displays the status of all the devices attached to Wide Ultra SCSI controller but not the ones attached to ServeRAID RAID controller.

The Server 330 provides additional disk status for each hot-swap disk installed into hot-swap tray type III through two LEDs located on the front of the tray, as shown in Figure 76. See Table 12 for more information about these LED lights.

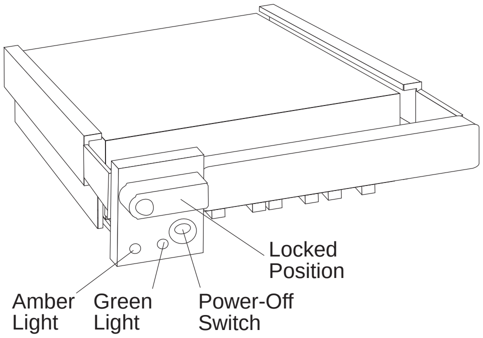


Figure 76. Hot-swap Drive Tray III

Table 12. Disk Status Shown by LED Lights of the Tray III

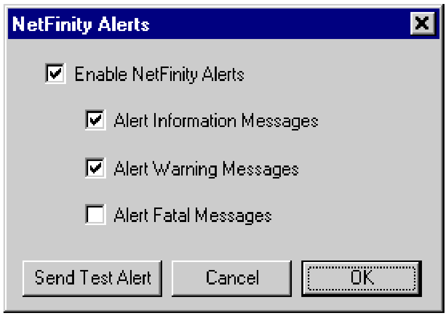
Amber LED (activity)	Green LED (status)	Description
Off	On	The drive tray is powered on but the drive is not in use.
Off	Blinking	The disk drive is not active and can be safely removed. (the On/Off button has just been pressed)
On or Blinking	On	The disk drive is in use.
Off	Off	The drive is defective, or no power is being supplied to the drive. You can safely remove the drive.

For more information about the LEDs on the front panel of both Server 325 and 330, and hot-swap drives with tray III, see *PC Server 325 User's Handbook* or *PC Server 330 User's Handbook*.

4.3.1.1 ServeRAID RAID Controller

A ServeRAID controller is implemented on the motherboard of the latest models of the Server 330 (8640-PM0, PT0 and PB0). Netfinity Manager provides the RAID Manager service to manage and monitor disks attached to the controller.

The ServeRAID Administration and Monitor Utility can also be configured to send alerts to Netfinity Manager's Alert Manager. From the administration utility, click on **Options** → **Alert Options** → **Netfinity**. Figure 77 on page 107 appears.



☑ Enable NetFinity Alerts

☑ Alert Information Messages

☑ Alert Warning Messages

□ Alert Fatal Messages

Figure 77. ServeRAID Device Management Window

Other server functions and environmental conditions, such as temperature, can be monitored by using the Advanced Systems Management Adapter. See the following sources for details:

- Advanced Systems Management Adapter: Chapter 3, “Advanced Systems Management Adapter” on page 63.
- Netfinity Manager features: Chapter 2, “Netfinity Manager” on page 3.
- Server features: Server 325 or Server 330 *User's Handbook*.

4.3.1.2 Diagnostics with Netfinity Manager

As well as providing the standard management functions as described in Chapter 2, “Netfinity Manager” on page 3, Netfinity Manager offers additional options on some models of the Server 325 and 330 in the form of offline diagnostics of the key hardware subsystems.

Does My Server Support This Feature?

This function is available on servers running OS/2 or NetWare. Windows NT is not supported.

Only the newer models of the Server 325 and 330 with the I^{2}C bus are supported by this feature. 8639-xTx, 8639-xBx, 8640-Pxx support this feature, but 8639-xJx, 8639-xSx and 8640-Exx do not support the diagnostics function.

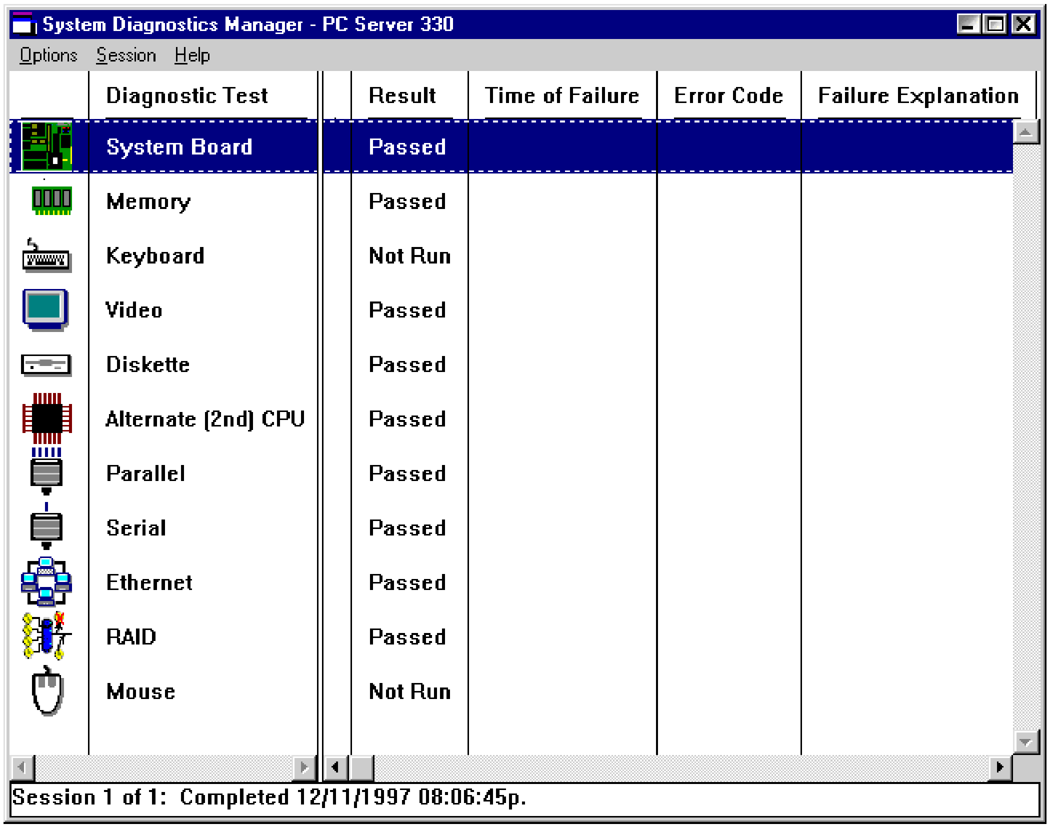
If your server supports this feature then the following icon will appear in the Netfinity Manager main window when running it locally or when connected to the server remotely from another Netfinity Manager machine.

If you expect to see this service on your Server 325 or 330 but it does not appear, make sure all of the following are true:

1. You are running OS/2 or NetWare on your server. Windows NT does not allow this sort of hardware access so the function is not available.
2. You are not running Netfinity Manager locally at the server. This service is *remote only* — if you are at the server, you can invoke ROM diagnostics during POST and do not need Netfinity Manager.

3. You have at least the 5.00.2 level of Netfinity Manager at both the server and your workstation.
4. The model number information is correct at the server. If the model number VPD information is missing, Netfinity Manager will not install the service since it is applicable only to certain models. If you have to change the model number using the system's configuration utilities, make sure that you reinstall Netfinity after the model number is corrected so that the missing pieces will be installed.

Open the function produces the following window (see Figure 78) showing the results of the last run diagnostic on the machine.



Diagnostic Test	Result	Time of Failure	Error Code	Failure Explanation
System Board	Passed			
Memory	Passed			
Keyboard	Not Run			
Video	Passed			
Diskette	Passed			
Alternate (2nd) CPU	Passed			
Parallel	Passed			
Serial	Passed			
Ethernet	Passed			
RAID	Passed			
Mouse	Not Run			

Session 1 of 1: Completed 12/11/1997 08:06:45p.

Figure 78. System Diagnostics Manager

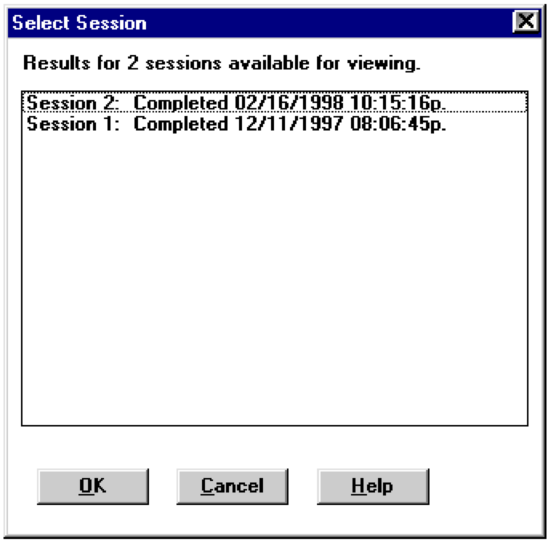
To run a new set of diagnostics, select **Option→Run Diagnostics...**. This will allow you to run all or selected tests one or more times. At this point, the server will shut-down and reboot (operating system shutdown for Windows NT and an effective Ctrl-Alt-Del for OS/2 Warp Server) and the set of ROM-based system diagnostics will run on the machine.

While the diagnostics are being performed, the following message will appear on the server:

```
*** WARNING Running Diagnostics ****
```

Once the diagnostics have been completed the server will reboot and the System Diagnostics Manager window will refresh and the results of the run will be displayed.

You can also review old diagnostic runs by selecting **Session→Select** from the main window. This will give you a list of all previously run tests, similar to Figure 79 on page 109.



Results for 2 sessions available for viewing.

Session 2: Completed 02/16/1998 10:15:16p.
Session 1: Completed 12/11/1997 08:06:45p.

Figure 79. Previously Run Diagnostics

4.3.2 Advanced Systems Management Adapter

Notice

For this section, we have tested the Advanced Systems Management Adapter installation using a Server 330 model 8640-PB0. For Server 325 and other Server 330 models, the location of connectors may vary. (see Figure 81 on page 110)

To verify the location of required connectors, see the system board diagram located inside the cover of your server or see your server's user guide.

Before installation, locate the following cables and connectors for an easy installation:

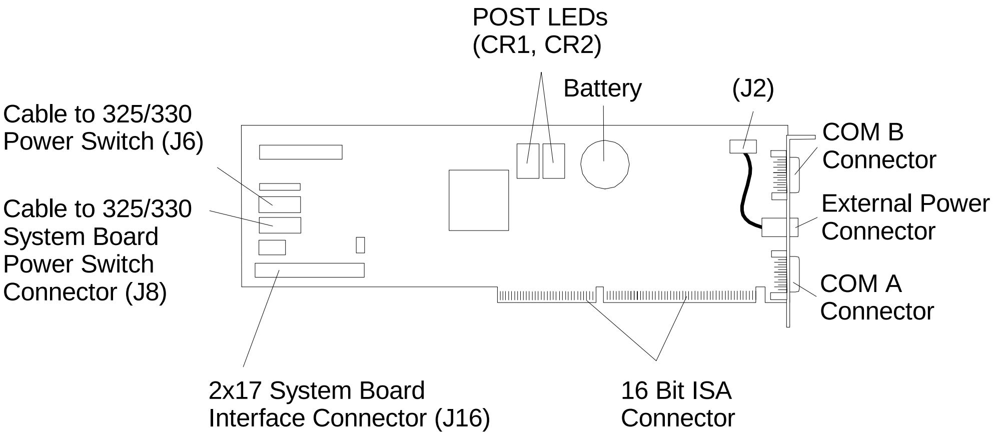


Figure 80. Advanced Systems Management Adapter

- **Advanced Systems Management Adapter**: (see Figure 80)
  - Cables
    - 34-pin
    - 16-pin
  - Connectors
    - System Board Interface (J16)
    - 325/330 System Board Power Switch (J8)
    - 325/330 Power Switch (J6)

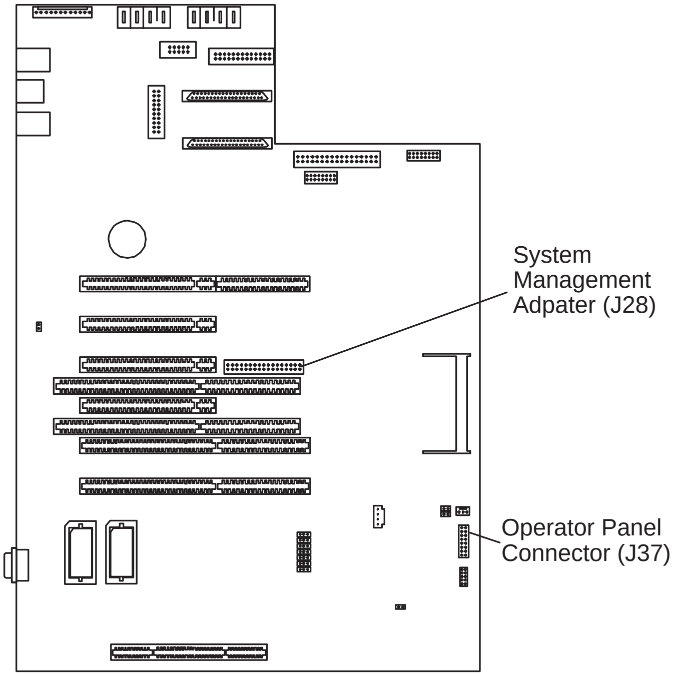


Figure 81. Server 330 System Board

- Connectors on the system planar (see Figure 81):
  - System Management Adapter (J28)
  - Operator Panel (J37)

To install the Advanced Systems Management Adapter in Server 330, perform the following steps:

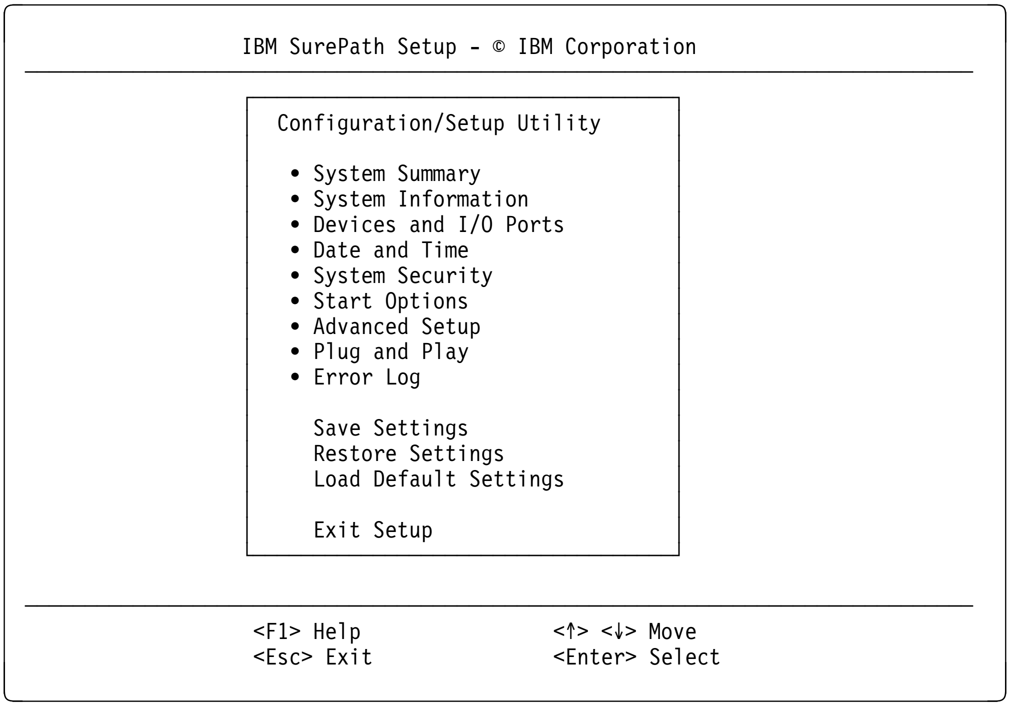
1. Disconnect the cable from J37.
2. Connect one end of the 34-pin cable to J28.
3. Connect the other end of the 34-pin cable to J16.
4. Connect one end of the 16-pin cable to J37.
5. Connect the other end of the 16-pin cable to J8.
6. Connect the cable that you disconnected in Step 1 to J6.
7. Now the card is ready to be installed into any ISA slot.

Installation Tip

Since the connector J28 is close to PCI/ISA shared slot #4, we recommend to insert the Advanced Systems Management Adapter into this slot.

Now the card is ready to be configured to operate on the server. See Chapter 3, “Advanced Systems Management Adapter” on page 63 for instructions. To complete the system setup, perform the following steps: (see Figure 82 on page 111)

1. Restart the server and run the **Configuration/Setup Utility** .
2. Reserve the I/O addresses for the adapter ports by selecting **Plug and Play** → **I/O ports**.
3. Reserve the interrupts for the adapter Service Processor port and the two adapter COM ports by selecting **Plug and Play** → **Interrupt**.
4. Follow the on-screen prompts to exit the Configuration/Setup Utility.



```
                 IBM SurePath Setup - © IBM Corporation

                   Configuration/Setup Utility

                    • System Summary
                    • System Information
                    • Devices and I/O Ports
                    • Date and Time
                    • System Security
                    • Start Options
                    • Advanced Setup
                    • Plug and Play
                    • Error Log

                      Save Settings
                      Restore Settings
                      Load Default Settings

                      Exit Setup

                 <F1> Help                <↑> <↓> Move
                 <Esc> Exit               <Enter> Select
```

Figure 82. Server 330 System Setup Main Window

4.3.2.1 Using Advanced Systems Management Adapter with Other ISA/EISA Adapters

Reference: RETAIN Tip H163424

There is a known problem when configuring memory resources for the Advanced Systems Management Adapter in certain models of the PC Server 325 and 330 when other ISA or EISA adapters are installed.

Models Affected

The models affected are: PC Server 325 models EJ0, ES0, ESV, RS0, PT0, PTW, PB0 and RB0. PC Server 330 models ES0, ES2, ESS, EM2, PT0, PB0 and PM0.

The symptoms are the following POST errors at startup:

```
112 I2C interface hardware error
173 Configuration change has occurred
188 System ID information destroyed - Bad VPD CRC#2
```

The Advanced Systems Management Adapter uses 300h-307h temporarily during POST regardless of the I/O Range it has been set to use. Other Adapters set to use the 300h-307h I/O address range will conflict with the Advanced Systems Management Adapter card During POST.

The solution is to configure the Advanced Systems Management Adapter Adapter for I/O address range 300h-307h and IRQ 5. (The default is IRQ 5 and I/O address 200h-207h).

4.4 IBM Netfinity 3000 and 3500

The IBM Netfinity 3000 and 3500 are designed for the small to medium sized business which requires a server for their e-business needs. The They are at home as a file and print server or as an entry level application server.

They are powered by Pentium II processors — the Netfinity 3000 uses one, and the Netfinity uses one or two processors. Both systems offer 512 KB of integrated Level 2 ECC cache. 32 MB or 64 MB of high-speed, 66 MHz synchronous or 100 MHz SDRAM 72-bit ECC system memory is standard and is upgradable to 512 MB. Figure 83 on page 114 shows an exploded view of the Netfinity 3500.

4.4.1 System Management

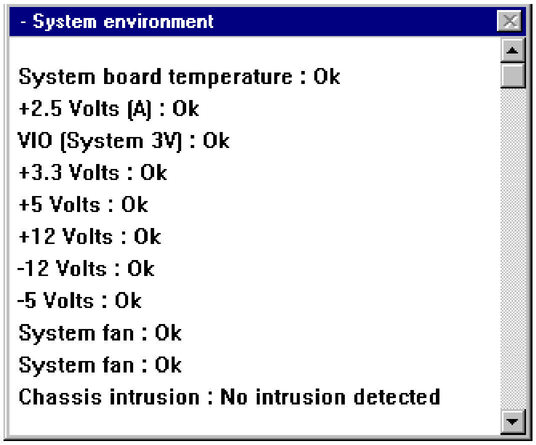
As well as the standard Netfinity Manager functions, the Netfinity 3000 and 3500 have a National Semiconductor LM78 management processor and I²C bus on the planar which provide a a number of hardware monitors that can be integrated into Netfinity Manager.

Note: These additional management functions are only available for OS/2, Windows 95 and Windows NT. No support is provided for NetWare.

The monitors available are:

- System board temperature status
- Power supply voltage status
- CPU voltage status
- Fan status
- Chassis Intrusion

These monitors are available to the System Monitor function of Netfinity Manager and alerts can be set on them to notify you when their status changes. The real-time monitor window is as shown in Figure 84.



System board temperature : Ok
+2.5 Volts (A) : Ok
VIO (System 3V) : Ok
+3.3 Volts : Ok
+5 Volts : Ok
+12 Volts : Ok
-12 Volts : Ok
-5 Volts : Ok
System fan : Ok
System fan : Ok
Chassis intrusion : No intrusion detected

Figure 84. Netfinity 3000/3500 Hardware Monitors

A history of all changes to these monitors is also available by right-clicking on the System Environment window and selecting **View** → **Attribute History**.

Each of the monitored attributes can be one of a set of predefined values, as shown in Table 13 on page 114. Alerts can be set up in System Monitor by

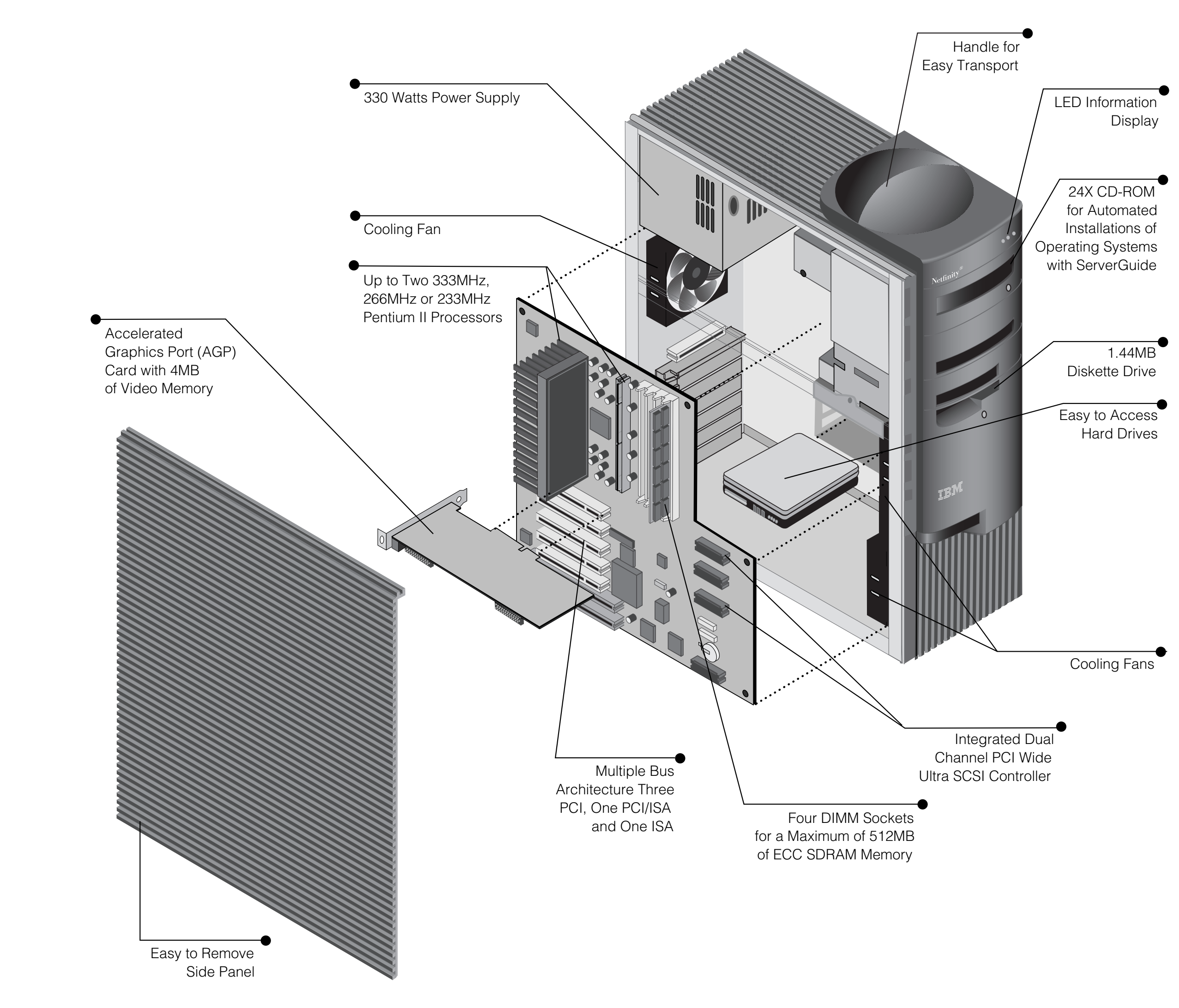

Handle for Easy Transport
330 Watts Power Supply
LED Information Display
24X CD-ROM for Automated Installations of Operating Systems with ServerGuide
Cooling Fan
Up to Two 333MHz, 266MHz or 233MHz Pentium II Processors
Accelerated Graphics Port (AGP) Card with 4MB of Video Memory
1.44MB Diskette Drive
Easy to Access Hard Drives
Netfinity
IBM
Cooling Fans
Integrated Dual Channel PCI Wide Ultra SCSI Controller
Multiple Bus Architecture Three PCI, One PCI/ISA and One ISA
Four DIMM Sockets for a Maximum of 512MB of ECC SDRAM Memory
Easy to Remove Side Panel

Figure 83. The Netfinity 3500 Exploded view

right-clicking on the monitor window and selecting **Open** → **Thresholds**. These can then be used by Alert Manager to perform specific actions. See 2.4, “Alerts” on page 24 for more information on how to set up actions in Alert Manager.

Table 13 (Page 1 of 2). Preset Values for Netfinity 3000/3500 Monitors

Attribute	**Possible Values**
System board temperature	OK, High, Too High
+2.5 Volts	Low, OK, High
VIO (System 3V)	Low, OK, High
+3.3 Volts	Low, OK, High
+5 Volts	Low, OK, High
+12 Volts	Low, OK, High
-12 Volts	Low, OK, High
-5 Volts	Low, OK, High
System fan #1	Too Low, OK

Table 13 (Page 2 of 2). Preset Values for Netfinity 3000/3500 Monitors

Attribute	**Possible Values**
System fan #2	Too Low, OK
Chassis intrusion	Detected, Not detected

For each attribute, thresholds have already been set by default. You can create new thresholds or modify the existing ones.

As well as system monitors, the Netfinity 3500 can also gather the serial numbers of certain hardware components through the **System Information** → **Vital Product Data** function. The serial numbers it gathers are:

- Processor(s)
- Hard disk(s)
- Diskette drive
- Power supply
- System board
- Memory DIMM(s)

4.4.1.1 Management Driver Installation

Prior to installing Netfinity Manager, you need to install the necessary management drivers.

Note: The drivers are only available for OS/2, Windows 95 and Windows NT. No support is provided for NetWare.

The diskette image for the Netfinity 3500 is available on ServerGuide 4.0.1 or later. The diskette image for the Netfinity 3000 is available on ServerGuide 4.0.4 or later. They should also be available from:

```
http://www.pc.ibm.com/us/support
```

Select **Intel Processor Based Servers Support**, then your server, then **Downloadable Files**

Note: The driver may also be known as the *ClientCare* diskette.

To build the diskette image from ServerGuide, follow these steps: (if you already have Diskette Factory installed, skip to Step 6).

1. Insert CoPilot ApplicationGuide 3A CD-ROM
2. CoPilot should automatically start for Windows NT systems. Run `SCOS2.CMD` to start CoPilot from OS/2
3. Select your desired language (for example, English).
4. Select **Diskette Factory**
5. Click on the Install button.
6. Run Diskette Factory **Start** → **Programs** → **ServerGuide Utilities** → **Diskette Factory**
7. Select **Other Servers** and click on the "►" button.
8. Select **IBM Netfinity 3500 System Diskettes** or **IBM Netfinity 3000 System Diskettes** or and click on "►" to continue.
9. Deselect all options, by clicking on the **Select/Deselect All** button
10. Select **Windows NT Device Drivers** or **OS/2 Device Drivers** and click on "►."
11. Insert the SoftwareGuide CD-ROM and a blank diskette and Click **OK** to continue.

Once the diskette is created, run the following command to install the drivers:

for Windows NT, run `A:\WINNT\NETFINST`
for OS/2, run `A:\OS2\NETFINST`

Once the drivers are installed, you will need to reboot your server, then install or reinstall Netfinity Manager.

4.4.2 Advanced Systems Management Adapter

The Advanced Systems Management Adapter is also available as an option in the Netfinity 3000 and Netfinity 3500. The adapter, in conjunction with Netfinity Manager, allows you to better manage the availability of your server. The Netfinity 3500 supports the Advanced Systems Management Adapter in either of the two ISA slots (slots 5 or 6).

All of the functions of the Advanced Systems Management Adapter are supported except for the following:

- POST timeout
- Operating system loader timeout
- Remote POST console

4.4.2.1 Adapter Installation

As there is no I²C connector on the system board, the installation of the Advanced Systems Management Adapter is straight forward:

1. Install the adapter in the slot using the usual electrostatic precautions.
2. Reserve an IRQ and a port address for the adapter in ISA Legacy Resources section of the Setup utility.

   This can be accessed by pressing F1 at the IBM logo during system POST. The resources you can reserve are as per Table 14.

   Table 14. Valid I/O Addresses and Interrupts

I/O Address	Interrupt (IRQ)
100-107	3
120-127	4
140-147	5
168-16F	9
188-18F	10
200-207	11
220-227	14
240-247	15
268-26F	
300-307	

   We recommend that you use the default settings, port 200-207 and IRQ 5.

3. Boot the server using the *Advanced Systems Management Adapter Configuration Update Utility and Device Driver* diskette and set up the Service processor to the resources you reserved. We used version 2.20 of this diskette and we setup port 200-207 and IRQ 5 for the card.
4. Set up the COM ports on the adapter.

   For further information on the configuration of COM ports see Chapter 3, “Advanced Systems Management Adapter” on page 63

Chapter 5. IBM Cluster Systems Management

IBM Cluster Systems Management (ICSM) is IBM's cluster systems management tool focused exclusively on managing Netfinity clusters in a Microsoft Cluster Server (MSCS) environment. It provides portable, generic cluster systems management services that integrate into existing Systems Management tools such as IBM Netfinity Manager, Intel LANDesk, and Microsoft SMS.

ICSM offers enhancements to the manageability of MSCS in three distinct categories:

1. Ease-of-Use

   ICSM provides a portable, generic cluster systems management GUI program with associated services that reside on the client and integrate into Netfinity, LANDesk, or SMS. This GUI interface allows administrators to easily discover and select clusters on all domains that can be accessed by the workstation as icons with names associated with them, and use the Cluster Expert Wizard to manage the setup of resource groups including the management of Virtual IP addresses in the MSCS environment.

2. Productivity

   The Cluster Scheduler is a productivity tool within ICSM that provides a unique set of functions that give administrators flexibility to schedule cluster-related events. This feature, for the first time, allows manual scheduled load balancing of MSCS resource groups. As an example, a Database Group in MSCS may consist of a database application, IP address, tape backup, and a shared disk. The database group could be scheduled to be taken offline, put online, or moved even if the original owning node goes offline.

3. Event/Problem Notification

   One of the strongest functions of MSCS is its ability to send a notification to an application via its API when a change occurs for any object within the cluster hierarchy. ICSM takes advantage of this base underlying function through a more capable alert management system.

   Two key components of the alert management function:

   a. It allows an administrator, using one GUI interface, to configure alerts and alert actions by clicking on an Alert button and launching an Alert Window in the selected opened cluster.

   b. Since ICSM has the ability to discover all of the clusters in the current Windows NT domain, alerts are generated for a group of clusters if significant changes occur at the resource, group, and node within a particular domain level.

   This single GUI interface offers administrators the benefit of a single location for setup and configuration of alerts for single and multiple clusters.

IBM Cluster Systems Management is implemented as plug-in modules for IBM Netfinity Manager, Intel LANDesk and Microsoft SMS.

5.1 Installing ICSM

Before you can install IBM Cluster Systems Management, the Microsoft Cluster Server environment must be installed and running on the cluster servers. You must also have one of the following management tools installed:

- IBM Netfinity Manager, Version 5.1 or above
- Intel LANDesk for Server Manager, Version 2.52 or above
- Microsoft SMS, Version 1.2 or above

You can install ICSM on either a cluster server or a workstation. The workstation must have Windows NT Workstation 4.0 or above installed.

ICSM is included in ServerGuide Version 4.0 or later. When you install Netfinity Manager, ICSM will be automatically installed during the process. An additional icon **Cluster Manager** will appear in the Netfinity Manager main window.

If you wish to integrate ICSM with Microsoft SMS or Intel LANDesk, you need to first install those products then use ServerGuide CoPilot (from the ApplicationGuide 3A CD-ROM) and select **IBM Cluster Server Management** from the list of installable applications.

5.2 Running ICSM

Depending on which management software you installed, the icon to start ICSM will be located as follows:

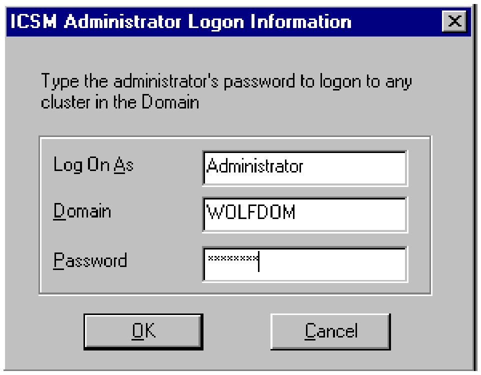
- For Netfinity Manager, double click on the **Cluster Manager** icon in the Netfinity Manager main window.
- For LANDesk, start the LANDesk Server Management console and select **ICSM**.
- In an Microsoft SMS environment, start the SMS administrator. From the tools menu, select **ICSM**.

When starting ICSM for the first time, you will have to provide a user ID, domain name and password (see Figure 85 on page 119). To administer the cluster, log on with a user account that has domain administrator privileges.

User Privileges

If you cannot log on with your user account, check that the user has the privilege to log on to Windows NT as a service in a domain account.

For detailed information about user accounts refer to the *Microsoft Cluster Server Administrator's Guide*.



Type the administrator's password to logon to any cluster in the Domain

Log On As: Administrator

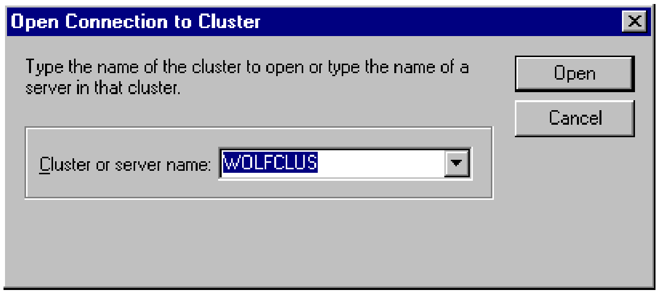
Domain: WOLFDOM

Password: ********

Figure 85. Enter User Information when Starting ICSM for the First Time

The ICSM window will appear. Click on **File** → **Open connection**.

In the panel shown in Figure 86 fill in the cluster name you want to connect to or the name of one of the cluster servers. In our configuration we could either fill in the cluster name WOLFCLUS or the name of a cluster server, for example WOLF1 or WOLF2.

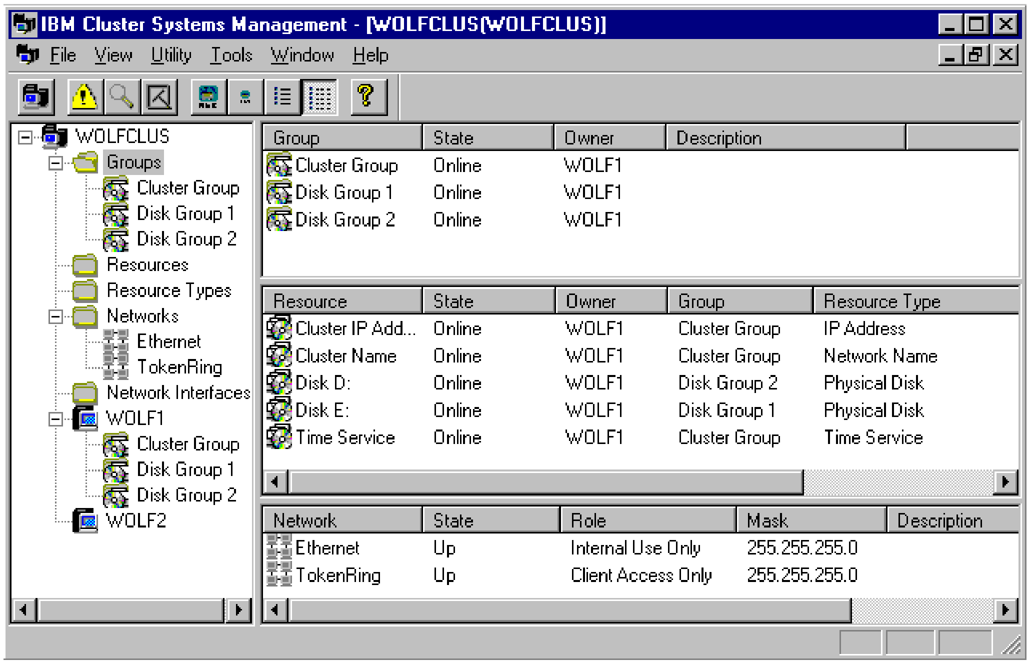


Type the name of the cluster to open or type the name of a server in that cluster.

Cluster or server name: WOLFCLUS

Figure 86. Open the Connection to a Cluster

Click on **Open** and you will see the window shown in Figure 87 on page 120.



Group	State	Owner	Description
Cluster Group	Online	WOLF1	
Disk Group 1	Online	WOLF1	
Disk Group 2	Online	WOLF1	

Resource	State	Owner	Group	Resource Type
Cluster IP Add...	Online	WOLF1	Cluster Group	IP Address
Cluster Name	Online	WOLF1	Cluster Group	Network Name
Disk D:	Online	WOLF1	Disk Group 2	Physical Disk
Disk E:	Online	WOLF1	Disk Group 1	Physical Disk
Time Service	Online	WOLF1	Cluster Group	Time Service

Network	State	Role	Mask	Description
Ethernet	Up	Internal Use Only	255.255.255.0	
TokenRing	Up	Client Access Only	255.255.255.0	

Figure 87. The ICSM Window

There are four views in this window. On the left side, there is the view of the whole cluster as we have seen it in the Microsoft Cluster Server administration window. What has changed compared to the Microsoft Cluster Server administration window is the information on the right side. Group, resource and network information is provided for any item you select on the left side.

For example, if you click on node WOLF1 on the left side, you will see the appropriate information of the node on the right side. The groups belonging to node WOLF1 will be displayed as well as all resources that are owned by WOLF1 and its network interfaces.

5.3 Administering the Cluster

In the ICSM window, you can perform any tasks that were also available in the Microsoft Cluster Server administration window, such as creating groups and resources, defining failover and failback policies, bringing resources and groups online.

In this chapter, we discuss some of the *additional* features provided by ICSM.

For more information about ICSM, refer to the *ICSM User's Guide*. This is available from ServerGuide in printable format (PostScript) or in viewable format (INF):

\PUBS\EN\CLUSMGEN.PS on the BookFactory CD-ROM
\PUBS\EN\CLUSMGEN.INF on the SoftwareGuide CD-ROM

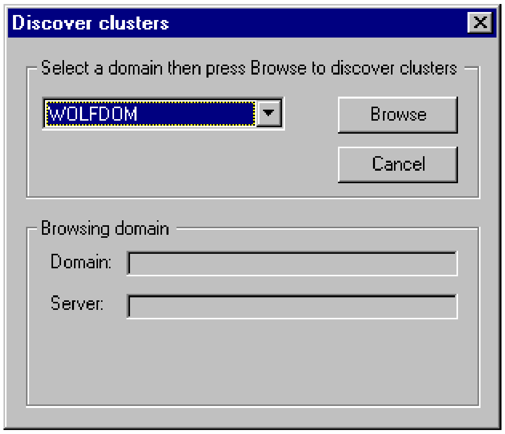
INF files can be viewed without additional software under OS/2. The viewer for Windows (XVIEW) can be obtained from

`http://www3.pc.ibm.com/techinfo/b216.html`

5.3.1 Discovery

With ICSM you can connect to a cluster even if you do not know the name of the cluster or the name of the domain the cluster belongs to. You can browse domains and determine which clusters are available.

To discover clusters from the main window, click on **Utility** then on **Discover Clusters**. A window will appear where you can select the domain you want to discover (see Figure 88). The default is All Domains. We want to discover the WOLFDOM domain where the cluster WOLFCLUS resides.



Discover clusters

Select a domain then press Browse to discover clusters

WOLFDOM

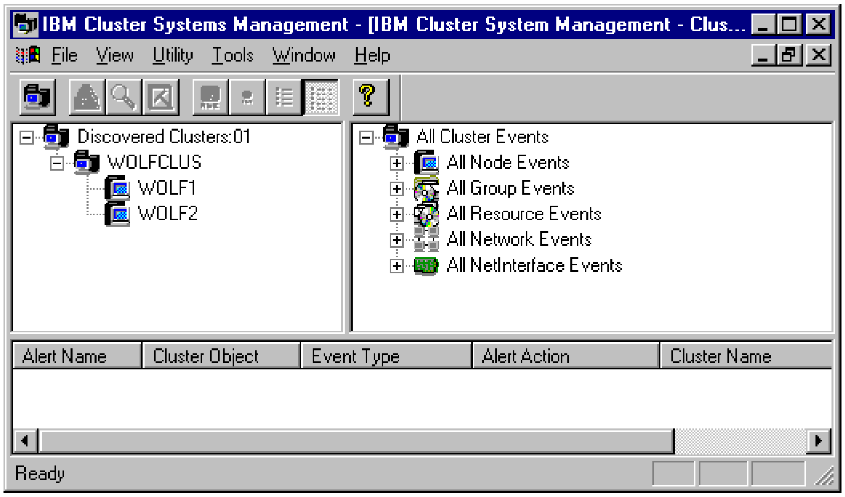
Browsing domain

Domain:

Server:

Figure 88. Define the Domain to be Discovered

Click on **Browse**. You will see the window shown in Figure 89.



IBM Cluster Systems Management - [IBM Cluster System Management - Clus...

Discovered Clusters:01
WOLFCLUS
WOLF1
WOLF2

All Cluster Events
All Node Events
All Group Events
All Resource Events
All Network Events
All NetInterface Events

Alert Name	Cluster Object	Event Type	Alert Action	Cluster Name

Ready

Figure 89. The Discovered Cluster WOLFCLUS of the Specified Domain WOLFDOM

On the left side, the cluster and cluster nodes that have been found are shown. The cluster events that have occurred are listed on the right side of the window. At the bottom you can see the alerts, that have been created within the cluster.

You can administer the cluster if you have an appropriate user account by clicking on the cluster nodes on the left side.

5.3.2 The Cluster Expert Wizard

The Cluster Expert Wizard provides an easy way to create predefined resource groups that are often used.

When you create a group with its resources in the Microsoft Cluster Server administration window, you have to consider which resources are dependent on other resources. You have to first define the resource, which has no dependencies on other resources.

With the Cluster Expert Wizard you can create the groups and resources *without* knowing which resources have dependencies. When this redbook was published, the following groups were available:

- File Share
- Internet Information Server
- Print Spooler

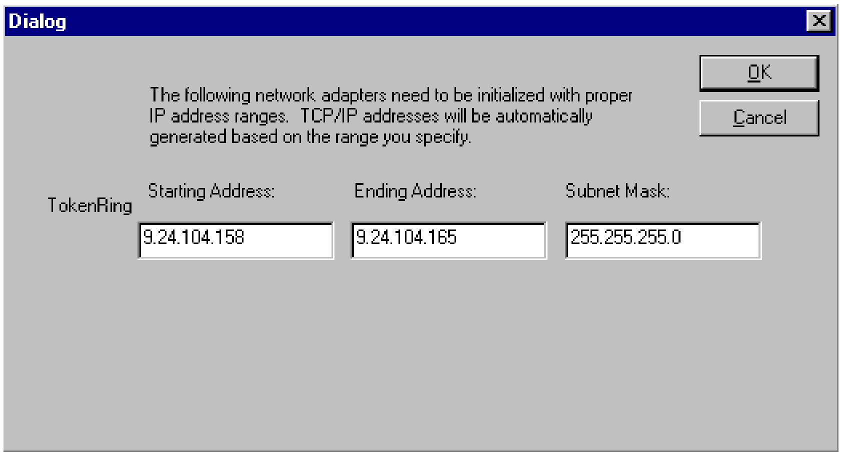
(The dependencies of each of their resources are described in the MSCS Administrator's Guide, or Chapter 5 of *Clustering and High Availability Guide for Netfinity and PC Servers*, SG24-4858.)

When you are creating the first group using the Cluster Expert Wizard, a window will appear as shown in Figure 90. You are asked to fill in a range of IP addresses that can be assigned to IP address resources for use in the cluster. Ask you LAN administrator for a valid range of IP addresses.

IP Address

Before using the Cluster Expert Wizard to create a resource group, be sure you have at least one IP address available for use in the cluster.

As mentioned above, the Cluster Expert Wizard creates dependencies within resources automatically. If the resource IP address must be created because of a dependency on that resource, an IP address must be available. The cluster administrator does not provide an IP address whenever one is needed, but provides several IP addresses in this window for future use.



The following network adapters need to be initialized with proper IP address ranges. TCP/IP addresses will be automatically generated based on the range you specify.

TokenRing Starting Address: 9.24.104.158 Ending Address: 9.24.104.165 Subnet Mask: 255.255.255.0

Figure 90. Providing IP Addresses for Future Use in the Cluster

During the installation procedure of Microsoft Cluster Server we defined the token-ring to be the network interface for client access to the cluster. Therefore we provide IP addresses for the token-ring network only.

5.3.2.1 File Share

Before you create a file share resource group, ensure that a physical disk is available.

To create or change a file share resource group, do the following:

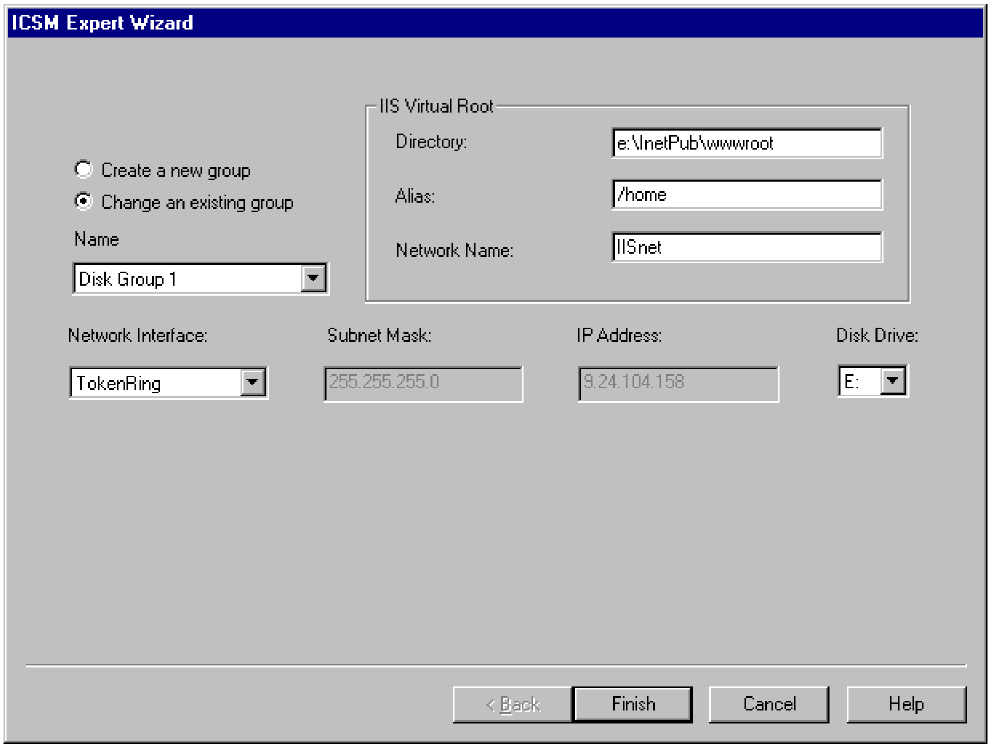
1. Click on **Utility** → **Cluster Expert Wizard** → **File Share**.
2. In the window that appears, specify if you want to create a new group or if you want to change an existing group.
3. You will also have to provide a share name, a path, and a network name.
4. Specify the network interface and choose a disk drive for the file share.
5. You need not care about any dependencies of resources within the File Share group.
6. The necessary resources for the file share will be created and brought online automatically.

5.3.2.2 Internet Information Server (IIS)

ICSM provides an easy way to configure MSCS groups compared to the standard Administration utility. This section describes how to use ICSM to use the Cluster Expert Wizard to create the IIS resources.

To create the IIS resource, follow these steps:

1. Click on **Utility** → **Cluster Expert Wizard** → **IIS Virtual Root**. You will see the window shown in Figure 91 on page 124.



ICSM Expert Wizard

○ Create a new group

● Change an existing group

Name: Disk Group 1

IIS Virtual Root

Directory: e:\InetPub\wwwroot

Alias: /home

Network Name: IISnet

Network Interface: TokenRing

Subnet Mask: 255.255.255.0

IP Address: 9.24.104.158

Disk Drive: E:

Figure 91. Creating the IIS Resource Group Using the Cluster Expert Wizard

2. Click on **Change an existing group**. Select a group, for example Disk Group 1 in our configuration.

   Use the disk group that contains the physical disk where you installed the Publishing Directories during IIS Software installation.

3. Specify the directory for the IIS Virtual Root.

   This is the path that you defined for the publishing directories when you installed the IIS Software, for example E:\INETPUB\WWWROOT.

4. In the Alias text box fill in `/HOME`, which refers to the directory E:\INETPUB\WWWROOT.

   If you fill in another alias, it must exist as a subdirectory in your publishing directory. For example, if we want to enter /IISALIAS, the directory structure E:\INETPUB\WWWROOT\IISALIAS must exist.

5. Enter a network name, for example IISnet. This is the name for the IIS Server that client workstations will see in the Network Neighborhood folder.

6. Define the network interface you want to use. As we defined the token-ring to be the client interface, a token-ring address is taken from the list provided in an earlier step and is automatically filled in.

7. The Disk Drive field specifies the drive where the disk group we use for the IIS resides.

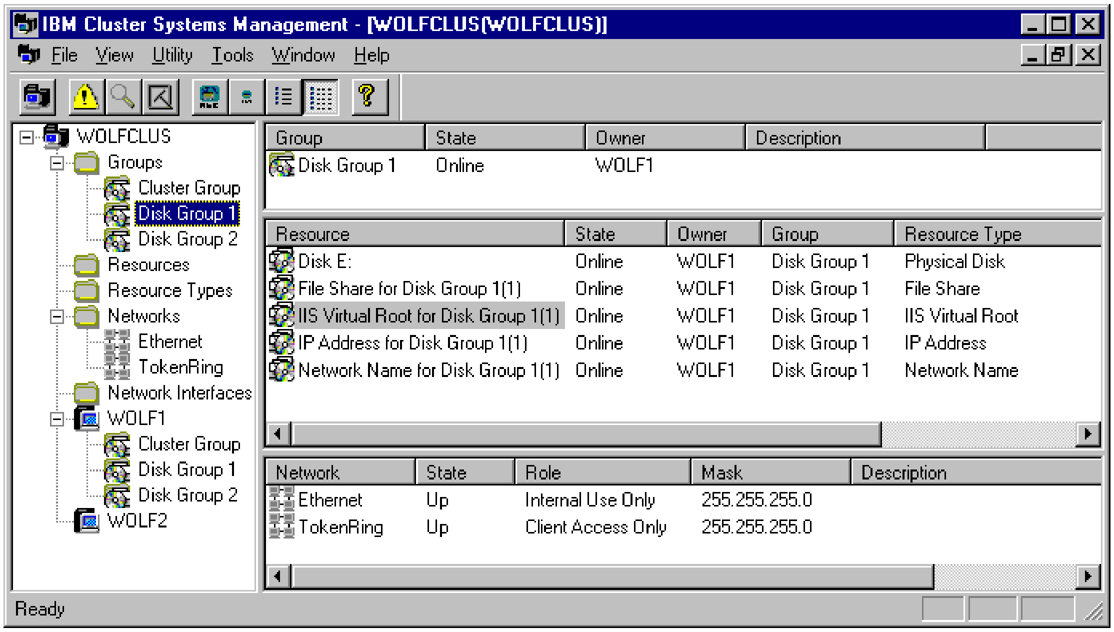
8. Click on **Finish** to create the IIS Virtual Root.

9. You will see an information window that you should check if all new resources are brought online.

10. Click on **OK**.

11. In the ICSM window click on the disk group that was used to create the IIS resources.

    On the right side, you will see that the resources for the IIS are created and brought online (see Figure 92).



Group	State	Owner	Description
Disk Group 1	Online	WOLF1	

Resource	State	Owner	Group	Resource Type
Disk E:	Online	WOLF1	Disk Group 1	Physical Disk
File Share for Disk Group 1(1)	Online	WOLF1	Disk Group 1	File Share
IIS Virtual Root for Disk Group 1(1)	Online	WOLF1	Disk Group 1	IIS Virtual Root
IP Address for Disk Group 1(1)	Online	WOLF1	Disk Group 1	IP Address
Network Name for Disk Group 1(1)	Online	WOLF1	Disk Group 1	Network Name

Network	State	Role	Mask	Description
Ethernet	Up	Internal Use Only	255.255.255.0	
TokenRing	Up	Client Access Only	255.255.255.0	

Figure 92. The IIS Resources Are Created and Brought Online

If they are not online, you can bring them online manually by clicking on **File** and **Bring Online**.

If a resource should fail, check the following:

- Did you entered the correct values during configuration, for example the directory name and the group name?
- Is a valid IP address used in the parameters window of the IP address resource?
- Is an entry created in the Internet Service Manager? You may have to add it manually.

Using the ICSM administration window:

When we created the IIS resources in the Microsoft Cluster Server administration window, we had to do the following:

1. Find out which resources are required for the IIS Virtual Root
2. Determine dependencies between the resources
3. Create a resource for the IP address
4. Create a resource for the network name
5. Create a resource for the file share
6. Create a resource for the IIS Virtual Root
7. Bring the group and its resources online

Now that we used the ICSM administration window, we could configure the IIS Virtual Root in one window. All dependent resources are brought online automatically.

5.3.2.3 Print Spooler

Before you create a print spooler resource group, ensure that a physical disk is available.

To create a print spooler resource group, do the following:

1. Click on **Utility** → **Cluster Expert Wizard** → **Print Spooler**.
2. In the window that appears, click on **Change an existing group**.
3. Define the spool folder, the job completion time and the network name for the print spooler.

   Spool folder is the directory path on the shared drive where the print jobs will be spooled.

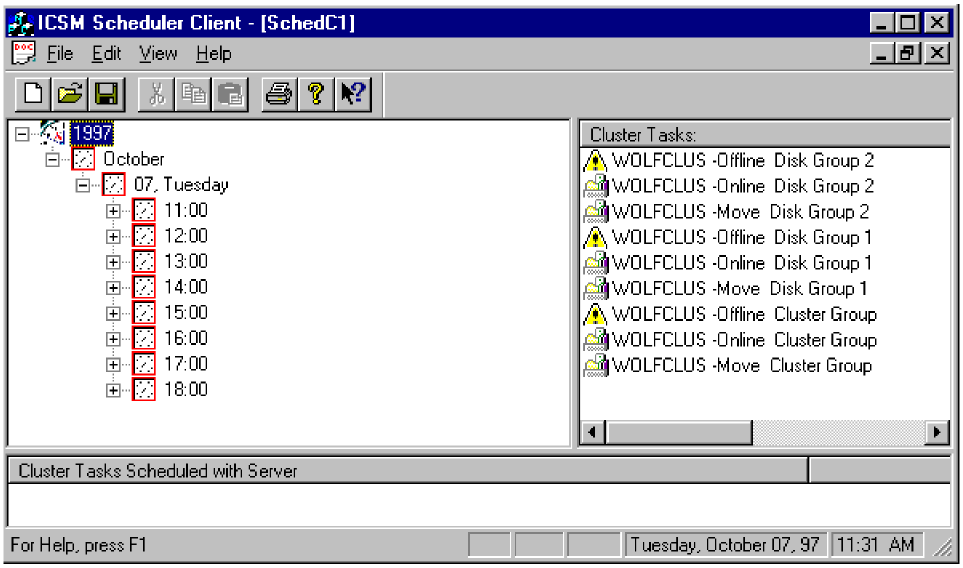
   Job completion is the length of time allowed for the print file to be completed by the print device. The file will be flushed if not completed within this period.

   The network name is the name users will see in the Network Neighborhood folder of their workstation.
4. Specify the network interface.
5. The Disk field should be automatically filled in if you use an existing group. If you create a new group, define a drive where the group and the print spooler resource will be located.
6. Click on **Finish** to create the Print Spooler resource group.
7. The group and its resources will be brought online automatically.

5.3.3 The Scheduler

The scheduler allows you to schedule manual load balancing of MSCS resource groups by allowing you to move the groups from one node to another node at a predetermined time. You can also schedule the starting or stopping of resource groups at predetermined times. You can check afterwards if the job was performed successfully with the ICSM Alert facility (see 5.3.4, “The Alert Utility” on page 127).

To start the scheduler, click on **Utility** and then on **Scheduler**. The scheduler window will appear, as shown in Figure 93 on page 127.



WOLFCLUS -Offline Disk Group 2
WOLFCLUS -Online Disk Group 2
WOLFCLUS -Move Disk Group 2
WOLFCLUS -Offline Disk Group 1
WOLFCLUS -Online Disk Group 1
WOLFCLUS -Move Disk Group 1
WOLFCLUS -Offline Cluster Group
WOLFCLUS -Online Cluster Group
WOLFCLUS -Move Cluster Group

Figure 93. The Scheduler Window

On the left side of the scheduler window the schedule date and time can be defined. The right side shows the tasks that can be scheduled. The jobs that have been scheduled to be performed appear at the bottom of the window. When the task is completed, the entry will be deleted from the list.

5.3.4 The Alert Utility

The Alert utility allows you to create alerts either for clusters in a domain or for groups, resources, nodes and network interfaces within one specified cluster.

You can create alerts for one or more clusters in the discovery window without being connected to a cluster (see 5.3.4.1, “Alerts in the Discovery View” on page 128).

To define alerts for a resource or group in a specified cluster you must be connected to the cluster (see 5.3.4.2, “Alerts in the Opened Connection Window” on page 128).

The following events can be reported within a cluster using the alert option:

- All cluster events
- All node events

  You can check if a special node is up or down or if a node is added to or deleted from the cluster.
- All group events

  You can be informed if a group goes into online, offline or failed state. If a group is added to or deleted from the cluster, you may want to be notified.
- All resource events

  The resource may go into online, offline or failed state. You can also be notified if resources are added to or deleted from the cluster.
- All network events

An alert can be generated if the network state changes to up, partitioned or down. You may also want to know if a network node has been added to or deleted from the cluster.

- All network interfaces

  If a network interface goes into up, unreachable or failed state you may want to be informed. You can get a notification if a network interface is added to or deleted from the cluster.

The alert actions are described in more detail in the *ICSM User's Guide* and in the User's Guide of your System Management software.

5.3.4.1 Alerts in the Discovery View

You can discover clusters in specified domains using the discovery utility as described in 5.3.1, “Discovery” on page 121. To create an alert from the discovery window for one or more clusters, follow these steps:

1. On the right side of the discovery window, double click on the event type you want to create an alert for.
2. In the Alert window, enter an alert name. The alert name must be unique.
3. Select the System Management tool you have installed on your system, for example Netfinity Manager.
4. Select an alert action and the severity for the alert. The severity option is different for each System Management tool.

   If you are using LANDesk, the alert window will appear after you click on **OK**.
5. Click on **OK**. The alert will be created at the bottom of the discovery window.

5.3.4.2 Alerts in the Opened Connection Window

Open the connection to a cluster as described in 5.2, “Running ICSM” on page 118. In the opened connection view you can specify alert for groups and resources within the cluster.

To create an alert from the opened connection window for a resource or group, follow these steps:

1. Click on **Utility** then on **Alert** in the ICSM menu. You will see the window shown in Figure 94 on page 129.

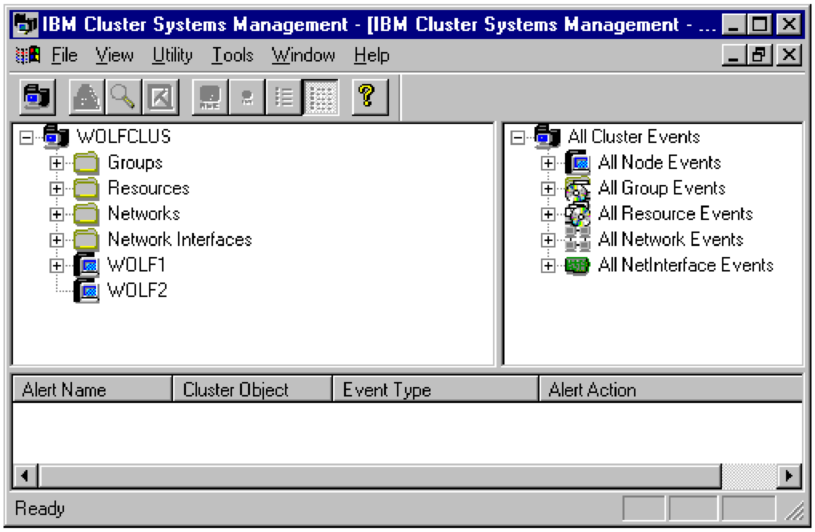


Figure 94. Alert Window for the Cluster WOLFCLUS

2. On the right side of the open connection window, double click on the event type you want to create an alert for.

3. In the Alert window, enter an alert name. The alert name must be unique.

4. Select the System Management tool you have installed on your system, for example Netfinity Manager

5. Select an alert action and the severity for the alert. The severity option is different for each System Management tool.

   If you are using LANDesk, the alert window will appear after you click on **OK**.

6. Click on **OK**. The alert will be created at the bottom of the discovery window.

Resources and Event Types must be Compatible

When you create an alert for a resource or group, make sure you combine the resource type with the appropriate event type.

For example, you can create an alert for the event type Resource deleted and the resource File Share for Disk Group 1.

Chapter 6. Example Scenarios

This chapter provides a number of example scenarios that use the features of the servers, Advanced Systems Management Adapter and Netfinity Manager to maintain a high level of availability to users and to ensure that when downtime occurs, it is kept to a minimum.

The following example scenarios are covered:

1. Air conditioning failure (Page 131) — using Netfinity Manager and the Advanced Systems Management Adapter to notify when temperature thresholds have been exceeded and ultimately to shut the server down.
2. Drive failure in an array (Page 142) — using Netfinity Manager to notify when a disk in an array fails and when the rebuild using a hot-spare is complete. Also notifies a remote service organisation that a disk needs replacing.
3. Power failure (Page 152) — using Netfinity Manager and PowerChute on our UPS to notify when power to the server room fails. Shuts the server down if power is not restored within a certain time.
4. Power supply failure (Page 160) — uses the Advanced Systems Management Adapter to notify when one of the redundant power supplies on a Netfinity 7000 fails.
5. Operating system hang (Page 164) — uses the Advanced Systems Management Adapter and Netfinity Manager to notify when the operating system hangs. Also automatically restarts the server.
6. POST timeout and remote POST console (Page 168) — notifies of a timeout restarts the server if the POST process take too long to complete. Use the remote POST console to view the POST process to perform problem determination.
7. Application failure and restart (Page 173) — uses Netfinity Manager to monitor an application and alert when it stops then automatically restarts it.
8. Remote BIOS Update (Page 177) — uses Netfinity Manager and the Advanced System Management service to remotely flash the system BIOS of the Netfinity 5500.

6.1 Example 1: Air Conditioner Failure

In this example, the air conditioning in the server room has failed. We have a Server 330 with an Advanced Systems Management Adapter installed and we want certain events to occur as the temperature rises, including contacting the administrator. Ultimately, we want the server to shut down when the temperature reaches an extreme value.

The specific actions we want are listed in Table 15.

Table 15 (Page 1 of 2). Temperature Thresholds for our Scenario

Description	Temperature	Action to perform
Hot	40°C	Send a warning alert to an administrator
Too Hot	50°C	Send an error alert to an administrator

Table 15 (Page 2 of 2). Temperature Thresholds for our Scenario

Description	Temperature	Action to perform
Danger	64°C	Power off the machine

Note: The values you set these thresholds to will depend on the location and the environment your server is working in. For example, if you server is in a chilled server room the temperature thresholds will be different than if in a regular office environment.

At the 40°C mark, we want the administrator to be paged with an information message. On the second event, the 50°C mark, we want her to be paged again with an error message. The final event will be at 64°C, which will power down the machine. The 64°C is hard-coded in the microcode in the Advanced Systems Management Adapter.

In this example, we are using OS/2 as our operating system, but the operating system choice should not make a difference.

These are the steps involved to set up the scenario:

1. Install the Advanced Systems Management Adapter

   Configure the card as per Chapter 3, “Advanced Systems Management Adapter” on page 63 and install the device driver before installing Netfinity Manager. If you do not install the driver first, Netfinity Manager will not be able to communicate with the Service Processor.

2. Configure a modem

   The scenario calls for the server to dial out to a remote pager so a modem is required to do this. Install your modem so that the operating system can communicate with it. We set this example up so that the Advanced Systems Management Adapter uses Port B and it is also shared with the operating system.

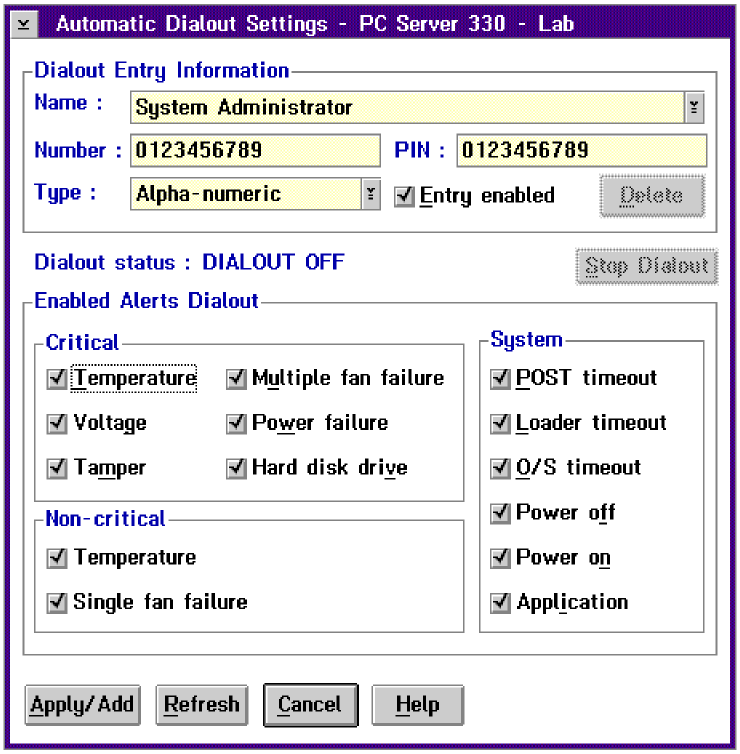
   Note: Sharing the port is not supported as described in 3.1.1, “COM Ports” on page 67. In a production environment we recommend that you use two modems, one connected to the Advanced Systems Management Adapter's port B and the other available to Netfinity to dial out with. We connected the modem to COM B of the adapter and gave it port address 2F8 and IRQ 3 which assigned this COM2: under OS/2.

3. Install Netfinity Manager

   See 2.2, “Installing Netfinity Manager” on page 5 for information on how to setup Netfinity Manager under your chosen operating system. Ensure you install Service Processor support.

4. Configure the Advanced Systems Management Adapter

   Using the installed Netfinity Manager, configure the dial out settings for the service processor. When configuring the Advanced Systems Management Adapter, set it to dial out on a critical temperature. This will allow a pager to be called when the system is powered off. The configuration can be seen in Figure 95 on page 133 and further details can be found in 3.2.4, “Automatic Dialout Settings” on page 79.



Automatic Dialout Settings - PC Server 330 - Lab

Dialout Entry Information

Name : System Administrator

Number : 0123456789 PIN : 0123456789

Type : Alpha-numeric ☑ Entry enabled Delete

Dialout status : DIALOUT OFF Stop Dialout

Enabled Alerts Dialout

Critical
- ☑ Temperature
- ☑ Multiple fan failure
- ☑ Voltage
- ☑ Power failure
- ☑ Tamper
- ☑ Hard disk drive

Non-critical
- ☑ Temperature
- ☑ Single fan failure

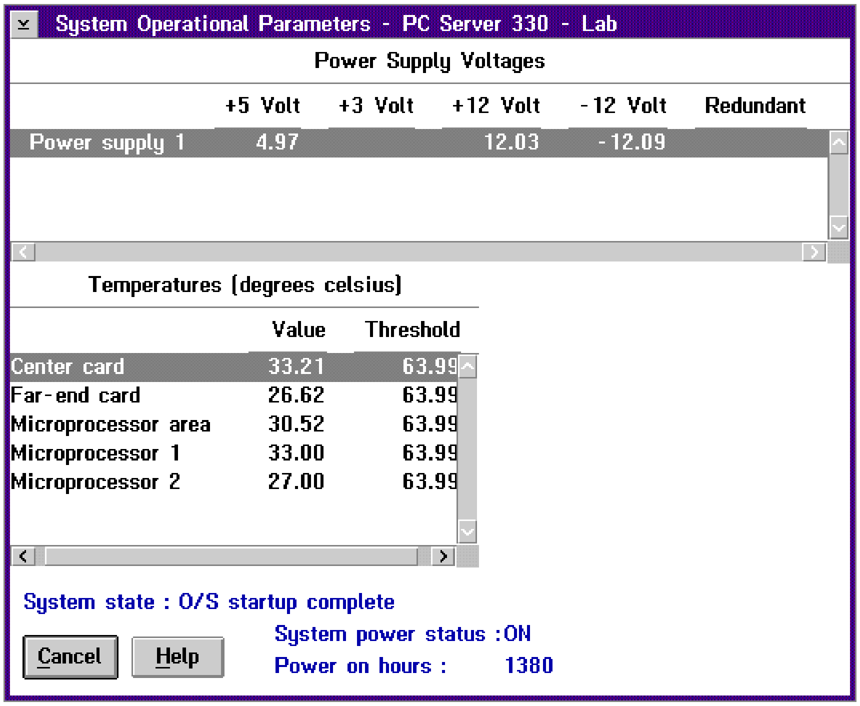
System
- ☑ POST timeout
- ☑ Loader timeout
- ☑ O/S timeout
- ☑ Power off
- ☑ Power on
- ☑ Application

Apply/Add Refresh Cancel Help

Figure 95. Service Processor Dial Out Setup. In our scenario, we need to have the Critical Temperature option set.

5. Configure System Monitor

   The Service Processor Operational Parameters window shows five temperature sensors on the Server 330 as shown in Figure 96 on page 134. The Advanced Systems Management Adapter has a thresholds associated with each these temperature sensors. If the temperature exceeds any one of these thresholds for more that one minute then the system will be powered off by the Advanced Systems Management Adapter card.



System Operational Parameters - PC Server 330 - Lab

Power Supply Voltages

	+5 Volt	+3 Volt	+12 Volt	-12 Volt	Redundant
Power supply 1	4.97		12.03	-12.09	

Temperatures (degrees celsius)

	Value	Threshold
Center card	33.21	63.99
Far-end card	26.62	63.99
Microprocessor area	30.52	63.99
Microprocessor 1	33.00	63.99
Microprocessor 2	27.00	63.99

System state : O/S startup complete

System power status :ON

Power on hours : 1380

Figure 96. Service Processor Operational Parameters

System Monitor will display three of these temperatures as monitors which you can set thresholds on.

- CPU 1 temperature
- CPU 2 temperature
- System Temperature (This directly relates to the Advanced Systems Management Adapter center of card temperature sensor)

6. Create a threshold for the system temperature

   The threshold can be setup for each of the monitors and allows you to set a limit, above which will generate an alert. We use **System Monitor** to configure the thresholds as per 6.1.1, “Configuring Thresholds.”

7. Set up Alert Manager profiles

   System Monitor will send a set of alerts to Alert Manager when the conditions are met. We need to configure Alert Manager to perform the required actions. This is discussed in detail in 6.1.2, “Configuring Actions” on page 136.

6.1.1 Configuring Thresholds

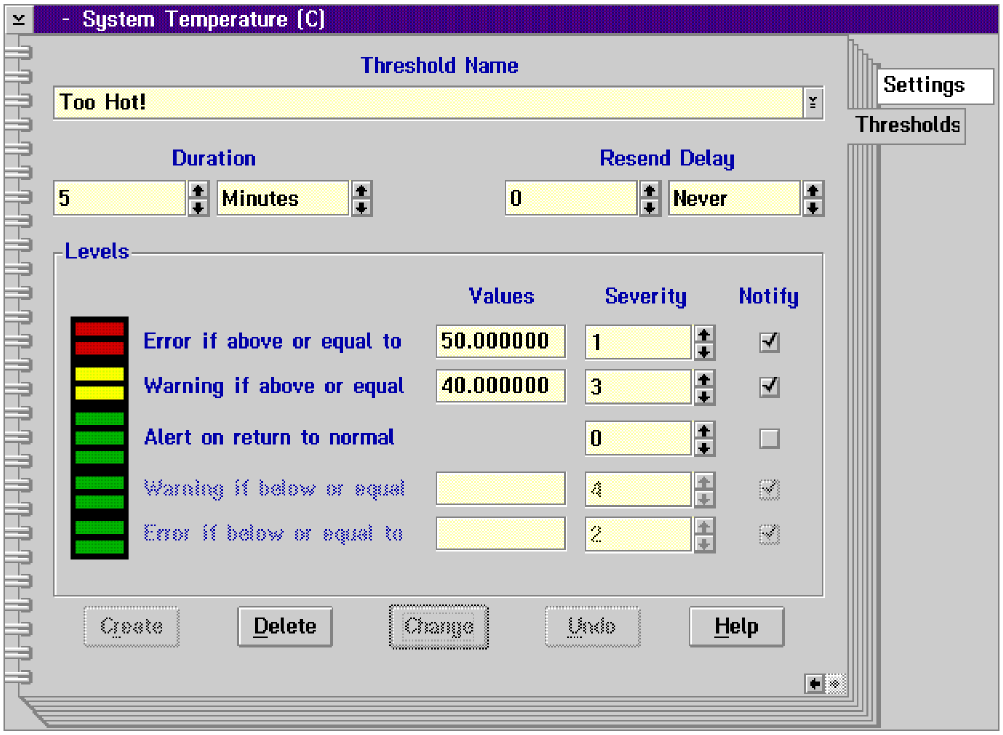
To configure the threshold in Netfinity Manager, do the following:

1. Start System Monitor and select **Windows** → **Show Monitors...** This will show a list of all the available monitors.

2. Select the **System Temperature** monitor and select **OK**.

   Note: If the System Temperature monitor is not in the list of available monitors, then it is likely you installed the Advanced Systems Management Adapter after you installed Netfinity Manager. You will need to reinstall Netfinity Manager.

3. Open the threshold settings window by either double-clicking on the monitor or right-clicking on the monitor and selecting **Open** → **Threshold**. Figure 97 on page 135 appears.



- System Temperature (C)

Threshold Name: Too Hot!

Duration: 5 Minutes

Resend Delay: 0 Never

Levels

	Values	Severity	Notify
Error if above or equal to	50.000000	1	☑
Warning if above or equal	40.000000	3	☑
Alert on return to normal		0	☐
Warning if below or equal		4	☑
Error if below or equal to		2	☑

Figure 97. System Temperature Threshold Settings

You now need to configure the threshold, as shown in Figure 97.

4. Name the threshold.

   This can be any name or phrase you would like but it does get passed to alert manager and does appear in the alert text. We called ours “Too Hot!” Once you start typing in this box the create button becomes active and you can then set the thresholds in the level boxes.

   > **NT User interface Tip!**
   >
   > Under Windows NT you will need to press Enter in the Threshold Name box to cause the create button to become active.

5. Set the threshold's duration.

   Specify the length of time that the monitor's threshold value must be exceeded before an alert is generated.

6. Set the resend delay.

   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 exceeded. For our example, we want only one alert to be sent.

7. Set the threshold's values.

   You can set up to four different threshold values, each of which will generate a different Netfinity alert.

8. Set the threshold's severity.

A default severity is set for each of the threshold values. The values can be adjusted for your own requirements.

9. Select notify values.

   If you want an alert to be sent locally on the threshold you have to select the **Notify** check box. We do want this to be sent so leave this as shown in Figure 97 on page 135 For an example of how to use this see 6.7, “Example 7: Application Failure and Restart” on page 173.

   The **Local Notify** checkbox is only seen if accessing from a remote manager and is useful if you want all alerts to be handled by one machine. If you want the threshold to generate a Netfinity alert on the system on which the threshold is being configured (thus enabling the local system to use it's Alert Manager to respond to the alert), select the **Local Notify** check box.

   We shall neither use this option nor see this option as we are configuring the alert locally. See 6.7, “Example 7: Application Failure and Restart” on page 173 for an example of when this is used.

10. Select alert on return to normal

    This will generate a separate alert to notify you that threshold values that were previously exceeded are no longer being exceeded, select the Alert on Return to Normal checkbox. We will not be using this option but it may be a useful item in your environment.

11. Save the threshold by clicking on **Create**.

    If the **Create** button is not highlighted then put the cursor in the Threshold Name field and press Enter. The button will then become active. If you have been editing a previously configured threshold, select **Change** to save the new threshold values.

System Monitor has now been configured to send alerts when the various temperatures are reached. We now need to configure Alert Manager to react to those alerts.

6.1.2 Configuring Actions

System Monitor will send a set of alerts to Alert Manager when the conditions are met. These alerts will be very similar as the Application ID and the Application Alert Type will be the same for both alerts.

As we want to have a different message sent to the administrator's pager when different conditions apply, we will set up the actions using profiles and not just Alert Conditions. This will allow us to name and group the alerts.

To enable Alert Manager to automatically respond to received alerts, you must associate (or *bind*) an alert profile to an action. 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. See 2.4, “Alerts” on page 24 for more information on alerts and alert profiles.

6.1.2.1 Configuring Alert Profile

To configure the alert profiles do the following:

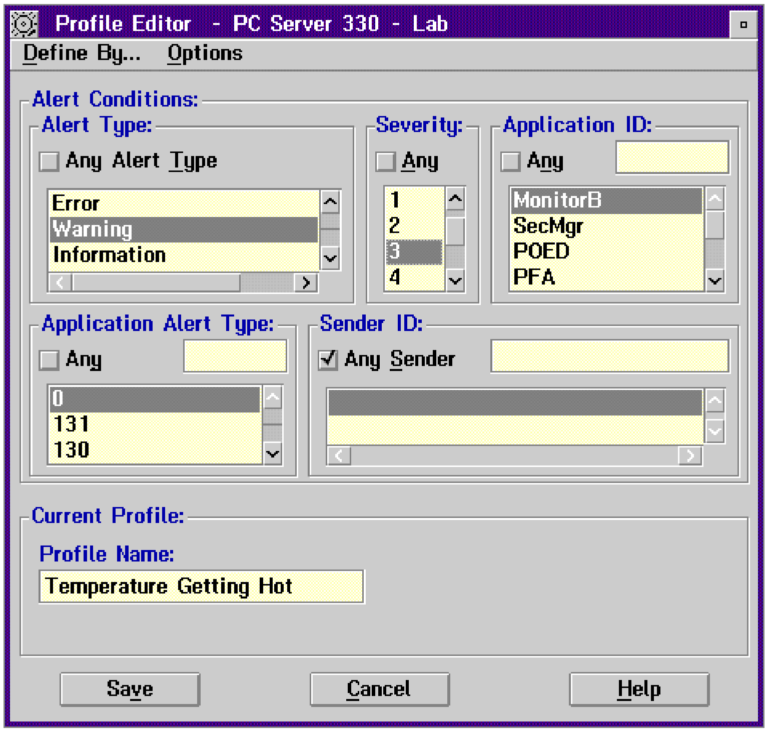
1. Open the Alert Manager on the Server 330.
2. Click the **Profiles** button.

   We need to define a alert profile for each of the three alerts that will be coming in to the Alert Manager on the server. Based on the thresholds we sent in 6.1.1, “Configuring Thresholds” on page 134, System Monitor will issue alerts for the 40°C and 50°C marks, and the Service Processor will issue an alert when the temperature reaches the critical 64°C point. The specifics of the alerts are shown in Table 16:

Table 16. Details for the Three Alerts

Alert Data	40°C Alert	50°C Alert	Power-off Alert
Alert Type	Warning	Error	Device Information
Severity	3	1	0
Application ID	MonitorB	MonitorB	SysMgt
Application Alert Type	0000	0000	0102
SenderID	Any	Any	Any

For the 40°C alert, we would get a severity 3 warning and at 50°C mark we would get a severity 1 error. The alert conditions are for the 40°C mark can be seen in Figure 98.



Profile Editor - PC Server 330 - Lab

Alert Conditions:

Alert Type: □ Any Alert Type
Error
Warning
Information

Severity: □ Any
1
2
3
4

Application ID: □ Any
MonitorB
SecMgr
POED
PFA

Application Alert Type: □ Any
0
131
130

Sender ID: ☑ Any Sender

Current Profile:

Profile Name: Temperature Getting Hot

Figure 98. Profile Editor for 40°C Alert

3. Click the **New** button to open a new profile in the profile editor. The profile editor enables the user to define profiles that match classes of alerts received by the Alert Manager.

4. From the Profile Editor window, ensure that Alert Conditions is selected in the menu and not Profiles Composition. Select **Define By... → Alert Conditions**

5. Select an Alert Type

   As per Table 16 on page 137, for the 40°C profile this is **Warning**.

6. Select a Severity

   For the 40°C profile this is **3**.

7. Select an Application ID

   For the 40°C profile this is **MonitorB**. If the Application ID required is not available from the list, you may add it to the list by entering the ID in the entry field above the selection list and pressing Enter.

8. Select an Application Alert Type

   For the 40°C profile this is **0000** as per Table 16 on page 137. If the Application Type required is not available from the list, you may add it to the list by entering the type in the entry field above the selection list and pressing Enter.

9. Select a Sender ID

   For the 40°C profile this is blank as it comes from the local machine. So we can set the tick box to specify that it is from any sender. If we wanted the local machine only we would either select the network address of the local machine or the blank line.

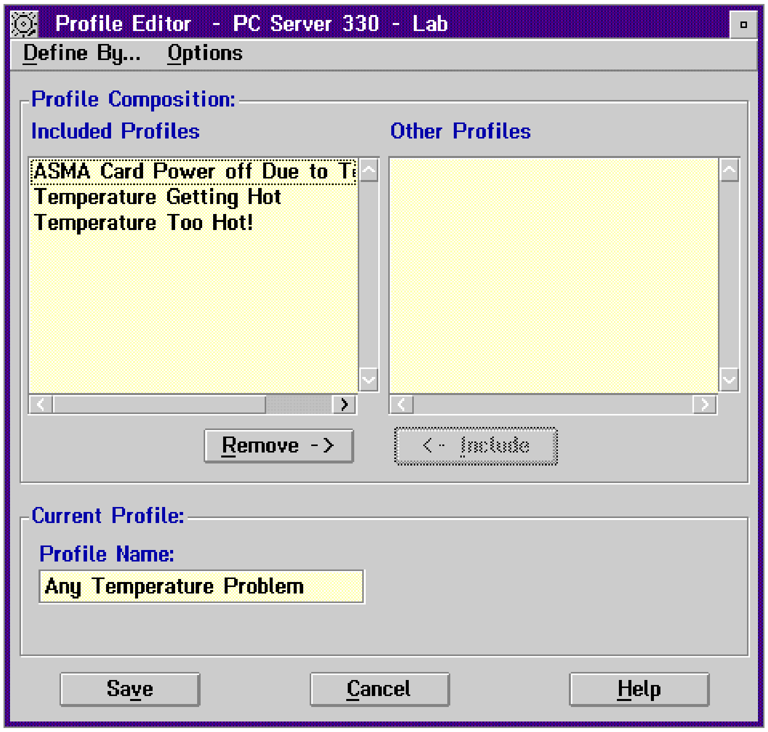
10. Name the Profile

    You must select a name for the profile. For the 40°C profile we set this to **Temperature Getting Hot**

11. Save the defined profile. This action will now appear in the Profile List window of the Alert Profiles window. The profile editor will look like Figure 98 on page 137 at this point.

12. Repeat Steps 137 to 138 but this time for the 50°C Alert and the Power off Alert. Refer to Table 16 on page 137 for the settings.

    We also want to log all temperature alerts so we now set up a new profile based on all previously defined alert profiles as shown in Figure 99 on page 139. To get to the window shown in Figure 99 on page 139, from the Alert Profiles window select **New** then the menu option **Define By... → Profile Composition**.



ASMA Card Power off Due to Te
Temperature Getting Hot
Temperature Too Hot!

Profile Name: Any Temperature Problem

Figure 99. Creating a Profile to Log All Temperature Alerts

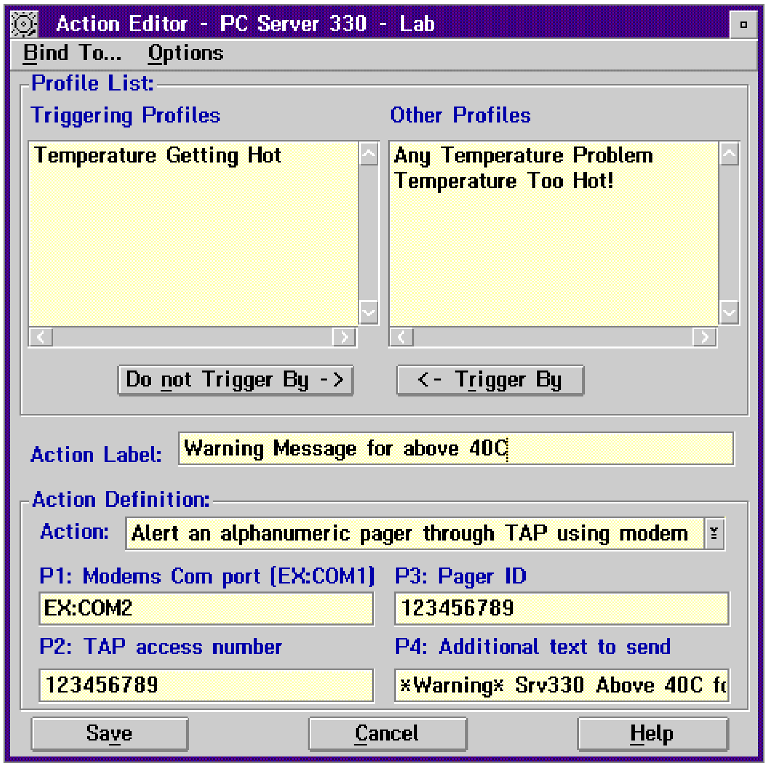
6.1.2.2 Configuring Alert Actions

Now that we have setup the profiles, we now need to set up the actions. The Action Editor enables the user to create and configure actions that the Alert Manager will take in response to specific alerts. It uses a series of user-defined Triggering Profiles like those we have set up to determine which alerts will trigger a defined action.

When it receives an alert, Alert Manager checks each of the alert conditions to see if it meets the specifications for a defined action. For this example we are only be using profiles.

1. Select the **Actions** button from the Alert Log window and then select **New**.
2. Select the menu option **Bind to...** → **Profiles** This allows us to select the predefined profile list and to select the action we want to use.
3. To configure an action to execute on a profile:
   - Select the Triggering Profiles you want the action to be triggered by as per Figure 100 on page 140.
   - Set an Action Definition.

     In this case we want to set the action to “Alert an alphanumeric pager through TAP using Modem.” See the online help and Chapter 2 of the *Netfinity Manager User's Guide* for more information.
   - Give the action a name by filling out the Action Label Box.
   - Save the defined action.



Profile List:

Triggering Profiles: Temperature Getting Hot

Other Profiles: Any Temperature Problem, Temperature Too Hot!

Action Label: Warning Message for above 40C

Action Definition:

Action: Alert an alphanumeric pager through TAP using modem

P1: Modems Com port [EX:COM1]: EX:COM2

P3: Pager ID: 123456789

P2: TAP access number: 123456789

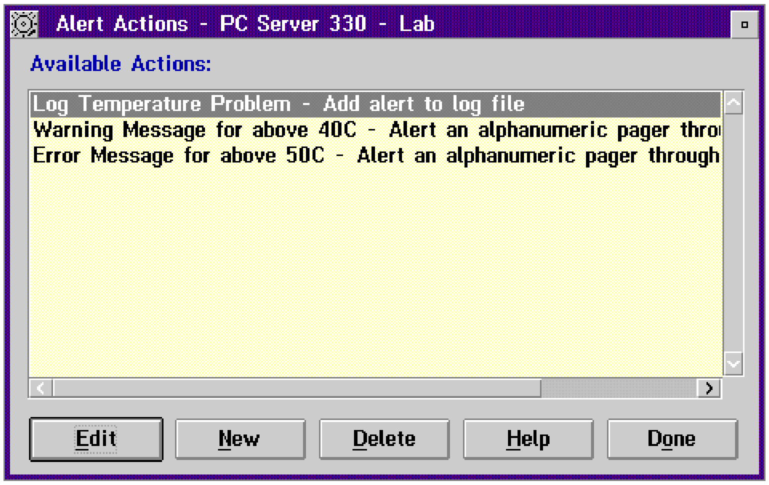
P4: Additional text to send: *Warning* Srv330 Above 40C fc

Figure 100. Profile Editor Setup for the 40°C setup

4. Set up the Triggering Profiles and Action Definition as shown in Figure 100 for the first profile.

5. Repeat for the 50°C profile but with a different description and text message to send.

6. Add a new action of Log to Temperature problem and set the action as “Add alert to log file.” Figure 101 shows the three profiles now bound to there actions.



Available Actions:

Log Temperature Problem - Add alert to log file
Warning Message for above 40C - Alert an alphanumeric pager thro
Error Message for above 50C - Alert an alphanumeric pager through

Figure 101. Alert Actions Defined

6.1.3 Summary

The server has now been configured to send alerts to the administrator's pager as the temperature rises. Table 17 shows the actions of the machine as the temperature rises.

Table 17. Temperature Thresholds

Threshold reached	**Action to Taken**
40°C	Alert from System Monitor is picked up by Alert Manager and two actions are preformed: 1. The alert is logged in the Alert Manager log. 2. Netfinity Manager dials out on COM2 and sends a warning text message to a pager.
50°C	Alert sent from System Monitor to the local system. This is picked up by Alert Manager and two actions are preformed: 1. The Netfinity Alert is logged in the Alert Manager Log. 2. Netfinity Manager dials out on COM2 and sends an Error text message to a pager.
64°C	The following actions are performed: 1. The Advanced Systems Management Adapter sends an alert to the local system with the Alert Text of System is over temperature. 2. The Netfinity Alert is logged in the Alert Manager Log. 3. The error is logged in the Advanced Systems Management Adapters own error log. 4. The system is powered off. 5. The Advanced Systems Management Adapter dials out to the predefined Pager after the machine has been powered off. **Note:** Netfinity Manager does not dial out as there is no time to make the connection before the machine will power off.

6.2 Example 2: Drive Failure in a RAID-5 Array

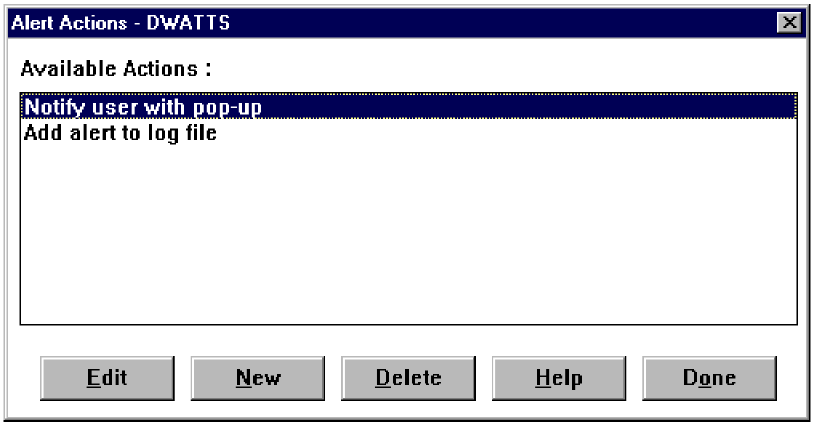
In this example, we have a Netfinity 3500 with Netfinity Manager installed. We have a ServeRAID II RAID adapter installed which connects a 3518 external enclosure containing a set of hot-swap drives to the server. An array is created with three RAID 5 logical drives defined. A single hot-spare drive is also configured.

The drive in the array fails and a rebuild using the hot-spare starts automaticaly. We want a message to be logged and displayed on the server itself as well as on the administrator's workstation.

We have an arrangement with the dealer that supplied the hardware to keep a stock of hard drives in case we need one, so we'd also like the dealer to be automatically notified of the failure so they can contact us to arrange to purchase a new drive from them (or replace it under warranty if the failure is covered).

6.2.1 Configuring the Scenario

By default, all severity 0-5 alerts are logged to the local machine and all severity 0-3 alerts are displayed as a pop-up on the local display. These actions are configured in Alert Manager:



Notify user with pop-up
Add alert to log file

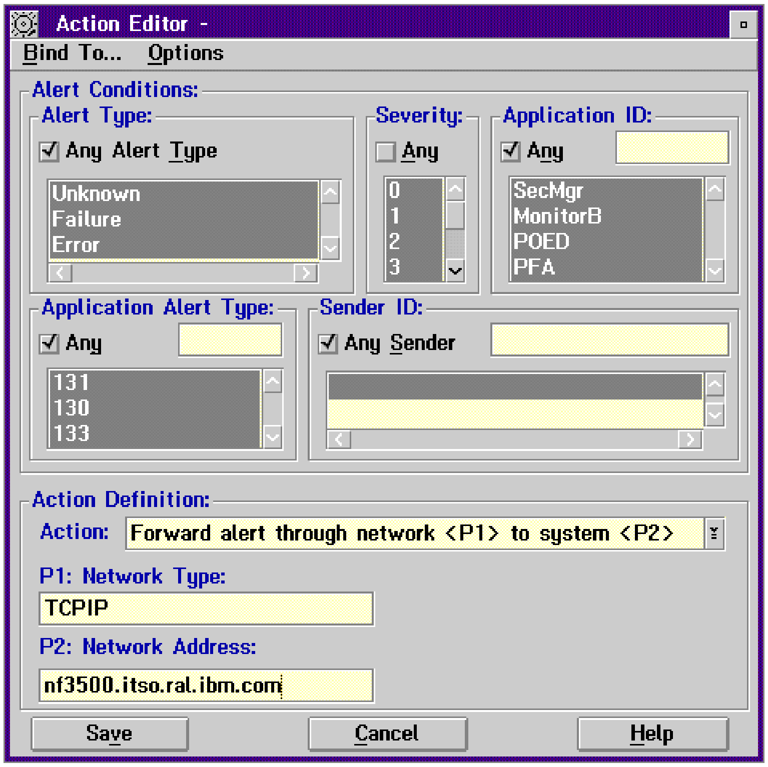
Figure 102. Standard Actions

We want to send all messages to the administrator's workstation so she is informed of all errors. We also want to send one message per failure to the dealer so they can contact us to replace it.

6.2.1.1 Notifying the Administrator

To notify the administrator, we set up an action to transmit all alerts to her workstation. To configure this action to happen on the alert conditions:

1. Open the **Alert Manager**.
2. Click on the **Action** button to display the existing actions.
3. Click on the **New** button to create a new action.
4. Setup the actions window as in Figure 103 on page 143.



Alert Type:
☑ Any Alert Type
Unknown
Failure
Error

Severity:
□ Any
0
1
2
3

Application ID:
☑ Any
SecMgr
MonitorB
POED
PFA

Application Alert Type:
☑ Any
131
130
133

Sender ID:
☑ Any Sender

Action: Forward alert through network <P1> to system <P2>

P1: Network Type:
TCPIP

P2: Network Address:
nf3500.itso.ral.ibm.com

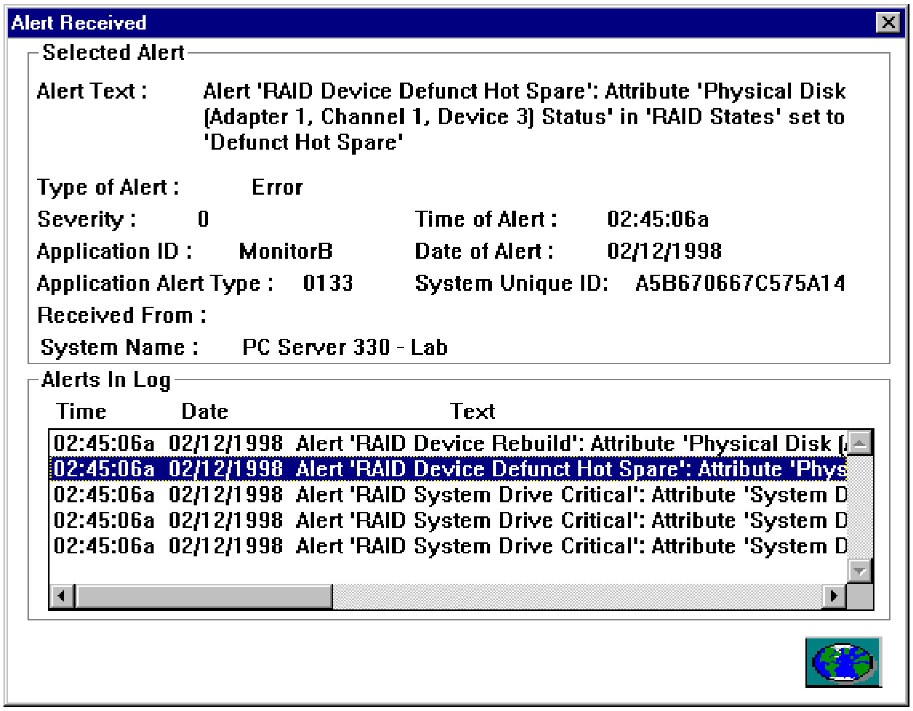
Figure 103. Configuring an Action to Send All Alerts to the Administrator

In our example, we only want to forward alerts of Sev 5 or higher. This will prevent “informational” messages being sent to her workstation.

5. Click on the **Save** button then **Yes** to save the action. The action now appears in the list.

6.2.1.2 Notifying the Dealer

We also want to inform the dealer of the drive failure, but during the course of the failure and recovery, many alerts are issued by the System Monitor service, as shown in Figure 104 on page 144.



Selected Alert

Alert Text : Alert 'RAID Device Defunct Hot Spare': Attribute 'Physical Disk [Adapter 1, Channel 1, Device 3] Status' in 'RAID States' set to 'Defunct Hot Spare'

Type of Alert : Error

Severity : 0

Time of Alert : 02:45:06a

Application ID : MonitorB

Date of Alert : 02/12/1998

Application Alert Type : 0133

System Unique ID: A5B670667C575A14

Received From :

System Name : PC Server 330 - Lab

Alerts In Log

```
Time      Date        Text
02:45:06a 02/12/1998  Alert 'RAID Device Rebuild': Attribute 'Physical Disk [
02:45:06a 02/12/1998  Alert 'RAID Device Defunct Hot Spare': Attribute 'Phys
02:45:06a 02/12/1998  Alert 'RAID System Drive Critical': Attribute 'System D
02:45:06a 02/12/1998  Alert 'RAID System Drive Critical': Attribute 'System D
02:45:06a 02/12/1998  Alert 'RAID System Drive Critical': Attribute 'System D
```

Figure 104. Alert Manager Pop-Up. An example of the pop-up messages when a drive fails in a RAID 5 array with one hot spare on a IBM ServeRAID card.

In our example, a total of five messages are sent to Alert Manager from System Monitor as a result of a drive failure in our RAID array:

- 3 messages, 1 from each logical drive, as each has now gone critical
- 1 message stating the rebuild process has started
- 1 message saying the failed drive has been marked as a “Defunct Hot Spare.”

We only want to transmit one alert to the dealer's machine for this event rather than all five. Likewise once the rebuild has completed we only want to sent one alert. As a result, we need to analyze all messages that are issued during the failure and rebuild processes to determine which are the best alerts to forward on.

As described in 2.4, “Alerts” on page 24, there are five values associated with every Netfinity Manager alert:

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

The alerts received locally when the drive failure occurs are shown in Table 18 on page 145.

Table 18. Alerts Received When a Drive Fails. Five alerts are received: three for each of the three logical drives going critical, one for the rebuild starting and one for the failed drive being set to a defunct hot spare.

Alert Message	Alert Type	Severity	Application ID	Application Alert Type
System Drive Critical	Warning	2	MonitorB	0131
System Drive Critical	Warning	2	MonitorB	0131
System Drive Critical	Warning	2	MonitorB	0131
Physical Drive Rebuild	Information	3	MonitorB	0136
Physical Drive Defunct Hot Spare	Error	0	MonitorB	0133

The alerts for a RAID-5 array once the rebuild has completed are shown in Table 19.

Table 19. Alert Details when Rebuild Has Completed. Four alerts are received: three for each logical drive returning online and one from the hot-spare becoming an online member of the array.

Alert Message	Alert Type	Severity	Application ID	Application Alert Type
System Drive Online	Information	3	MonitorB	0131
System Drive Online	Information	3	MonitorB	0131
System Drive Online	Information	3	MonitorB	0131
Physical Drive Online	Information	3	MonitorB	0130

If we now have a second drive failure without the protection of a hot-spare, the alerts are listed in Table 20.

Table 20. Second Failure Without a Hot-Spare

Alert Message	Alert Type	Severity	Application ID	Application Alert Type
System Drive Critical	Warning	2	MonitorB	0131
System Drive Critical	Warning	2	MonitorB	0131
System Drive Critical	Warning	2	MonitorB	0131
Physical Drive Defunct	Failure	0	MonitorB	0130

By looking at these tables, we can see that the alerts we want to notify the dealer with are all severity 0 “Failure” or “Error” alerts. We should therefore set up an alert condition based on the following values:

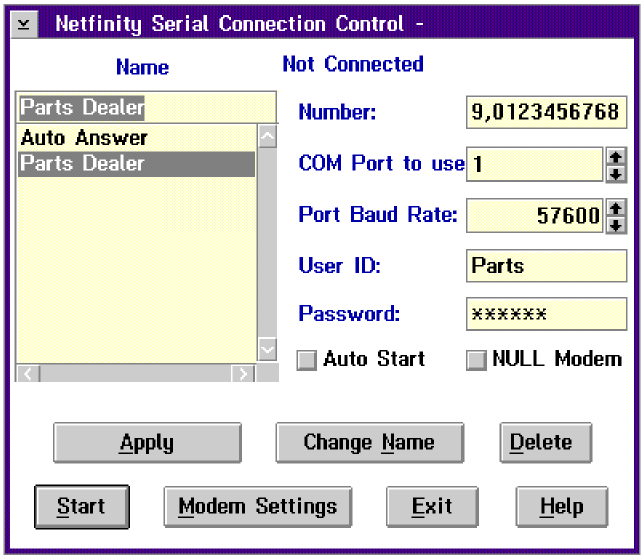
Type of Alert	Failure or Error
Severity	0
Application ID	MonitorB
Application Alert Type	0130 or 0133

We plan to dial out from the server to the dealer's Netfinity Manager machine. To do this we need to set up the Serial Control Manager.

To configure Serial Control follow these steps:

1. Double click on **Serial Control** from the main Netfinity Manager window.
2. You will see the a windows like in Figure 105 on page 146.

Serial Control is used to configure and dial a remote Netfinity Manager system. It is also used to set up a connection profile for use by Alert Manager.



Netfinity Serial Connection Control -

Name: Parts Dealer

Auto Answer
Parts Dealer

Not Connected

Number: 9,0123456768

COM Port to use 1

Port Baud Rate: 57600

User ID: Parts

Password: xxxxxx

□ Auto Start □ NULL Modem

Figure 105. Serial Control Setup

3. Fill out the connection name with any name you want. It is used by Alert Manager to specify the profile. It does not have to be the same name as the remote system you are dialing but will be the name that the local Netfinity Manager knows the system by.

4. Fill out the phone number, the COM port your modem is connected to and the port baud rate you will be connecting at. The port baud rate must be the same on the dealer's machine.

5. Fill out the userid and password that is defined on the dealer's Netfinity Manager Serial Control.

Security Implications

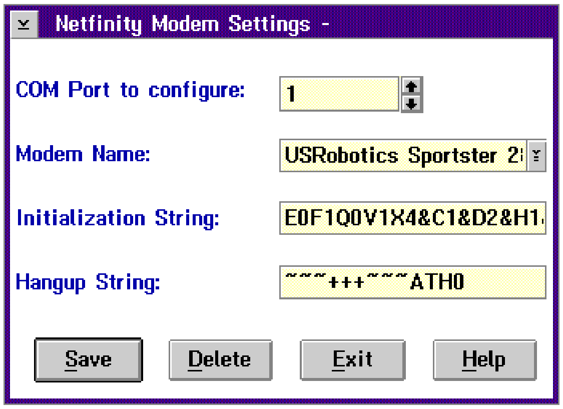
If you do not wish to let you dealer (or anyone else) dial into your server, you should prevent the Auto Answer connection from starting. To do this, highlight the **Auto Answer** connection, then click on **Auto Start** checkbox to deselect it.

At the dealer's Netfinity Manager system, Auto Answer must be enabled and the userid and password must be set. The dealer should also ensure that all access to Netfinity Manager functions is through specific userids and passwords. That is, all access through <PUBLIC> is removed.

Note: Userids and passwords are case sensitive.

6. Click on the **Apply** button to save the entry.

7. Configure your modem to a particular port by selecting **Modem Settings**. You will see a window like that in Figure 106 on page 147.


Netfinity Modem Settings -

COM Port to configure: 1

Modem Name: USRobotics Sportster 2

Initialization String: E0F1Q0V1X4&C1&D2&H1

Hangup String: ~~~+++~~~ATH0

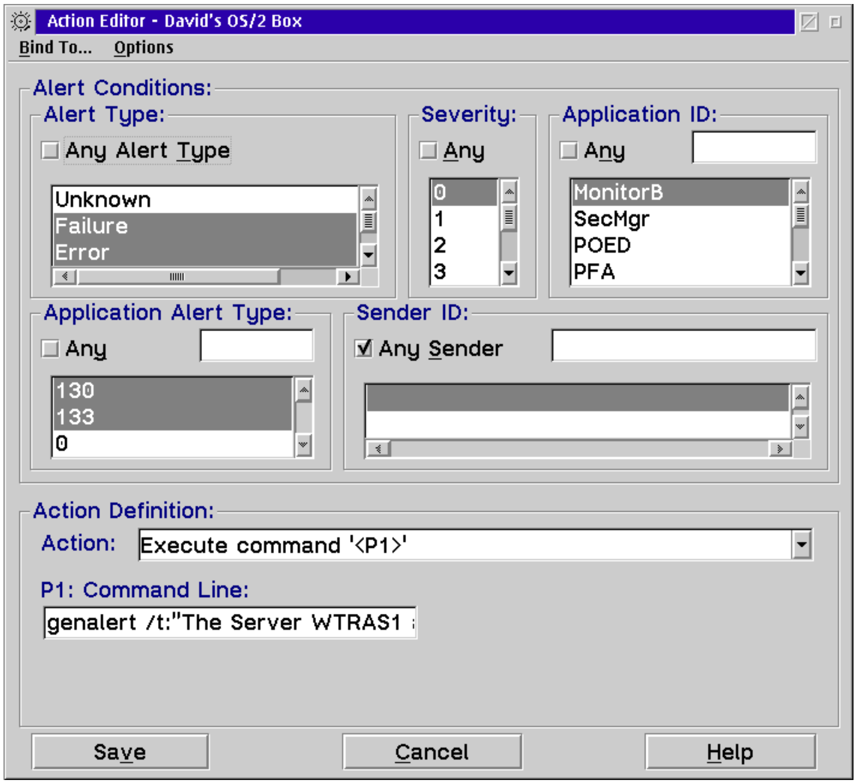
Figure 106. Serial Control Modem Settings

Here you can configure the modem attached to each COM port. Select the COM port then the modem or use the default and change the initialization and hang-up strings. Click on **Save** to save the modem configuration to the port displayed then **Exit** to leave the window.

8. Click on the **Exit** button to leave the Serial Control window. You will be given a warning message telling you that you need to save changes using the **Apply** button otherwise changes will be discarded.

Now we could just configure Alert Manager to send the Sev 0 Errors and Failures to the dealer via the modem we just defined. However, the messages that the dealer receives would be rather cryptic. Instead. We will process these Sev 0 errors and failure alerts by using Netfinity Manager's command-line interface to Alert Manager, GENALERT to create a more meaningful alert message which can be then forwarded to the dealer.

1. Open the **Alert Manager**.
2. Click on the **Action** button to display the existing actions.
3. Click on the **New** button to create a new action.
4. Setup the actions window as in Figure 107 on page 148. These correspond with the value we determined appropriate on Page 145.



Alert Conditions:

Alert Type: □ Any Alert Type
Unknown
Failure
Error

Severity: □ Any
0
1
2
3

Application ID: □ Any
MonitorB
SecMgr
POED
PFA

Application Alert Type: □ Any
130
133
0

Sender ID: ☑ Any Sender

Action Definition:

Action: Execute command '<P1>'

P1: Command Line: genalert /t:"The Server WTRAS1

Figure 107. Defining the Action to Build the Dealer Message

The action defined is to run a local program. In our example, we want to run the GENALERT program to generate an alert on the local system. The command we want to run is:

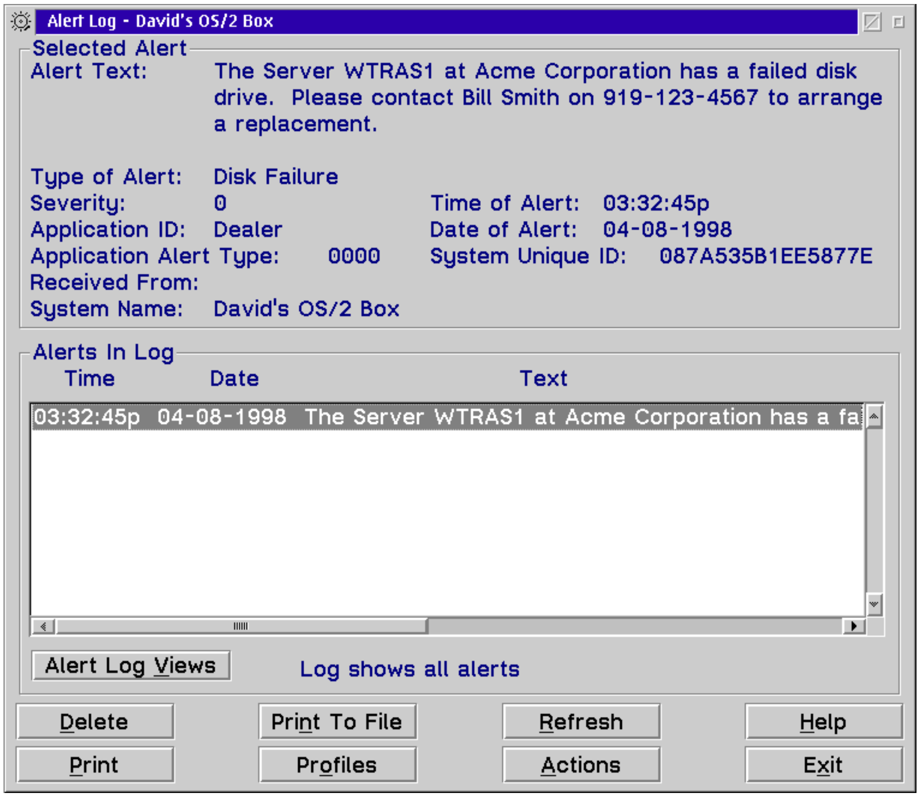
```
GENALERT /t:"The Server WTRAS1 at Acme Corporation has a failed disk
drive.  Please contact Bill Smith on 919-123-4567 to arrange a
replacement." /app:Dealer /sev:0 /type:dskflt
```

You can either put the GENALERT command in the Command Line field (as shown in Figure 107), or you can put the command in a batch file, and call the batch file instead.

If you want to know more about the syntax of GENALERT, type in `GENALERT` on the command line, or see “Alert Manager Command Line Operations” in Appendix G of *Netfinity Manager User's Guide*.

Note: We are actually defining a new Application ID, “Dealer” which we can then use in the next step. You need to run the above GENALERT command once to register the new Application ID in Alert Manager.

The alert that this generates is shown in Figure 108 on page 149



Selected Alert

Alert Text: The Server WTRAS1 at Acme Corporation has a failed disk drive. Please contact Bill Smith on 919-123-4567 to arrange a replacement.

Type of Alert: Disk Failure
Severity: 0
Time of Alert: 03:32:45p
Application ID: Dealer
Date of Alert: 04-08-1998
Application Alert Type: 0000
System Unique ID: 087A535B1EE5877E
Received From:
System Name: David's OS/2 Box

Alerts In Log

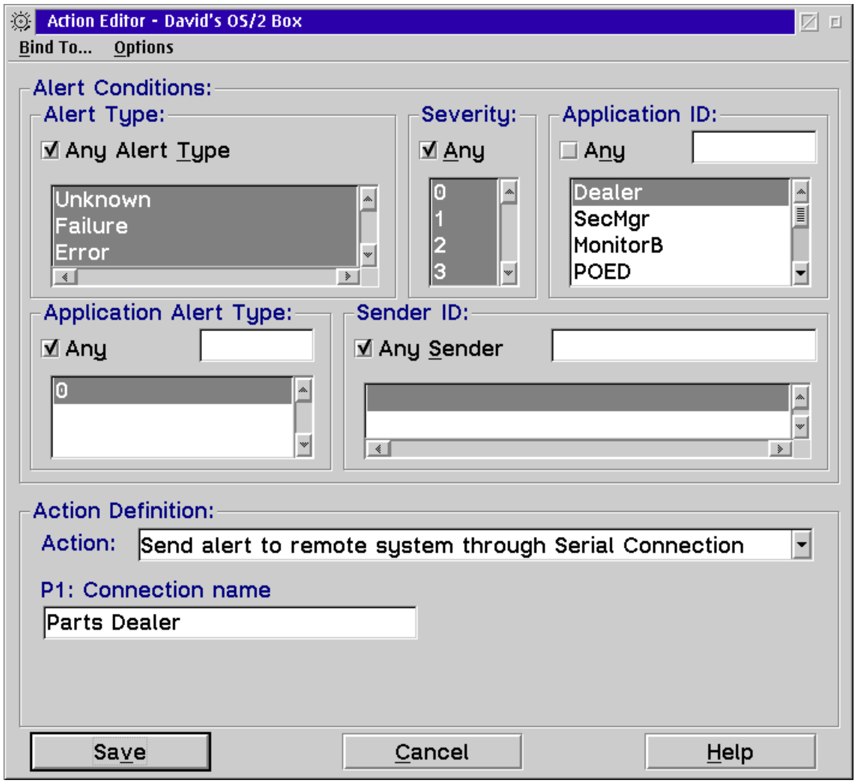
Time	Date	Text
03:32:45p	04-08-1998	The Server WTRAS1 at Acme Corporation has a fa

Log shows all alerts

Figure 108. Alert from GENALERT Command

5. Now you need to define an action based on Application ID “Dealer” to forward the alert to the dealer's Netfinity Manager machine.

   Set up a new action similar to Figure 109 on page 150



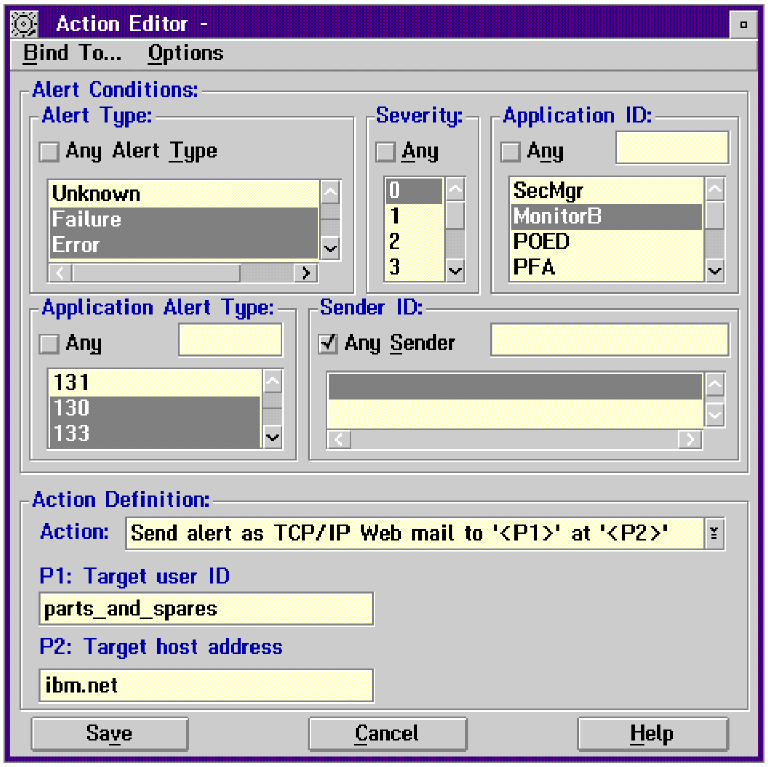
Action: Send alert to remote system through Serial Connection

P1: Connection name: Parts Dealer

Figure 109. Defining the Action to Send Alerts to the Dealer

You may not wish to use a modem to contact the dealer. An alternative would be to send email. Netfinity Manager offers a variety of email actions as described in Table 6 on page 33.

In our example, since our server is running OS/2 Warp Server and we have a connection to the internet via our LAN, we can use send mail using OS/2's standard SENDMAIL function. The action to do this is shown in Figure 110 on page 151.



Alert Conditions:

Alert Type: □ Any Alert Type
Unknown
Failure
Error

Severity: □ Any
0
1
2
3

Application ID: □ Any
SecMgr
MonitorB
POED
PFA

Application Alert Type: □ Any
131
130
133

Sender ID: ☑ Any Sender

Action Definition:

Action: Send alert as TCP/IP Web mail to '<P1>' at '<P2>'

P1: Target user ID
parts_and_spares

P2: Target host address
ibm.net

Figure 110. Sending Alerts to the Dealer using Email

6.2.2 Summary

The setup is now complete. When a drive fails, this is what will happen:

- The alerts are stored in Alert Manager's log both on the server and at the administrator's workstation.
- A pop-up box appears on the console both on the server and at the administrators workstation.
- The alert locally causes the dealers Netfinity Manager system to be dialed by the server and the alert routed to their machine.

6.3 Example 3: Power Failure

In this example, we discuss the situation when the power fails in the server room. We expect to get the following results:

- All the alerts will be sent to the administrator's workstation by Netfinity Manager
- The administrator will be paged at key times by Netfinity Manager
- The users will be notified by PowerChute every 5 minutes before the server shutdown sequence is started.
- The server will be safely shut down by PowerChute once the UPS reports low battery power.

In our example, we are using a Netfinity 3500 running Windows NT 4.0. The following are configured:

- An APC UPS is attached to COM2
- A modem is attached to COM1
- Netfinity Manager is installed
- PowerChute is installed
- PowerXtend is installed

Work at the Server

For our scenario, we are performing all steps locally at the server. We recommend you do the same.

6.3.1 Configuring the Server

Connect the UPS to the server, including the serial control interface. We suggest to use the server COM2 port for communicating with the UPS serial interface. If further assistance is needed to install the UPS, see the UPS documentation.

Connect the modem to the server. Use server COM1 port and ensure you can communicate the operating system with the modem. If further assistance is needed to install the modem, see the modem documentation.

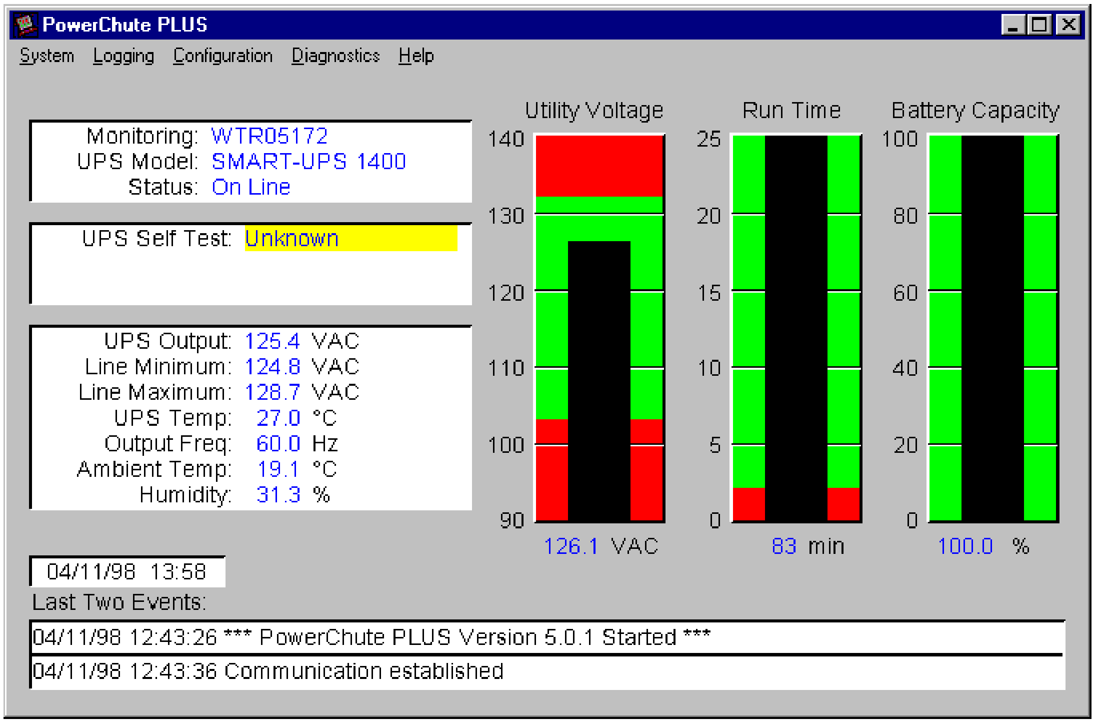
Install the necessary software on the server in the following order:

1. Netfinity Manager, as per 2.2, “Installing Netfinity Manager” on page 5
2. PowerChute, as per 2.5.1, “Installing PowerChute” on page 35
3. PowerXtend, as per 2.5.2, “Installing PowerXtend” on page 37

6.3.2 Configuring PowerChute

Once the software is installed, it is necessary to configure PowerChute to perform the necessary actions based on our scenario.

Start PowerChute. Select the locally attached UPS and click on **Attach**. The main window, Figure 111 on page 153 appears.



Monitoring: WTR05172
UPS Model: SMART-UPS 1400
Status: On Line

UPS Self Test: Unknown

UPS Output: 125.4 VAC
Line Minimum: 124.8 VAC
Line Maximum: 128.7 VAC
UPS Temp: 27.0 °C
Output Freq: 60.0 Hz
Ambient Temp: 19.1 °C
Humidity: 31.3 %

126.1 VAC
83 min
100.0 %

04/11/98 13:58

Last Two Events:

04/11/98 12:43:26 *** PowerChute PLUS Version 5.0.1 Started ***
04/11/98 12:43:36 Communication established

Figure 111. PowerChute Main Window

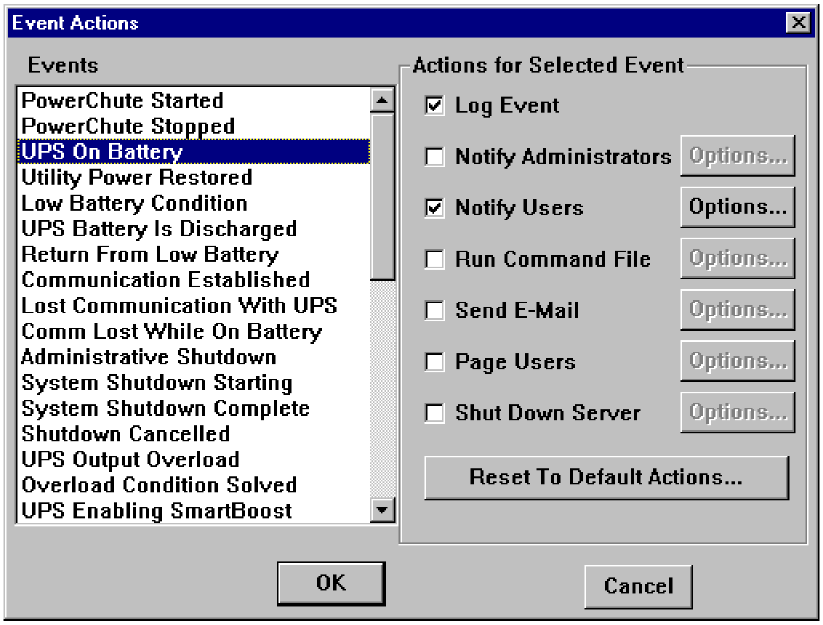
We need to configure the following events:

- UPS on Battery
- Low Battery Condition

6.3.2.1 Configuring “UPS On Battery”

Follow these steps to configure “UPS On Battery”:

1. Click on **Configuration** → **Event Actions**. Figure 112 appears.

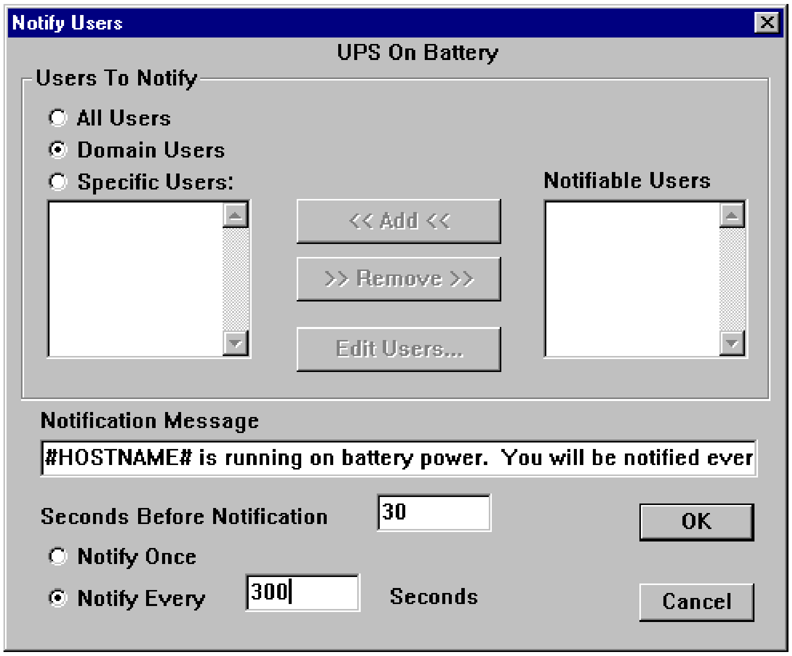


PowerChute Started
PowerChute Stopped
UPS On Battery
Utility Power Restored
Low Battery Condition
UPS Battery Is Discharged
Return From Low Battery
Communication Established
Lost Communication With UPS
Comm Lost While On Battery
Administrative Shutdown
System Shutdown Starting
System Shutdown Complete
Shutdown Cancelled
UPS Output Overload
Overload Condition Solved
UPS Enabling SmartBoost

☑ Log Event
☐ Notify Administrators
☑ Notify Users
☐ Run Command File
☐ Send E-Mail
☐ Page Users
☐ Shut Down Server

Figure 112. Configuring the UPS On Battery Event

2. Select **UPS On Battery**
3. Ensure check marks are on **Log Event** and **Notify Users** but not on the others, especially **Shut Down Server** which is checked by default.
4. Click on **Options** to the right of **Notify Users**. Figure 113 appears.



UPS On Battery

Users To Notify

○ All Users
● Domain Users
○ Specific Users:

Notification Message

#HOSTNAME# is running on battery power. You will be notified ever

Seconds Before Notification: 30

○ Notify Once
● Notify Every 300 Seconds

Figure 113. Setting the Options for “Notify Users”

We want all users logged onto the domain to receive a popup message from PowerChute when the server is running on battery. We want to wait 30 seconds before the first broadcast (in case someone just bumps the power cord) and then we want the users to be notified every 5 minutes (300 seconds).

5. Configure the notification as per Figure 113.
6. Tailor the message you want users to see as appropriate The message is limited to 128 characters. You can add variables to the message as listed in Table 21.

   Note: Variables must be used in uppercase.

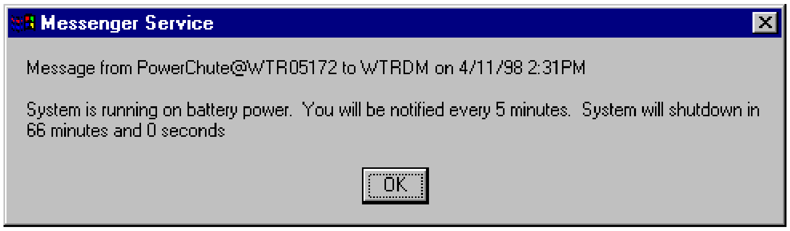
Table 21 (Page 1 of 2). Variables Available for User Messages

Variable	**Description**
#BATTERY_CAPACITY#	The battery capacity remaining in %
#CONTACT_NUMBER#	The Measure-UPS contact number
#HIGH_THRESHOLD#	The value of the high threshold
#HOSTNAME#	The name of the server
#LOW_THRESHOLD#	The value of the low threshold
#MAX_VOLTAGE#	The maximum reported voltage
#MIN_VOLTAGE#	The minimum reported voltage
#NORMAL_POSITION#	The normal operating position for the Measure-UPS contact

Table 21 (Page 2 of 2). Variables Available for User Messages

Variable	Description
#SHUTDOWN_DELAY#	The delay from the start of the shutdown process until the actual shutdown
#TIME_REMAINING#	The time until shutdown process starts in minutes and seconds
#USER_COMMENT#	The user-defined description for the Measure-UPS contact
Note: Note the following variables are only available when using APC Measure-UPS accessory: #CONTACT_NUMBER#, #NORMAL_POSITION#, and #USER_COMMENT#.	

In our example, when power fails, users will periodically see a message similar to Figure 114



Message from PowerChute@WTR05172 to WTRDM on 4/11/98 2:31PM

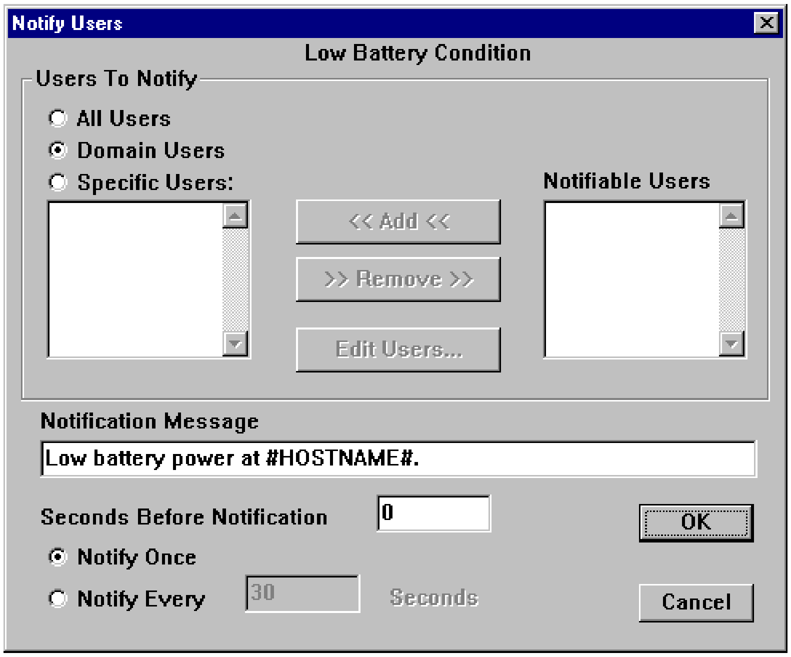
System is running on battery power. You will be notified every 5 minutes. System will shutdown in 66 minutes and 0 seconds

Figure 114. User Message when Power to the Server Fails

6.3.2.2 Configuring “Low Battery Condition”

Follow these steps to configure the “Low Battery Condition” event:

1. From the Event Actions window (Figure 112 on page 153), select the **Low Battery Condition** event.
2. Ensure check marks are on **Log Event**, **Notify Users** and **Shut Down Server** but not others.
3. Click on **Options** to the right of **Notify Users**. Figure 115 on page 156 appears.



Notify Users

Low Battery Condition

Users To Notify

○ All Users

● Domain Users

○ Specific Users:

Notifiable Users

Notification Message

Low battery power at #HOSTNAME#.

Seconds Before Notification 0

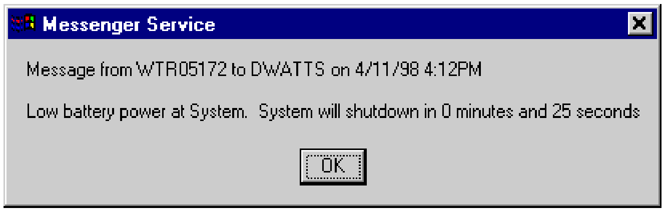
● Notify Once

○ Notify Every 30 Seconds

Figure 115. Setting the Options for “Notify Users”

4. We are leaving the default messages as is, but you may want to adjust it and any other settings.

   In our example, when batteries are about to run out, users will see a message similar to Figure 116



Messenger Service

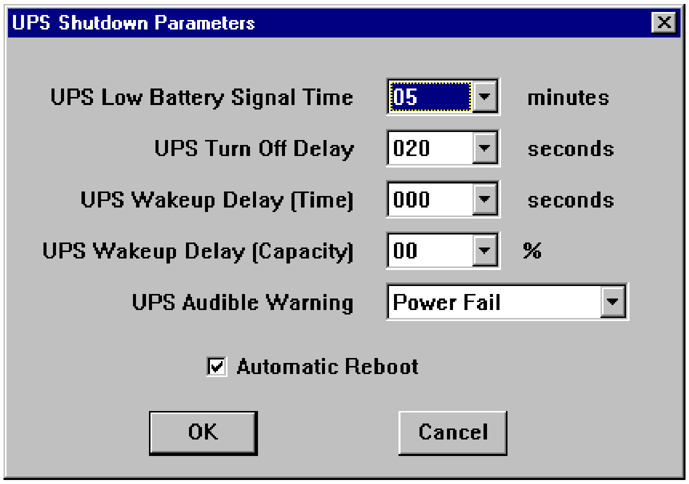
Message from WTR05172 to DWATTS on 4/11/98 4:12PM

Low battery power at System. System will shutdown in 0 minutes and 25 seconds

Figure 116. User Message When Shutdown Imminent

5. Specify when “Low Battery” is to occur.

   The time at which the Low Battery event will occur can be adjusted from the **Configuration → UPS Shutdown Parameters** window as shown in Figure 117 on page 157.



UPS Shutdown Parameters

UPS Low Battery Signal Time 05 minutes

UPS Turn Off Delay 020 seconds

UPS Wakeup Delay (Time) 000 seconds

UPS Wakeup Delay (Capacity) 00 %

UPS Audible Warning Power Fail

☑ Automatic Reboot

Figure 117. UPS Shutdown Parameters

6. Adjust the **UPS Low Battery Signal Time** to the point at which you want the event to occur. You should also adjust the **UPS Turn Off Delay** to a value greater than the normal time it takes to shut your server down.

   See Chapter 4 of the PowerChute User's Guide for details about the other options on this window. The guide is available on the ServerGuide ApplicationGuide 3A CD-ROM:

   ```
   \PWRCHUTE\EN\NTNOEXT\DOCS\MANUAL.PDF
   ```

6.3.3 Configuring Netfinity Manager

All alerts that occur in PowerChute are automatically routed locally to Netfinity Manager. All PowerChute alerts have an application ID of “PwrChute.”

We want to process these alerts in Netfinity Manager as follows:

- Transfer all PowerChute alerts to the administrator's workstation
- Page the administrator when power fails and the UPS is running on battery.
- Page the administrator when power is restored
- Page the administrator when the system is about to shutdown due to the battery draining.

Each of these is done through Alert Manager:

1. Open **Alert Manager**
2. Click on **Actions**
3. For each of the four actions we want, click on **New** and fill in the Action Editor as per Table 22 on page 158. Figure 118 on page 158 shows the settings for the first action, to transfer all alerts to the administrator's workstation:

Table 22. Actions to Set Up

	Type	Severity	App ID	App Type	Sender
Transfer All	Any	Any	PwrChute	Any	Any
Pager on Battery	Any	Any	PwrChute	2000	Any
Pager on Restore	Any	Any	PwrChute	1003	Any
Pager on Shutdown	Any	Any	PwrChute	2003	Any

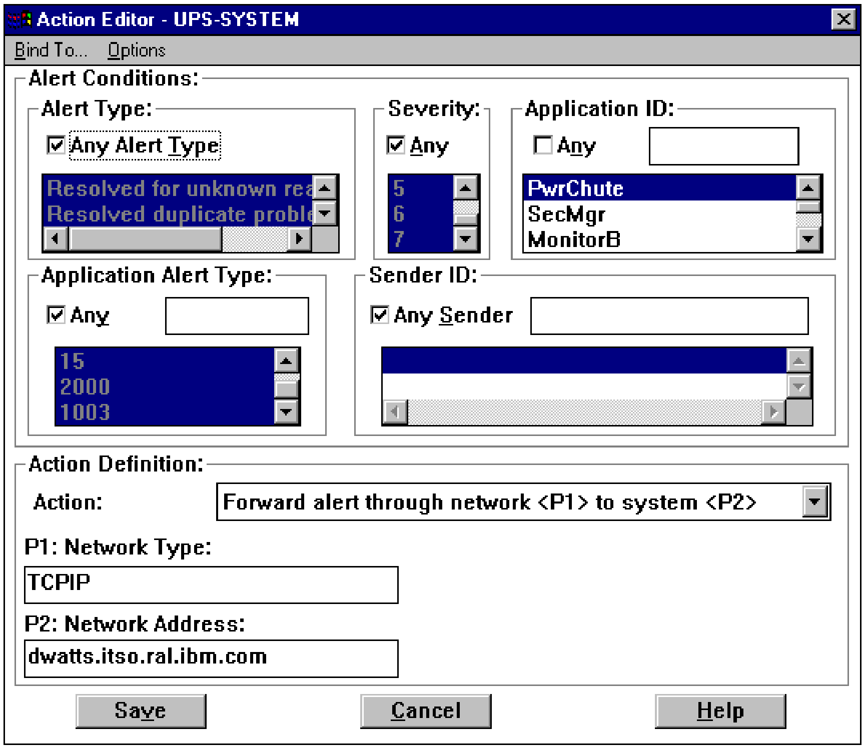
Refer to Table 7 on page 42 for a list of all Application Alert Types.

Tip

You might also want to page the administrator when any of the following occur:

- Communication with the UPS is lost (Application Type 3000)
- Communication with the UPS is re-established (1002).
- UPS Battery Failure (3016)

See Table 7 on page 42 for other types.



Alert Conditions:

Alert Type: ☑ Any Alert Type
Resolved for unknown rea
Resolved duplicate probl

Severity: ☑ Any
5
6
7

Application ID: ☐ Any
PwrChute
SecMgr
MonitorB

Application Alert Type: ☑ Any
15
2000
1003

Sender ID: ☑ Any Sender

Action Definition:

Action: Forward alert through network <P1> to system <P2>

P1: Network Type:
TCPIP

P2: Network Address:
dwatts.itso.ral.ibm.com

Figure 118. Transferring All Alerts to the Administrator's Workstation

4. Click on **Save** to save each of the actions.

6.3.4 Summary

We've now configured PowerChute and Netfinity Manager to alert the users and the administrator when power fails.

There are many other components in PowerChute you might want to consider setting. For example, by default, users will get a variety of other messages from PowerChute which you may not want them to be concerned with. There are also a number of other items in the Configuration pull-down menu that are worth examining. See Chapter 4 of the PowerChute User's Guide for explanations. * Example of Power Supply Failure

6.4 Example 4: Power Supply Failure on Netfinity 7000 Server

This example shows you how to set up an alert when a power supply fails on a Netfinity 7000 server. In this scenario, we use the Advanced Systems Management Adapter to alert the administrator since the system may have shut down preventing the local Netfinity Manager from sending the alert.

We will configure the adapter to dial-out to a remote Netfinity Manager system when a power supply fails, and forward the alert to it for further processing.

Note: The power supply failure alerts are only supported on Netfinity servers with redundant power supplies.

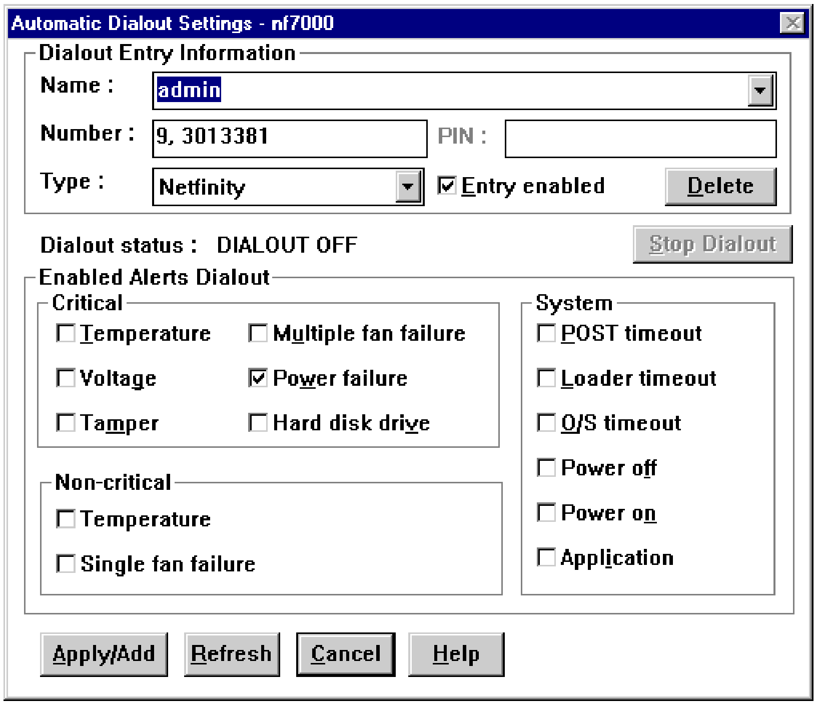
On a Netfinity 7000 Server, redundant power supply is only achieved with three power supplies active. If one power supply fails, the remaining two are sufficient enough to keep the server alive.

If two power supplies fail, leaving only one power supply active, a Netfinity 7000 server with 12 4.5 GB hard drives will stay up for approximately two minutes before the operating system shuts down and the server powers off.

If all power supplies fail on the Netfinity 7000, no alert will be issued by the Advanced Systems Management Adapter as there is no power source available to dial out — the external power supply option is not supported on the Netfinity 7000. In this instance, we recommend you use Netfinity Manager's Remote System Manager on another machine to monitor the server and notify the administrator when it becomes offline.

6.4.1 Service Processor Settings

In order to forward a dial-out alert, you need to configure you Service Processor. Use Automatic Dialout Settings to enable dial-out alerts you want to be send to your remote system.



Automatic Dialout Settings - nf7000

Dialout Entry Information

Name : admin

Number : 9, 3013381 PIN :

Type : Netfinity ☑ Entry enabled Delete

Dialout status : DIALOUT OFF Stop Dialout

Enabled Alerts Dialout

Critical

□ Temperature □ Multiple fan failure

□ Voltage ☑ Power failure

□ Tamper □ Hard disk drive

Non-critical

□ Temperature

□ Single fan failure

System

□ POST timeout

□ Loader timeout

□ O/S timeout

□ Power off

□ Power on

□ Application

Apply/Add Refresh Cancel Help

Figure 119. Service Processor Dial-out setting for Power Failure

Figure 119 shows the Automatic Dialout Setting window. See 3.2.4, “Automatic Dialout Settings” on page 79 for details of this window.

Here, we want the Service Processor to dial out on a power failure, so we selected **Power failure** as the only alert to be sent out. You may want to select other alerts for your system. To set up your Service Processor, perform the following:

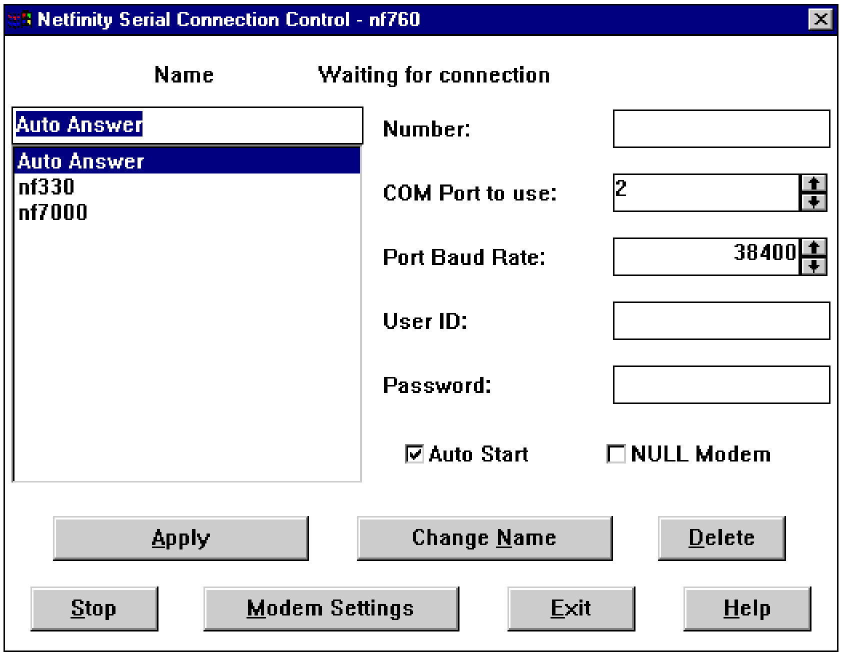
1. Open **Netfinity Manager** → **Service Processor** → **Automatic Dialout Settings**
2. Enter a name and phone number.
3. Select the type of alert that will be send out. We are dialing a remote Netfinity Manager system, so we've selected **Netfinity**. Other options are numeric and alphanumeric pagers.
4. Check the **Entry enabled** box.
5. Check any box for other alerts you want forwarded.
6. Click on **Apply/Add** to store the settings.

The remote Netfinity Manager system that will receive the call needs to be in Auto Answer mode. To set your remote system to Auto Answer mode, do the following:

1. Open **Netfinity Manager** → **Serial Control**.
2. Select **Auto Answer** and click on **Start**.

Figure 120 on page 162 shows a system in Auto Answer mode.

Note: If you select the **Auto Start** box the system will automatically be in Auto Answer mode after every re-boot. In Auto answer mode, the modem is unavailable to any other program such as HyperTerminal.


Netfinity Serial Connection Control - nf760

Name: Auto Answer

Waiting for connection

Auto Answer
nf330
nf7000

Number:

COM Port to use: 2

Port Baud Rate: 38400

User ID:

Password:

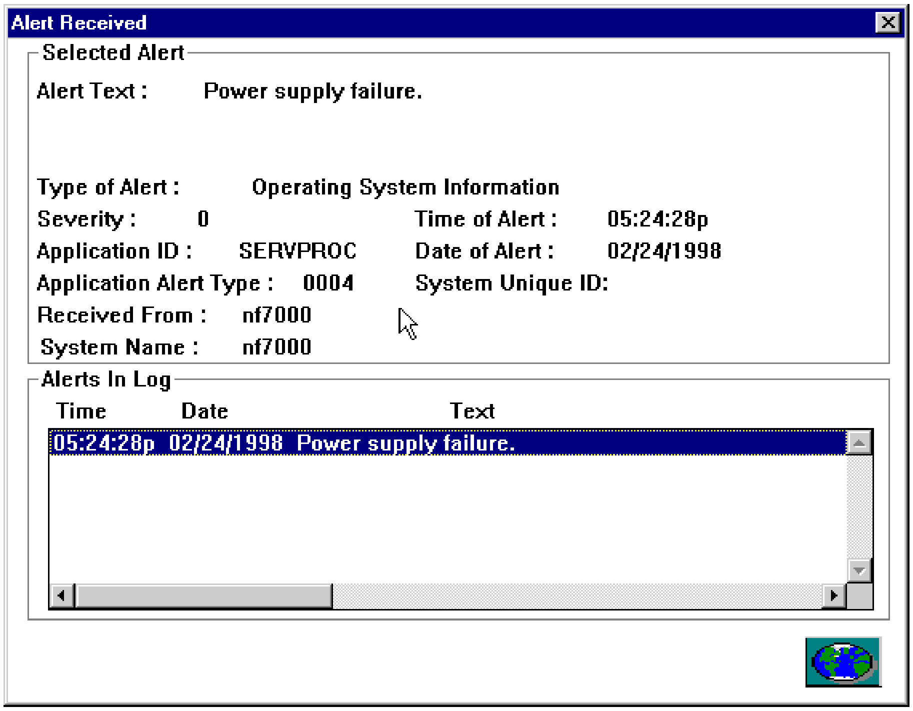
☑ Auto Start ☐ NULL Modem

Figure 120. Netfinity Manager Serial Control in Auto Answer Mode

6.4.2 Receiving the Alert

The Service Processor will poll the power supplies every 90 seconds or so. In case a power supply fails, the Service Processor will attempt to forward an alert to all enabled dial-out entries. As we specified the recipient to be a Netfinity Manager system, it will receive a standard alert similar to Figure 121 on page 163

The administrator can then configure further actions to occur based on that alert as necessary.



Alert Text : Power supply failure.

Type of Alert : Operating System Information

Severity : 0

Time of Alert : 05:24:28p

Application ID : SERVPROC

Date of Alert : 02/24/1998

Application Alert Type : 0004

System Unique ID:

Received From : nf7000

System Name : nf7000

```
Time        Date        Text
05:24:28p  02/24/1998  Power supply failure.
```

Figure 121. Service Processor Power Supply Failure pop-up Message

6.5 Example 5: Operating System Timeout

This example describes how to set up the Service Processor to generate a dial-out alert in the event of Operating System (OS) timeout.

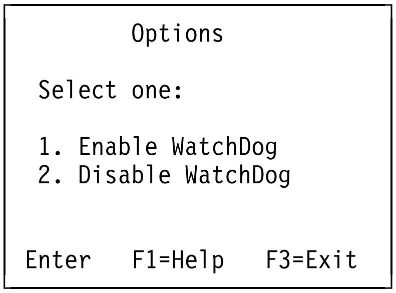
If your server's operating system traps, abends or hangs, the Service Processor will attempt to restart the server and forward an alert message to a remote system. You need to follow these steps to set up your Service Processor to do this.

1. Enable the OS Watchdog Timer with the Configuration diskette
2. Set the OS Timeout value in Service Processor Manager
3. Create a dial-out entry in Service Processor Manager

6.5.1 Enable the OS Watchdog

Before you can configure the OS Watchdog, you must first enable it. If it as been previously enabled, you can skip this step.

1. Boot from the Advanced Systems Management Adapter Configuration Diskette
2. from the main menu, select **5. Configure OS WatchDog Timer** You will then see the following window



```
         Options

  Select one:

  1. Enable WatchDog
  2. Disable WatchDog


 Enter   F1=Help   F3=Exit
```

3. Select **Enable WatchDog** and press Enter.
4. Once the configuration has been updated, press F3 to exit the Configuration program.
5. Power off the server, then back on again.

6.5.2 Configure the OS WatchDog

You now need to configure the OS WatchDog in the Service Processor Manager in Netfinity Manager

1. Start Netfinity Manager
2. Double click on **Service Processor**. The Service Processor Manager window Figure 122 on page 165 appears.

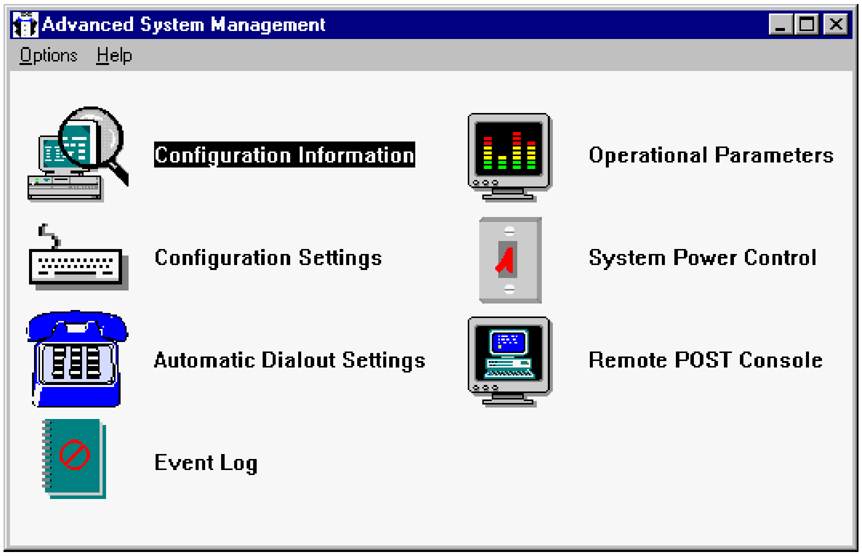
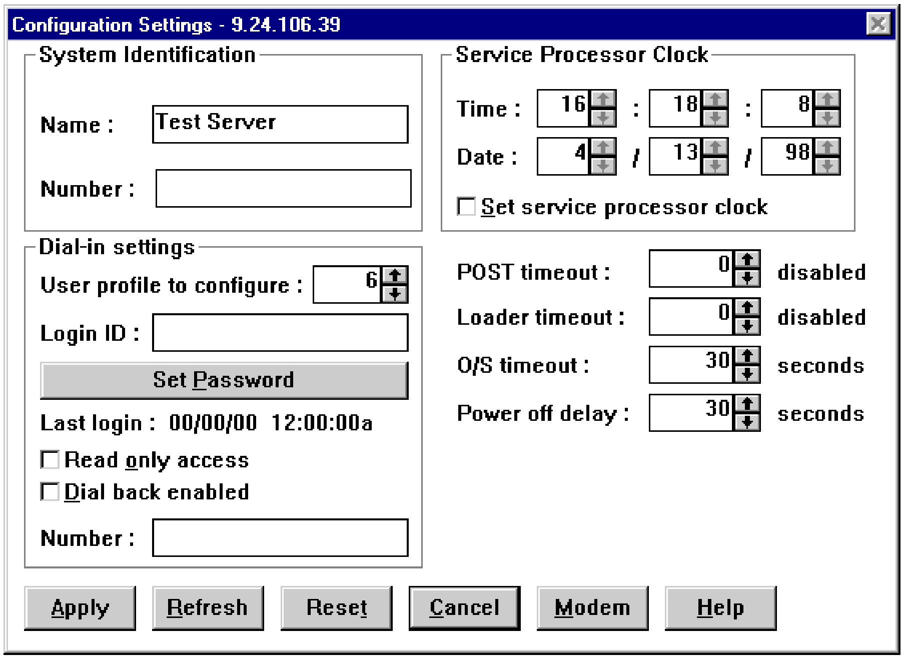


Figure 122. Service Processor Manager Window

3. Double click on **Configuration Settings**. Figure 123 appears.


Configuration Settings - 9.24.106.39

System Identification

Name : Test Server

Number :

Service Processor Clock

Time : 16 : 18 : 8

Date : 4 / 13 / 98

□ Set service processor clock

Dial-in settings

User profile to configure : 6

Login ID :

Last login : 00/00/00 12:00:00a

□ Read only access

□ Dial back enabled

Number :

POST timeout : 0 disabled

Loader timeout : 0 disabled

O/S timeout : 30 seconds

Power off delay : 30 seconds

Figure 123. Configuration Settings

4. Enter a value in the **O/S timeout** field.

   This is the number of seconds that the Service Processor will allow for the system's operating system to stop responding before generating a O/S Timeout event. Since we have enabled the watchdog timer, if the OS takes longer than the configured amount of time to respond, the Service Processor will attempt to restart the system.

   The number you set here depends on the applications you are using. If you have applications such as databases that are sufficiently CPU intensive, they could prevent the WatchDog from confirming the status of the system. In this situation, you should increase this value. Running your system in test with the Watchdog timer enabled will confirm if you have set the value sufficiently high to prevent unnecessary restarts.

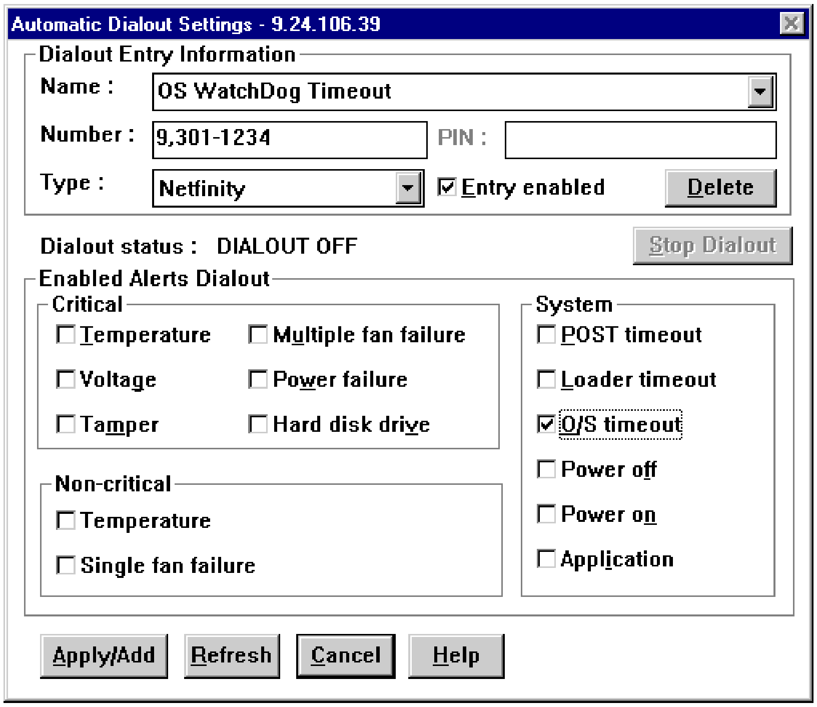
See 3.2.2, “Configuration Settings” on page 73 for information about the rest of this window.

5. Click on **Apply** then **Cancel** to close the window.

6.5.3 Configuring a Dial-Out Entry

Now that the Advanced Systems Management Adapter has been configured to issue an alert when the OS WatchDog Timer expires, we want to configure the card to send an alert to a remote Netfinity Manager system via the attached modem.

1. From the Service Processor Manager window, double click on **Automatic Dialout Settings**. Figure 124 appears.



Automatic Dialout Settings - 9.24.106.39

Dialout Entry Information

Name : OS WatchDog Timeout

Number : 9,301-1234 PIN :

Type : Netfinity ☑ Entry enabled

Dialout status : DIALOUT OFF

Enabled Alerts Dialout

Critical

□ Temperature □ Multiple fan failure

□ Voltage □ Power failure

□ Tamper □ Hard disk drive

Non-critical

□ Temperature

□ Single fan failure

System

□ POST timeout

□ Loader timeout

☑ O/S timeout

□ Power off

□ Power on

□ Application

Figure 124. Automatic Dialout Settings

2. Type in a phone number and a descriptive name

3. Select **Netfinity** from the Type field to specify that the number to call will be answered by Netfinity Manager

4. Click **O/S timeout** and any other alerts you wish to cause this number to be called.

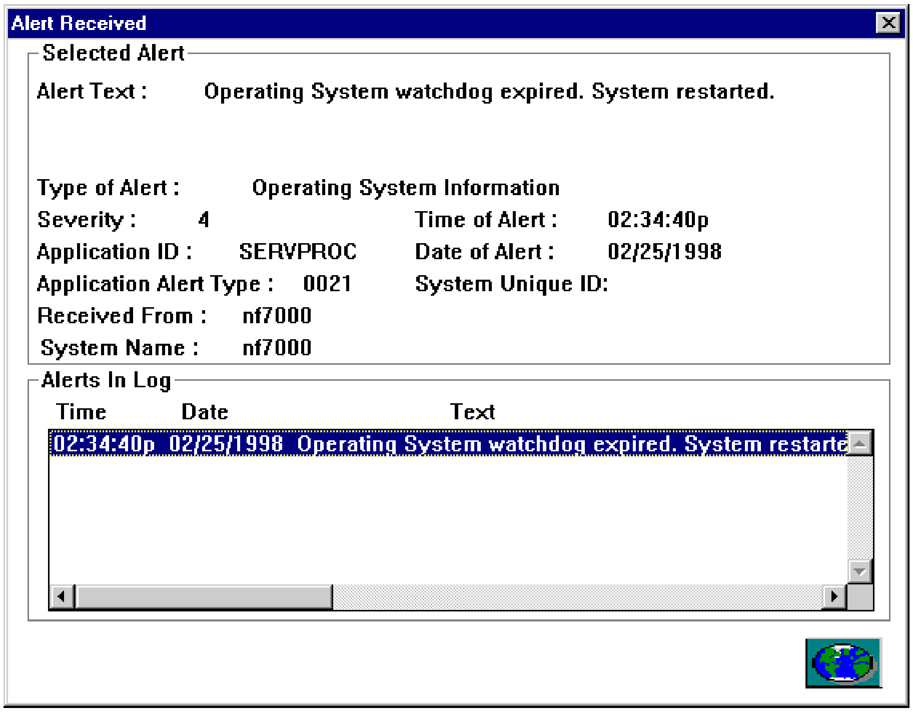
5. Click on **Apply/Add** to add the entry then **Close** to exit the window.

For more information about this window see 3.2.4, “Automatic Dialout Settings” on page 79.

6.5.4 Running the Scenario

The Service Processor monitors the Operating System and the CPU. The watchdog process sends queries to the system kernel and CPU about its status. If the Operating System traps, hangs or abends these queries are not being answered and the Service Processor assumes an operating system timeout.

If this happens, the watchdog process will wait for the amount of time you selected in OS timeout and initiate a system restart. A message as seen in Figure 125 will be forwarded to the remote Netfinity Manager system.



Alert Text : Operating System watchdog expired. System restarted.

Type of Alert : Operating System Information
Severity : 4
Time of Alert : 02:34:40p
Application ID : SERVPROC
Date of Alert : 02/25/1998
Application Alert Type : 0021
System Unique ID:
Received From : nf7000
System Name : nf7000

Time	Date	Text
02:34:40p	02/25/1998	Operating System watchdog expired. System restarte

Figure 125. Service Processor OS Timeout Alert

You could then process the alert as follows:

- send a message via network messaging to all users logged onto the domain informing them of the restarted server.
- notify the administrator so they can ensure the server restarted correctly.

6.6 Example 6: POST Timeout and Remote POST Console

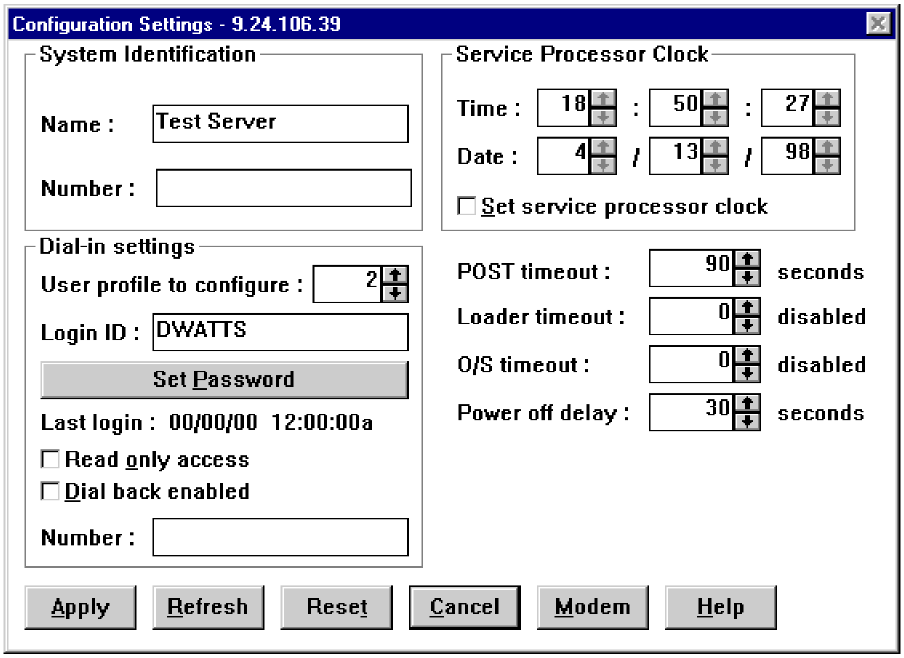
In this scenario, we have a Server 330 and we want to be notified when the POST process takes too long to complete. Upon notification, we will use the Advanced Systems Management Adapter's Remote POST Console to remotely watch the POST to determine where the problem lies.

Note: The POST timeout function is currently only available on the Server 325 and Server 330. The Remote POST Console is currently only available on the Server 325, Server 330 and Netfinity 7000.

6.6.1 Configuring the POST Timeout

Follow these steps to configure your Service Processor for POST Timeout

1. From Netfinity Manager, start the Service Processor Manager
2. Open Configuration Settings. Figure 126 appears.



Configuration Settings - 9.24.106.39

System Identification

Name : Test Server

Number :

Service Processor Clock

Time : 18 : 50 : 27

Date : 4 / 13 / 98

□ Set service processor clock

Dial-in settings

User profile to configure : 2

Login ID : DWATTS

Last login : 00/00/00 12:00:00a

□ Read only access

□ Dial back enabled

Number :

POST timeout : 90 seconds

Loader timeout : 0 disabled

O/S timeout : 0 disabled

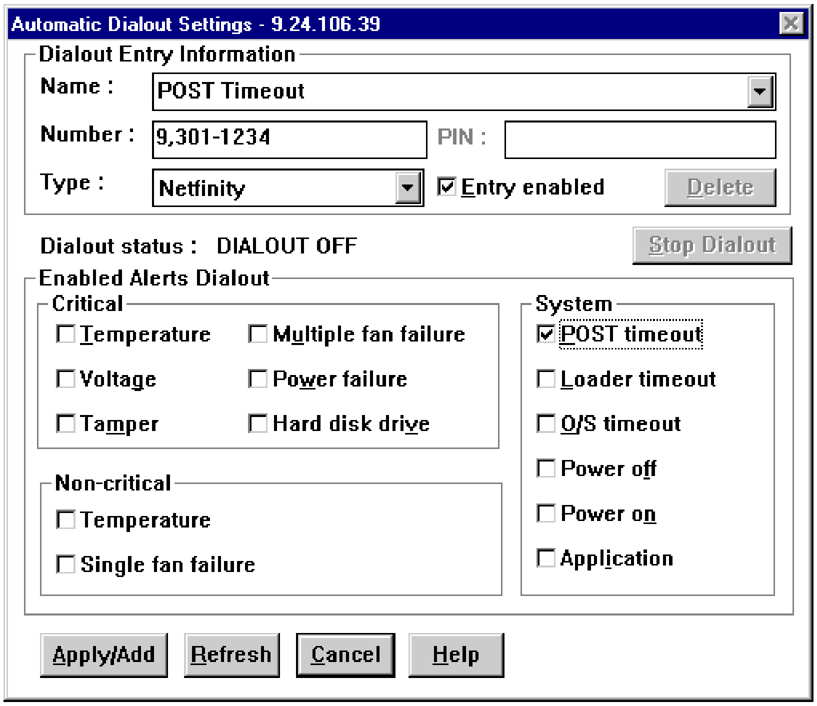
Power off delay : 30 seconds

Figure 126. Service Processor Configuration Settings

3. Select a time value for POST timeout that is greater than the time it normally takes your server to complete POST.
4. Click on **Apply**.

Now, you want to configure the Advanced Systems Management Adapter to dial-out with a Netfinity Manager alert when the POST timeout occurs.

1. Open **Automatic Dialout Settings** Figure 127 on page 169 appears.



Name : POST Timeout

Number : 9,301-1234 PIN :

Type : Netfinity ☑ Entry enabled

Dialout status : DIALOUT OFF

Critical: □ Temperature □ Multiple fan failure □ Voltage □ Power failure □ Tamper □ Hard disk drive

Non-critical: □ Temperature □ Single fan failure

System: ☑ POST timeout □ Loader timeout □ O/S timeout □ Power off □ Power on □ Application

Figure 127. Service Processor Automatic Dialout Settings

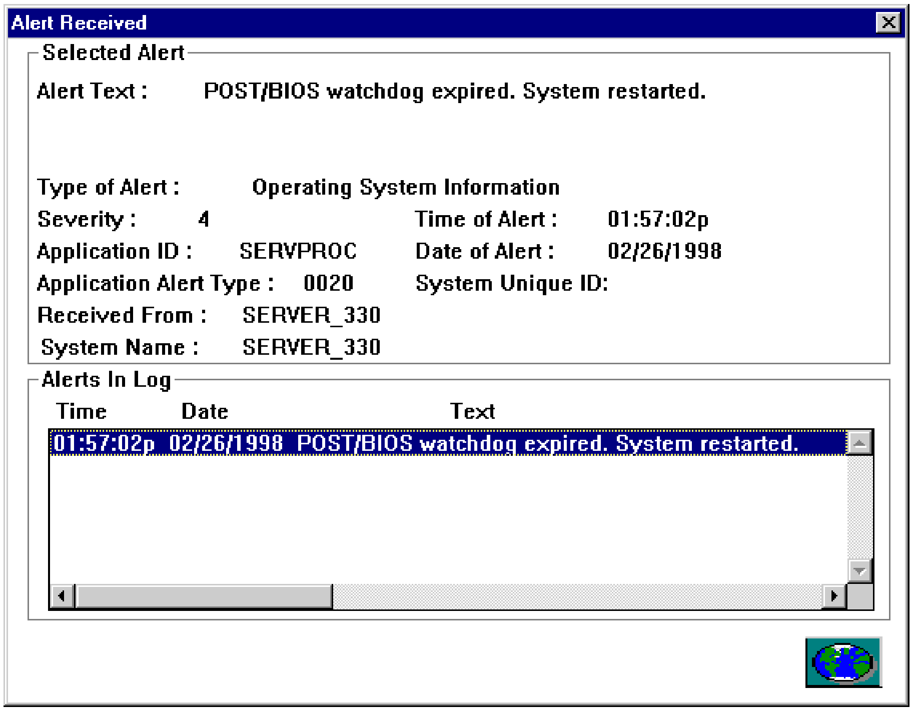
2. Enter a phone number and set the Type to **Netfinity**
3. Put a checkmark in **Entry enabled**
4. Put a checkmark in **POST timeout**
5. Adjust any other settings.
6. Click on **Apply/Add** to save the settings and then **Cancel** to close the window.

See 3.2.4, “Automatic Dialout Settings” on page 79 for details on other settings in this window.

Your system is now set to monitor the POST for timeout.

6.6.2 What Happens

The Service Processor monitors the system start up process. It will measure the POST time and compare with the value you set in the Configuration Settings window. If the time for POST takes longer, the Service Processor assumes the system experienced a problem and attempts to restart the system. Simultaneously, it will forward an alert your remote system. Figure 128 on page 170 shows an example of a POST timeout alert.



Alert Received

Selected Alert

Alert Text : POST/BIOS watchdog expired. System restarted.

Type of Alert : Operating System Information

Severity : 4

Time of Alert : 01:57:02p

Application ID : SERVPROC

Date of Alert : 02/26/1998

Application Alert Type : 0020

System Unique ID:

Received From : SERVER_330

System Name : SERVER_330

Alerts In Log

Time	Date	Text
01:57:02p	02/26/1998	POST/BIOS watchdog expired. System restarted.

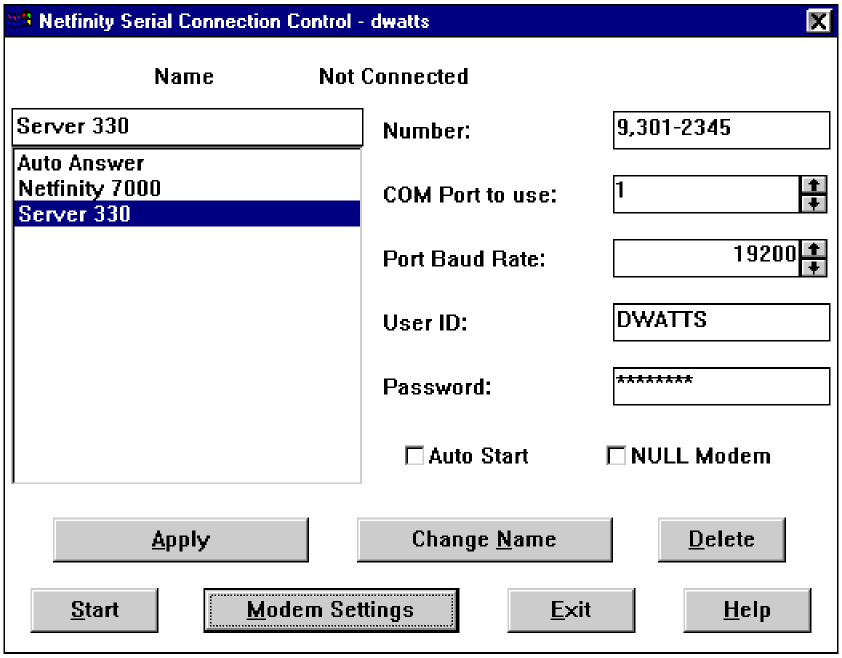
Figure 128. Service Processor POST timeout Alert

6.6.3 Using the Remote POST Console

The Service Processor has the ability to redirect the POST through the adapter and serial link to a remote system. The Remote POST Console is a full functioning mirror of the actual system. If you have a Server 325 or Server 330, you can also run diagnostics.

In order to run Remote POST Console, you need to connect to remote system via a serial link, either dial-in or with a null modem cable. Follow these steps to set up a connection.

1. If you have not done so already, create a new entry in Serial Control Manager in Netfinity Manager as per Figure 129 on page 171.



Netfinity Serial Connection Control - dwatts

Name: Server 330 — Not Connected

Auto Answer
Netfinity 7000
Server 330

Number: 9,301-2345

COM Port to use: 1

Port Baud Rate: 19200

User ID: DWATTS

Password: ********

□ Auto Start □ NULL Modem

Figure 129. Configuring a Serial Connection

2. Save your new entry by clicking on **Apply**

   The user ID and password you set here must match the one set in the Dial-In settings in the Configuration Settings window of the Service Processor as shown in Figure 126 on page 168.

3. Close Serial Control and open Service Processor.

4. From the menu bar select **Connect** as shown in Figure 130

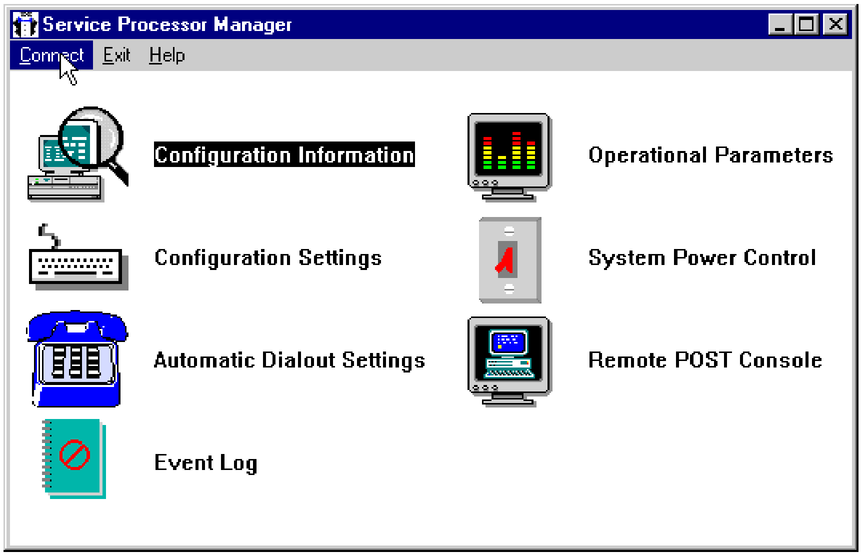


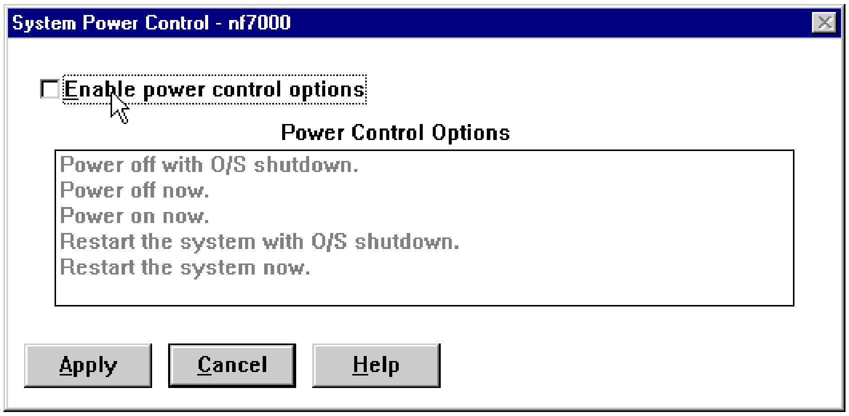
Figure 130. Connecting to a Remote Service Processor

5. Select your dial-out entry for the server you want to examine.

6. Click on **Start**.

7. Wait until you are connected, then click on **Exit**.

8. Open the **Operational Parameters** appears. window and check the **System power status** field.
9. Press **Cancel** and open the **System Power Control** window. Figure 131 appears.


System Power Control - nf7000

□ Enable power control options

Power Control Options

Power off with O/S shutdown.
Power off now.
Power on now.
Restart the system with O/S shutdown.
Restart the system now.

Figure 131. Service Processor System Power Control

10. Check **Enable power control options** and select **Power off now** or **Power off with OS shutdown**.
11. Click on **Apply**.
12. Open the **Operational Parameters** window again and check System power status. Wait until the System power status changes to OFF.
13. Click **Cancel** and open Remote POST Console.
14. Leaving the Remote POST Console window open, open the **System Power Control** window.
15. Enable power control and select **Power on now**
16. Click **Apply** and then **Cancel**.
17. Return focus to the Remote POST Console window.

You now can proceed as if you were sitting in front of the server. In the title bar, you will see information about POST status such as `POST has started` or `POST finished`.

Once POST has finished, you can replay the POST using the Replay option from the menu bar. In order to do so you need to disconnect form the remote Service Processor.

6.7 Example 7: Application Failure and Restart

You can use Netfinity Manager to monitor processes through Process Manager. If the process stops or starts, you can configure Process Manager to send an alert. Based on the alert you can perform the standard set of actions including running a program. This means you can use Netfinity Manager to automatically restart an application when it fails.

In this example, we have set up a server running Adobe Acrobat Distiller, a program which converts PostScript files into PDF files. Recent versions of the program have the tendency to abort when converting large PS files.

This can easily be handled by Netfinity Manager:

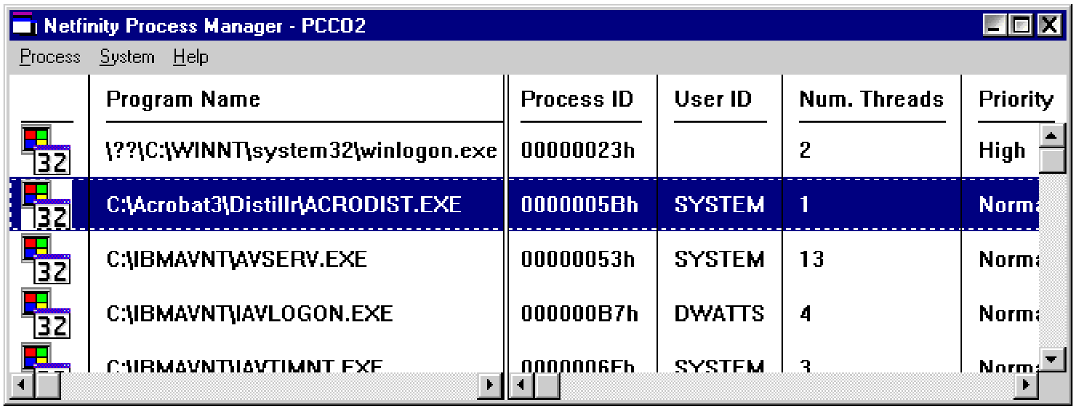
1. Use Process Manager to monitor the ACRODIST.EXE process
2. If the process stops, issue a Sev 2 alert
3. Based on the alert:
   - Log the alert at the server
   - Popup a message on the administrator's workstation
   - Restart the process
4. Once the process starts again, issue a Sev 2 alert and send the alert to the administrator's workstation.

6.7.1 Monitoring the Process

From the administrator workstation, start Netfinity Manager and use Remote System Manager to access the server running ACRODIST.EXE. (we'll explain why its better to work remotely in a moment).

1. If ACRODIST isn't already running, start it using Remote Workstation Control.

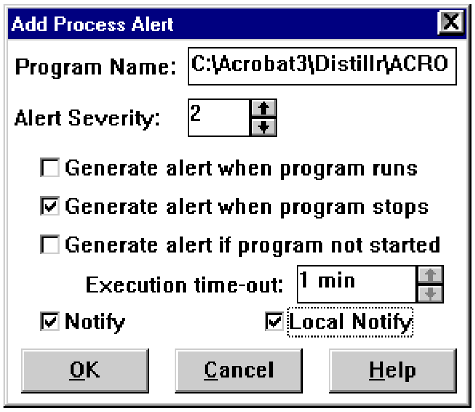
2. Double-click on the server's **Process Manager** icon and scroll down the list until you see the ACRODIST process as shown in Figure 132.



Program Name	Process ID	User ID	Num. Threads	Priority
\??\C:\WINNT\system32\winlogon.exe	00000023h		2	High
C:\Acrobat3\Distillr\ACRODIST.EXE	0000005Bh	SYSTEM	1	Norma
C:\IBMAVNT\AVSERV.EXE	00000053h	SYSTEM	13	Norma
C:\IBMAVNT\IAVLOGON.EXE	000000B7h	DWATTS	4	Norma
C:\IBMAVNT\IAVTIMNT.EXE	0000006Fh	SYSTEM	3	Norma

Figure 132. ACRODIST in Process Manager

3. Right click on the ACRODIST process and click on **Add Process Alert**. Figure 133 on page 174 appears.



Add Process Alert

Program Name: C:\Acrobat3\Distillr\ACRO

Alert Severity: 2

□ Generate alert when program runs

☑ Generate alert when program stops

□ Generate alert if program not started

Execution time-out: 1 min

☑ Notify ☑ Local Notify

Figure 133. Adding an Alert When ACRODIST Stops

4. Fill in the fields of the window as follows:

   - Set the severity to 2
   - Select **Generate alert when program stops**
   - Select **Notify**
   - Select **Local Notify**

   We have arbitrarily selected the alert to be at severity 2. The thinking goes that it shouldn't be a Sev 0 or Sev 1 alert since Netfinity Manager will automatically handle the alert. Since the process affects users, it is still a high severity incident.

   Selecting **Notify** causes the alert to be sent to the Netfinity Manager system where you are currently working — the administrator's workstation in this case. Selecting **Local Notify** causes the alert to be sent to the server's Alert Manager.

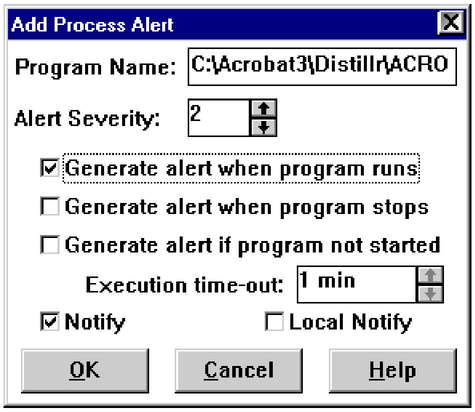
   By working from the administrator's workstation, you get both of these notify check boxes. If you had worked locally at server, you would only get **Notify**.

   Note: If you have them both *not* selected, no alert will be issued to any Netfinity Manager system.

5. Click on **OK** to save the Alert

6. Right-click on the ACRODIST and select **Add Process Alert** again.

7. This time, fill out an alert for when ACRODIST starts or restarts, as per Figure 134 on page 175.



Program Name: C:\Acrobat3\Distillr\ACRO

Alert Severity: 2

☑ Generate alert when program runs

□ Generate alert when program stops

□ Generate alert if program not started

Execution time-out: 1 min

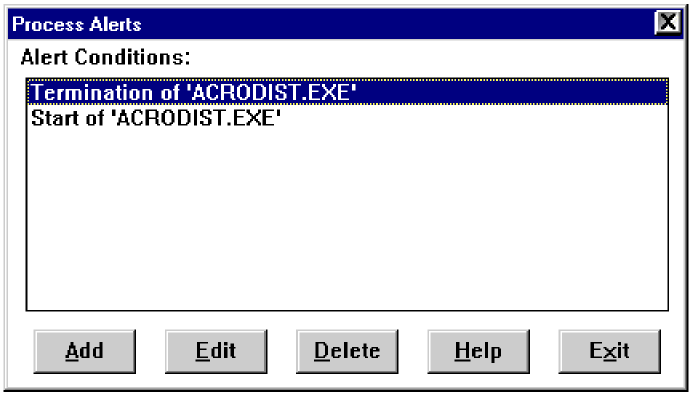
☑ Notify □ Local Notify

Figure 134. Adding an Alert When ACRODIST Starts

We don't want Alert Manager on the server to be sent the alert, just the administrator's workstation. Hence **Notify** is checked and **Local Notify** is not.

8. Click on **OK** to save the Alert

Tip: If you want to edit the process alerts once they've been defined, click on **Process** → **Process Alerts**. Figure 135 appears letting you select and edit each alert.



Alert Conditions:

Termination of 'ACRODIST.EXE'
Start of 'ACRODIST.EXE'

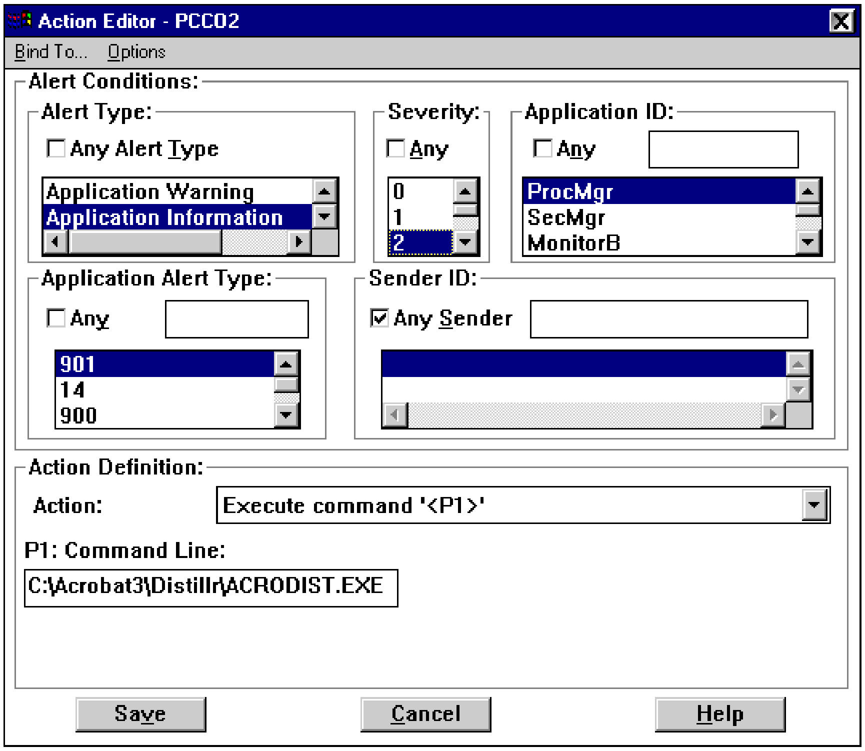
Figure 135. Editing Existing Process Alerts

6.7.2 Actions When the Process Stops

We now need to set up the actions that will occur when ACRODIST stops. We want the following to occur at this point:

- Log the alert at the server — already configured since we specified **Local Notify** in Figure 133 on page 174.
- Popup a message on the administrator's workstation — already configured since we specified **Notify** in Figure 133 on page 174 and the administrator's workstation should, by default, be configured to pop-up all Sev 2 messages.
- Restart the process

To restart ACRODIST when the alert is received locally by the server, we use Alert Manager to create a new action. Clicking on **Actions** in Alert Manager yields the Action Editor window, shown in Figure 136 on page 176.



Alert Type:
□ Any Alert Type
Application Warning
Application Information

Severity:
□ Any
0
1
2

Application ID:
□ Any
ProcMgr
SecMgr
MonitorB

Application Alert Type:
□ Any
901
14
900

Sender ID:
☑ Any Sender

Action: Execute command '<P1>'

P1: Command Line:
C:\Acrobat3\Distillr\ACRODIST.EXE

Figure 136. Action Editor

The alert received when the ACRODIST process stops has the following characteristics:

Alert Type: Application Information
Severity: 2
Application ID: ProcMgt
Application Alert Type: 0901

We therefore configure the action based on those values as shown in Figure 136. Our action is to execute a command, and the P1 field is the command to restart the process.

6.7.3 Actions When the Process Starts

Once the ACRODIST program is restarted, we want the alert to be sent to the administrator's workstation. As this was already configured in Figure 134 on page 175, there is nothing further to do.

As additional steps, your further actions could be performed on the administrator's workstation when the stop and start alerts are received. For example, you might want to play a WAV file, or send a pager message. Bear in mind that it should be just an informational notification only as Netfinity Manager has already restarted the application.

One final note: Process Manager checks the processes every 10-15 seconds. Consequently, if your application restarts and stops again within that time, Process Manager will not recognize the change and the alert will not be issued. This means that for applications that fail just after they are started, this example will not be sufficient to ensure they restart every time.

6.8 Example 8: Remote Update of Netfinity 5500 BIOS

This scenario explains the process of using the Netfinity Advanced Remote Management processor to update the system BIOS of the Netfinity 5500 that is remote from a Netfinity Manager workstation.

The hardware and software prerequisites for this function are:

- Netfinity Manager 5.10.4 on both the workstation and the remote Netfinity 5500.
- The installation option, “System Management Support” installed on both systems.
- The workstation running the manager code of Netfinity Manager
- The remote server running either client or manager code of Netfinity Manager
- Modem attached to COM port on the workstation
- Modem attached to the Management Port (COM C) on the server

6.8.1 The Process

The steps are as follows:

1. Configure dialling into the 5500's Advanced Remote Management processor
2. Setup dialout from workstation
3. Dial into the Advanced Remote Management processor
4. Power off the server
5. Perform BIOS update
6. Restart the server

These steps are now described in detail.

Recovering from a BIOS Failure

The Netfinity 5500 maintains two versions of the system BIOS: a primary version and a backup version. You can select which version the system is to boot from by changing jumper J30 on the system board (see Figure 70 on page 99).

This function is useful because it allows you to recover from a BIOS upgrade that caused errors.

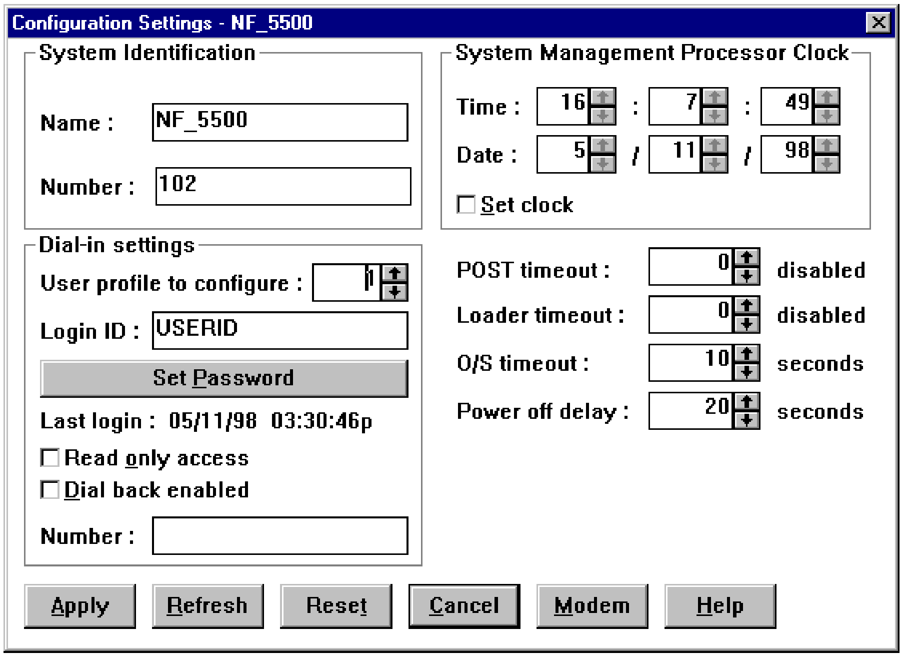
When you upgrade the system BIOS you are always updating the primary version. When upgrading locally at the server, you are given the option to copy the existing primary version to the backup. When upgrading remotely, you do not get the option and the copy does not occur.

6.8.1.1 Configure Dial-In

Before we can dial into the Netfinity 5500, we need to configure the Advanced Remote Management processor to allow dial-in via modem.

1. Either at the server or via Remote Systems Manager in Netfinity Manager,

   open the **Configuration Settings** window in the Advanced System Management function of Netfinity Manager. Figure 137 on page 178 appears.



Configuration Settings - NF_5500

System Identification

Name : NF_5500

Number : 102

System Management Processor Clock

Time : 16 : 7 : 49

Date : 5 / 11 / 98

□ Set clock

Dial-in settings

User profile to configure : 1

Login ID : USERID

Last login : 05/11/98 03:30:46p

□ Read only access

□ Dial back enabled

Number :

POST timeout : 0 disabled

Loader timeout : 0 disabled

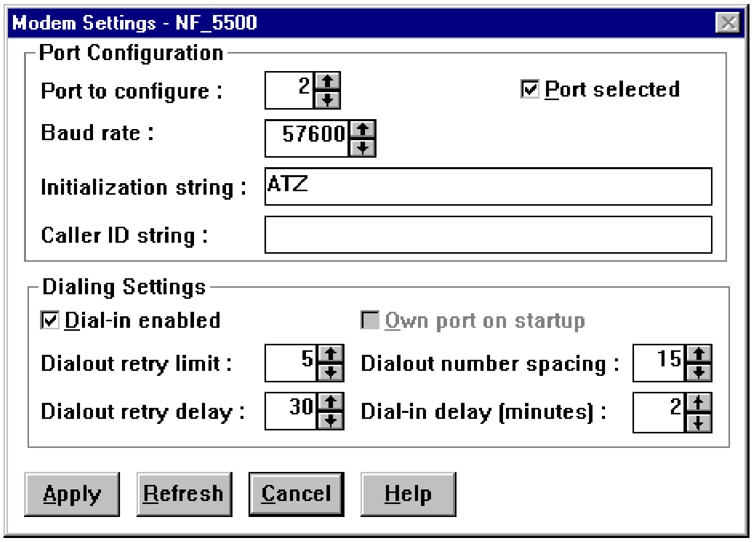
O/S timeout : 10 seconds

Power off delay : 20 seconds

Figure 137. Advanced Remote Management Processor Dial-in Settings

2. Enter a userid and password that you plan to use to dial into the Advanced Remote Management processor with later in the example. See 3.2.2, “Configuration Settings” on page 73 for details on this window.

3. Click on **Modem** Figure 138 appears.



Modem Settings - NF_5500

Port Configuration

Port to configure : 2

☑ Port selected

Baud rate : 57600

Initialization string : ATZ

Caller ID string :

Dialing Settings

☑ Dial-in enabled

□ Own port on startup

Dialout retry limit : 5

Dialout number spacing : 15

Dialout retry delay : 30

Dial-in delay (minutes) : 2

Figure 138. Advanced Remote Management Processor Modem Settings

4. Configure your own modem. See 3.2.3, “Port and Dialing Settings” on page 76 for details on this window.

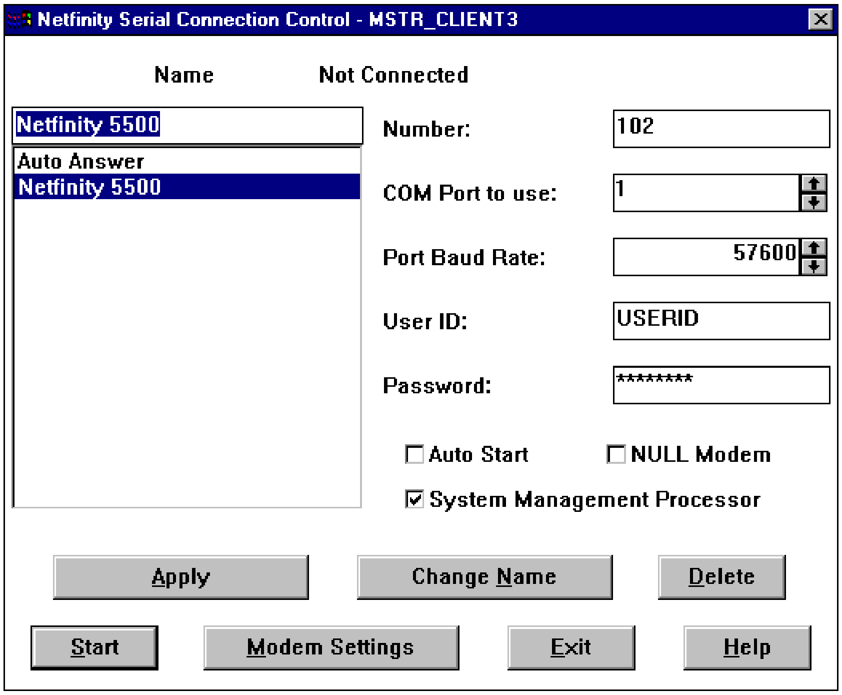
   Notice that that port 2 is configured as the one connected to the modem. Port 2 corresponds to COM C, the management port on the Netfinity 5500. Save your modem settings.

5. Click on **Apply** to save your dial-in userid settings.

6.8.1.2 Configure Dial-Out and Dial the Server

Now we need to configure the local workstation to dial the Advanced Remote Management processor in the remote Netfinity 5500.

1. Open the **Serial Connection Control** window in the Netfinity Manager. Figure 139 appears.



Netfinity Serial Connection Control - MSTR_CLIENT3

Name: Netfinity 5500 — Not Connected

Number: 102

COM Port to use: 1

Port Baud Rate: 57600

User ID: USERID

Password: ********

□ Auto Start □ NULL Modem

☑ System Management Processor

Figure 139. Serial Control Settings

2. Fill in the fields in the window to match the userid you specified in 2 in 6.8.1.1, “Configure Dial-In” on page 177 and the phone number and modem parameters of your modem.

3. Put a check mark in the **System Management Processor** field.

4. Click on **Apply** to save the new settings.

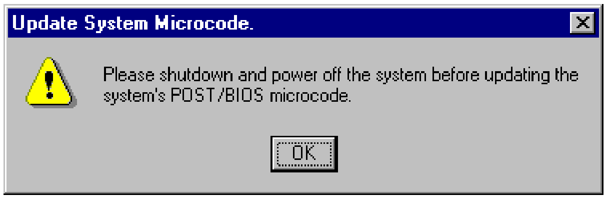
5. Click on **Start** to dial the Advanced Remote Management processor on the Netfinity 5500.

   Once the connection is made, you will see `Connected` at the top of the window.

6. Click on **Exit** then **OK** to confirm exit without saving changes.

6.8.1.3 Power Off the Server

Before you can *flash* (update) the system BIOS, you must first power down the server. If you do not, the following message will appear when you attempt the update:



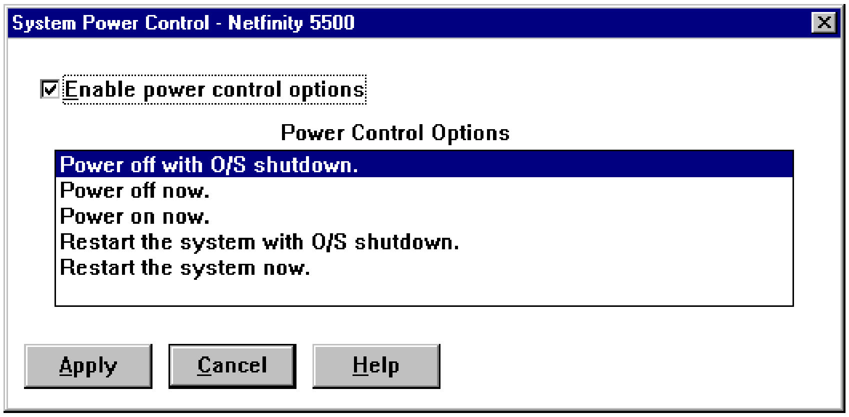
Update System Microcode.

Please shutdown and power off the system before updating the system's POST/BIOS microcode.

Figure 140. Shut the Server Down Before BIOS Update

1. To power down the server, go to the Advanced System Management window and open **System Power Control**. Figure 141 appears.

   As you are already dialed into the server, you are now controlling it from your local workstation through the Advanced System Management interface.



System Power Control - Netfinity 5500

☑ Enable power control options

Power Control Options

Power off with O/S shutdown.
Power off now.
Power on now.
Restart the system with O/S shutdown.
Restart the system now.

Figure 141. System Power Control on the Netfinity 5500

2. Click on **Enable power control options**
3. Select **Power off with O/S shutdown**
4. Click on **Apply**. The operating system now shuts down and the server powers off.
5. Click on **Cancel** to leave the window.

Note: Even though the server has been powered off, the Advanced Remote Management processor still has power and the connection from your local workstation to it is still active. You can confirm this by going to **Serial Connection Control** and verifying that `Connected` is still displayed at the top of the window.

6.8.1.4 Flash the BIOS

Now that the server is powered down, the BIOS can be upgraded (*flashed*).

1. From the Advanced System Management window, click on **Options** → **Update Microcode** → **System** as shown in Figure 142 on page 181.

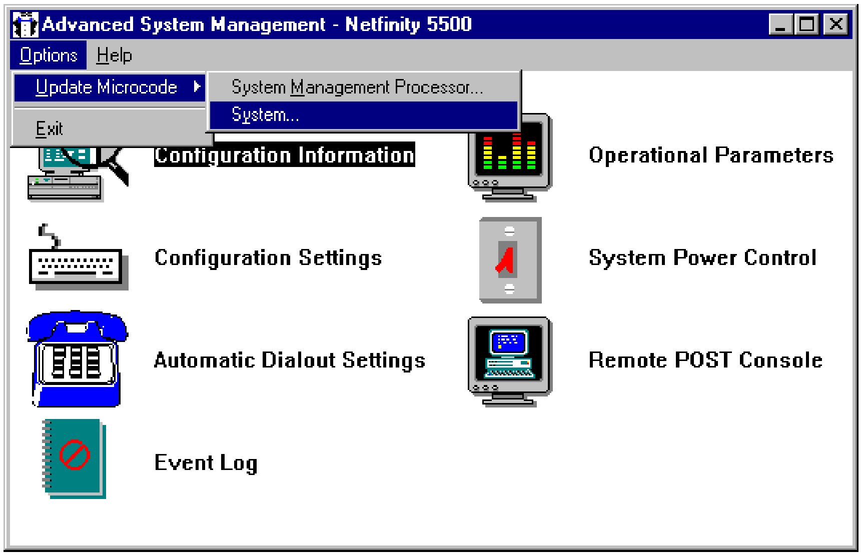


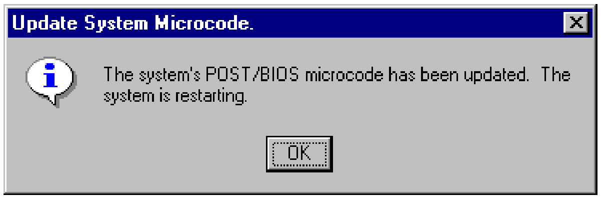
Figure 142. Starting the BIOS Update Process

2. At this point you'll be prompted to confirm the update of the system's BIOS. Click on **Yes** to continue.
3. Specify the location of the BIOS diskette or files. The upgrade process is looking for a .PKT file.
4. The process will then compare the diskette with current microcode on the server to see if they match. If they do, you will be prompted to confirm that you want to upgrade anyway.
5. You will then be given one last chance to cancel the upgrade process. Click on **OK** to continue.
6. The server will then be restarted and the transfer of BIOS data to the server will begin. You will see the following message on the server during the transfer:

   ```
   Receiving a file for remote flash update...xx%
   ```

   Once the transfer is complete, checksum calculations are performed on the data to ensure its integrity, then the programming of the EEPROM will begin.
7. Once the process is complete, you will get the message shown in Figure 143.

   Note: The actually download of BIOS data to the server can take five to ten minutes.



The system's POST/BIOS microcode has been updated. The system is restarting.

Figure 143. BIOS Update Complete

Note: You can monitor the progress of the reboot of the server by examining the **Operating Parameters** window in the Advanced System Management service. Check the **System State** field.

6.8.2 Summary

The remote update of the Netfinity 5500's BIOS can only be performed when dialled in from another Netfinity Manager workstation. It can also only be performed when the server is powered down.

Chapter 7. Working With Other Management Products

Netfinity Manager and the Advanced Systems Management Adapter can be used as stand-alone robust, yet cost-effective PC and server management solution. However, most corporate networks today are growing in size and diversity as are the number and criticality of the applications running on them. Not only are there multiple systems and protocols, but many customers implement more than one management solution. IBM Netfinity Manager provides integration with workgroup and enterprise managers so that Netfinity Manager can be incorporated into overall management strategies including Tivoli Management Software, Microsoft SMS and HP OpenView. Customers can grow naturally into an overall solution that meets their system management needs while preserving their financial and skill investments.

- Tivoli Management Software

  Netfinity Manager is a *Tivoli Ready* product because it tightly integrates with Tivoli Management Software. Through Tivoli LAN Access, Netfinity Manager can participate in Tivoli Inventory, Software Distribution and Enterprise Console — without the need for a Tivoli agent on the Netfinity Manager-enabled systems. This is accomplished through the Multi-platform Manager (MPM) API, an open and published API developed by Tivoli, Intel and other major systems management providers to establish an unparalleled level of integration and interoperability between enterprise and PC management products. This solution also provides a convenient upgrade path from Netfinity Manager to Tivoli Management Software, which helps to protect your investment in systems management technologies.

- Microsoft Systems Management Server (SMS)

  Netfinity Manager also integrates with SMS to provide consolidated operations in three areas:

  1. Netfinity Manager inventory data can be integrated into the SMS database, thereby enhancing the SMS inventory functions by adding IBM-specific data to its query capability and consolidating the SMS and Netfinity Manager inventory functions.
  2. Netfinity Manager can send any alert to SMS in the form of an SNMP trap. Therefore the system administrator can be notified of potential problems from both SMS and Netfinity Manager on the SMS console.
  3. Netfinity Manager can be launched for a particular system from the SMS topology map, so when an alert is received from a Netfinity Manager system on the SMS console. The administrator can drill down through the SMS topology map to the “problem” system, then launch Netfinity Manager on that system to identify and correct the problem — all from within the SMS console.

- Intel LANDesk

  Netfinity Manager also tightly integrates with Intel LANDesk to provide consolidated alerting and inventory functions. Netfinity Manager can be launched from both LANDesk to give you access to RAID, cluster management and more functions to complement these tools, providing you with an integrated management solution.

- SNMP

> Netfinity Manager now provides more extensive integration with SNMP managers. It generates unique SNMP traps for each Netfinity Manager alert and can forward these traps to any SNMP management platform such as HP OpenView or CA Unicenter. Then the SNMP manager may issue commands to any Netfinity Manager to take an action in response to these alerts through Netfinity Manager's command line interface. Netfinity Manager also ships with MIBs for monitor, inventory and alert data, which are installed on the SNMP management platform, so the SNMP manager may “get” this information whenever it needs it.

This chapter describes how to integration IBM Netfinity Manager with Microsoft SMS. Future editions of this redbook will cover detailed instruction on how to integrate Netfinity Manager with the other management suites.

7.1 Netfinity Integration with Microsoft's SMS

As described in 2.1, “Introduction” on page 3, Netfinity Manager can help you manage your networked PCs and servers. For the systems administrator, the prospect of integrating Netfinity Manager into an existing systems management solution may create additional problems. Netfinity Manager has been designed to provide integration with management solutions such as Microsoft's Systems Management Server (SMS) with the same efficiency and simplicity that are characteristic of the Netfinity Management framework.

7.1.1 Prerequisites

To install SMS, make sure your server meets the following requirements. The server must be a primary or backup domain controller running Windows NT Server version 3.51 or higher. You must be logged with administrator privileges locally before running setup.

The Hardware specifications are:

- Processor: Intel 486/66 or higher
- RAM: 32 MB
- Disk Space: 300 MB on your C: drive
- CD-ROM drive

The supported Networks are:

- Microsoft Windows NT Server version 3.51 and later
- Microsoft LAN Manager version 2.1 and later
- Novell NetWare 3.1x and 4.x
- IBM LAN Server 3.0 and 4.0
- Any network protocol supported by Windows NT Server, including TCP/IP and IPX
- LU 6.2 provided by Microsoft SNA Server
- Remote access protocols including ISDN, X.25, and asynch

The clients supported are:

- Microsoft Windows 3.1
- Microsoft Windows 95 operating system
- Microsoft Windows for Workgroups 3.11
- Microsoft Windows NT Workstation 3.5 and later
- Microsoft MS-DOS 5.0 and later

- IBM OS/2 2.x and OS/2 WARP
- Apple Macintosh System 7
- PATHWORKS servers
- UNIX: AIX, HP-UX, OSF/1, Sun OS, Solaris, and Ultrix
- VMS

7.1.2 What Netfinity Manager Provides

For the SMS environment, Netfinity Manager can provide:

- Enhanced inventory capability to any SMS client

  Netfinity Manager provides for the generation of MIF files. This custom inventory of Netfinity Manager provides SMS with a richer database of attributes which can then be queried and monitored by the SMS administrator console. It includes such features as RAID information, PCI/EISA/MCA device information, serial numbers of IBM systems and other vital product data of components in your systems.

- Integration of Netfinity Manager alerts with the SMS Administrator console

  Netfinity Manager uses alert actions configured through Alert Manager service to define a set actions. There are three alert actions that provide integration with SMS:

  1. Add event to NT Event Log
  2. Map Alert to a SNMP trap
  3. Send a SNMP trap

- Netfinity Manager launch support

  When examining individual client systems with Netfinity installed, the Netfinity Manager interface can be started from within the SMS environment and further system management can be done for that remote system.

The system requirements for this integration are SMS 1.2 with SMS Service Pack 2 and Netfinity Manager. We recommend that you use the latest version of Netfinity Manager and any later SMS Service Packs. Either the client services component or the manager component of Netfinity Manager must be installed on all SMS clients you wish to manage with SMS and Netfinity Manager. Netfinity Manager must be installed on all SMS Administrator consoles for which the launch support and sharing of management features is desired.

The first step is install SMS on the managing workstation and managed clients, then to install Netfinity Manager on those machines.

Note: All configuration in this chapter is done using Windows NT Server 4.0 and SMS v1.2.

7.1.3 Installing the SMS Manager

To install SMS on the managing system, perform the following steps:

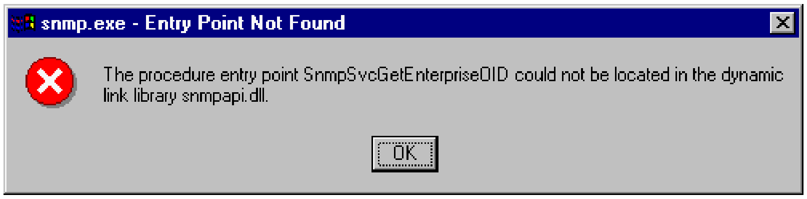
1. Remove any existing copy of Netfinity Manager.

   This is not entirely necessary but you will have to reinstall Netfinity Manager after installing SMS and it ensures you have a clean installation. You can backup any existing configuration using Service Configuration Manager and restore using Event Scheduler.

2. Reboot your server after the Netfinity uninstall to ensure the product is fully removed.
3. Install SQL Server and SMS as described in the install instructions provided with the product.
4. Shutdown and reboot after the installation.
5. if you plan to receive SNMP alerts from Netfinity Manager or from SMS client then you will need to install the Windows NT SNMP service

   To install the SNMP service perform these steps:

   a. Start **Control Panel**
   b. Double-click on the **Network** icon
   c. Select the **Services** tab
   d. Click on the **Add...** button
   e. Highlight the **SNMP Service**
   f. Select **OK** to install the SNMP service.
   g. Select the SNMP service and select properties.
   h. Ensure you have selected **Application** and **End-to-End** in the **Agent** tab as this is required for SMS.
   i. Shutdown and restart you system.
6. Install or re-install your Windows NT Service Pack 3. If you do not do this, you will get an event log entry telling you that the SNMP service cannot find the file \SYSTEM32\INETMIB1.DLL and you will get the pop-up message seen in Figure 144.


snmp.exe - Entry Point Not Found

The procedure entry point SnmpSvcGetEnterpriseOID could not be located in the dynamic link library snmpapi.dll.

Figure 144. SNMP Error Pop-up — Reapply the Service Pack

7. Install Netfinity Manager.
8. If you want the local machine in the inventory then install the SMS client before Netfinity Manager and then create the custom MIF file. See the 7.1.5.1, “Netfinity Manager MIF Generator” on page 188 for instructions on how to generate this.

7.1.4 Installing SMS Clients

Now that we have installed SMS, a set of file shares have been setup to gain access to the client part of SMS. These shares are used to gain access to the client code for installation and to pass inventory information back to the SMS site manager.

The SMS client also uses a special UserID to run the Client Configuration Manager (CCM) service. SMS Client Setup uses the CCM service to install, upgrade, and remove SMS client components on computers running Windows NT. When SMS Client Setup needs to perform actions that may require special access on a computer running Windows NT, it posts a client configuration request to the CCM service. The CCM service then carries out the request if the SMSService user has the appropriate rights.

The CCM service configures the following components on Windows NT-based computers running as SMS clients:

- Inventory Agent service.
- Remote Control service.
- SNMP Event to Trap Translator.

What if my client is in another NT domain?

When the SMS client installs, it can pass inventory information back to the SMS site by using a share but when the CCM agent needs to run on the client then it requires administrative rights back to the SMS site.

The CCM service uses the SMSService user as its access in to the SMS site. This means that the remote domain needs to either have a Trust relationship with the SMS Sites domain or there be a local user with the same name and password. When setting up the SMSService user on the remote domain, it needs to have the *Log-on as a Service* right. For trusted domains a trust relationship needs to be established.

If you find you cannot run one of the previous CCM services then you may have an access problem with the CCM service.

To install the SMS client manually, on a Windows NT platform, to integrate with Netfinity Manager follow the steps below. For other platforms and for automation of the installation see the on-line SMS Users Guide.

1. If you plan to send SNMP information from a Windows NT SMS client, install the Windows NT SNMP service as you did for the SMS server:

   a. Start **Control Panel**
   b. Double-click on the **Network** icon
   c. Select the **Services** tab
   d. Click on the **Add...** button
   e. Highlight the **SNMP Service**
   f. Select **OK** to install the SNMP service.
   g. Select the SNMP service and select properties.
   h. Ensure you have selected **Application** and **End-to-End** in the **Agent** tab.
   i. Shutdown and restart you system.

2. Install or re-install Window NT Service Pack 3 or higher.

3. Using either command line or the Network Browser connect to the share

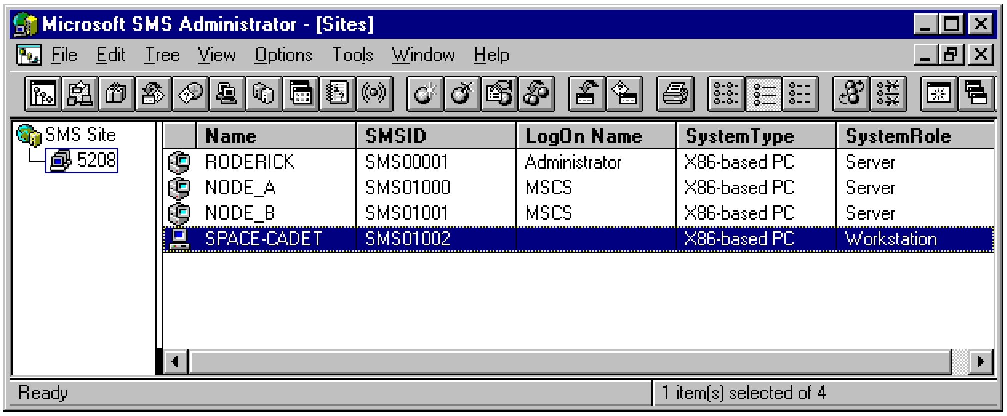
   ```
   \\yourSMSserver\SMS_SHR
   ```

   on the Windows NT Server running the SMS site that you just installed.

4. From this share connection, run batch file `RUNSMS` This batch file will install the client components on the client and then inventory the computer's hardware and software.

5. Reboot the SMS client.

6. The client should now appear automatically in the client group section of your SMS server. The configuration changes appear after the client computer has been restarted. You can see in Figure 145 on page 188 that the clients are accessed on the left had panel of the sites view.



Microsoft SMS Administrator - [Sites]

Name	SMSID	LogOn Name	SystemType	SystemRole
RODERICK	SMS00001	Administrator	X86-based PC	Server
NODE_A	SMS01000	MSCS	X86-based PC	Server
NODE_B	SMS01001	MSCS	X86-based PC	Server
SPACE-CADET	SMS01002		X86-based PC	Workstation

1 item(s) selected of 4

Figure 145. The SMS console showing a small site.

7. Install Netfinity Manager on the client system
8. Create the MIF file for the local client. See the 7.1.5.1, “Netfinity Manager MIF Generator” for instructions on how to generate this.
9. Reboot the SMS client.

Now when you open up SMS administrator you will see the SMS clients in your SMS domain.

Due to the way SMS handles updates to it's database, the period of time that it takes for an update to be reflected in the SMS console can vary. For the purpose of testing we set the site properties to take a hardware and software inventory every time a workstation logged on.

To set this follow these steps:

1. Select the Site
2. Select **File** → **Properties...**
3. Select **Inventory**
4. Select **Proposed Configuration**
5. Select **Hardware inventory every Workstation Logon**
6. Select **Software inventory every Workstation Logon**
7. Select **OK** twice
8. Then save the settings.

7.1.5 Integrating Netfinity Manager with SMS

Once the software is installed the two products need to be configured so they can communicate with each other.

7.1.5.1 Netfinity Manager MIF Generator

A Management Information Format (MIF) file contains information about the hardware and software installed and running on a workstation or server. Netfinity Manager includes MIF Generator to create such files.

MIF Generator is a utility that can generate a MIF containing data about your system configuration. The syntax of the MIF file is 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 the SMS database. The Netfinity Manager MIF Generator can be used to add custom inventory data to the Personal Computer Properties of an SMS client.

This utility can be found in the installed Netfinity Manager directory or on the installation CD. The syntax for this utility for SMS is as follows:

```
SIMIFMAK SMS.MFT /SMS
```

The template file SMS.MFT is the file used as a template for MIF generation. SMS.MFT provides the Netfinity Manager 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. This cycle is governed by settings in the Site Properties window. See Page 188 for details on this.

The generation of the MIF file can be integrated into SMS in several ways. It can be scheduled to run in the following ways:

- Login scripts every time a user logs on
- Periodically using the Windows NT AT command
- Using a SMS job.

For information on configuring SMS to perform these functions automatically, refer to the SMS documentation.

7.1.5.2 Launch Support for Netfinity Manager in SMS

Within the SMS console you can start Netfinity Manager at particular systems.

If you have installed Netfinity Manager after installing your SMS site you will have a menu option to launch Netfinity Manager. The menu option is added to the **Tools** menu when you are examining the Personal Computer Properties, and only appears when you are examining these properties. When the menu option is selected then it will launch the Netfinity Manager for that system.

Netfinity Security

SMS launches Netfinity Manager and uses the Security Manager entry for the server you want to access. If no entry exists then it uses the default. If the default is no access, you will be presented with a log-in box but if the default is to have limited access then that is the window that you are presented with.

To get around this either setup your servers with no public access or use Remote System Manager in Netfinity Manager to log-in to the systems you have cataloged in SMS before trying to access them through SMS, and responding **Yes** when prompted to make this userid your default access for this system.

7.1.5.3 Sending Netfinity Manager Alerts Via SNMP

Netfinity can convert it's alerts in to SNMP traps using Alert Manager. The alert needs to be handled by Alert Manager and then converted by an action to an SNMP trap. Before that is done though, we need to add the SNMP Service to Windows NT. Follow the instructions on Page 187 to add the SNMP to the client.

Note: If you have not installed the SNMP service before Netfinity Manager you will have to reinstall Netfinity Manager before the the SNMP options will appear in the action list.

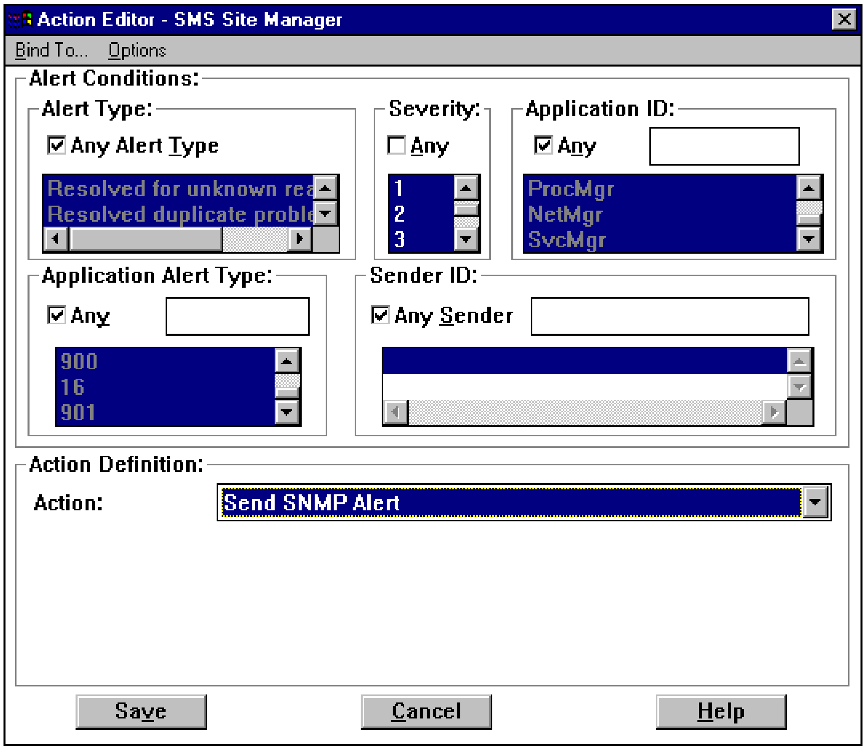
To setup the client follow the instructions in 7.1.4, “Installing SMS Clients” on page 186, making sure you install the SNMP service on the client for NT machines

1. Start **Control Panel**.
2. Double-click on the **Network** icon.
3. Select the **Services** tab.
4. Select the **Traps** tab and add your community name. A *Community* is a administrative group of systems. The group take part in authentication of messages and have the name as part of the SNMP packet.
5. Add the address of the system that you want to forward the SNMP alerts to the **Trap Destinations** section. This should typically be the SMS site server.
6. Close the SNMP properties and the Network box.
7. Restart the SNMP service in the services icon. The server does not need to be rebooted.

Netfinity Manager can then be set to respond to an alert by sending it to the SNMP service by following these steps:

1. Open **Alert Manager** in Netfinity.
2. Click the **Action** button to open the Action list window.
3. To setup a new Action click on the **New** button.
4. Set the alert conditions you require for an alert to be forwarded.
5. Set the action to **Send SNMP Alert**.
6. Save the action.

In Figure 146 on page 191 you can see an example action setup to send any alert received in Netfinity Manager sent out as an SNMP alert.



Alert Conditions:

Alert Type: ☑ Any Alert Type
Resolved for unknown rea
Resolved duplicate proble

Severity: ☐ Any
1
2
3

Application ID: ☑ Any
ProcMgr
NetMgr
SvcMgr

Application Alert Type: ☑ Any
900
16
901

Sender ID: ☑ Any Sender

Action Definition:
Action: Send SNMP Alert

Figure 146. Action Editor Setup to Send an SNMP alert

Now that the client has been configured the setup on the Server needs to be considered:

The SMS console needs to be set so that it can receive SNMP information from the clients and Netfinity Manager

To set this follow these steps:

1. Select the Site you wish to receive the SNMP alerts
2. Select **File** → **Properties...**
3. Select **SNMP Traps**
4. Select **Proposed Configuration**
5. Select the button **Create...**, this will bring up the a new filter window.
6. Fill out the **Description**, and the **OID** number. The screen should be filled out as in Figure 147 on page 192

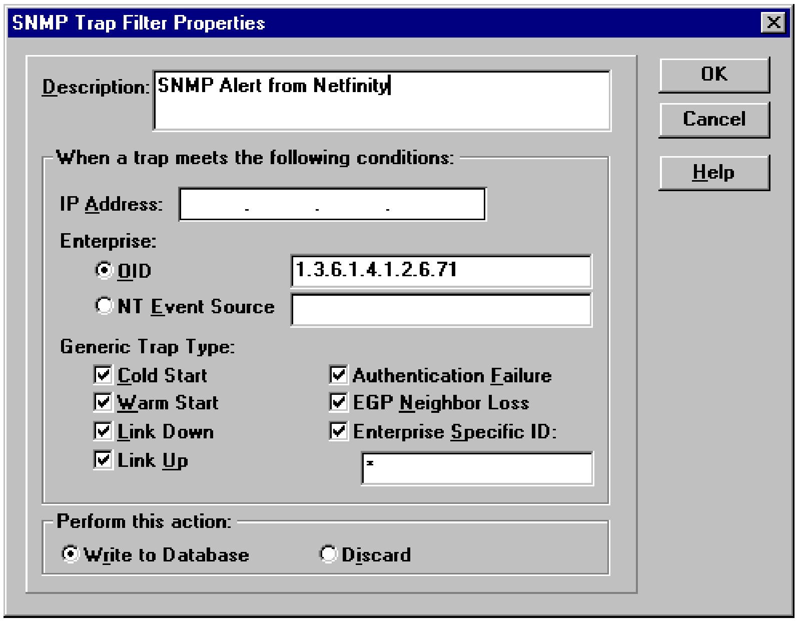
   An Object Identifier (OID) is a sequence of integers which traverse a global tree. This tree describes managed objects and each level is assigned to various groups to do with as they want. The structure of the number assigned to Netfinity is below and shows a progressive structure:

   1 for International Organization for Standards
   3 for other national or international organizations
   6 for the US Department of Defense
   1 for Internet Activities Board (IAB)
   4 for Designated by the IAB for Private organizations
   1 for International ANA registered enterprise
   2 for IBM Corporation
   6 for IBM products
   71 for Netfinity Manager

So the number is **1.3.6.1.4.1.2.6.71** or **iso.org.dod.internet.private.enterprise.ibm.ibmprod.netfinity**

For further information, see the Internet Request For Comment (RFC) 1155, 1156 and 1157.

7. Select **OK**Figure 147 show the setup for the SNMP alerts from Netfinity to be trapped in SMS.



SNMP Trap Filter Properties

Description: SNMP Alert from Netfinity

When a trap meets the following conditions:

IP Address: . . .

Enterprise:

● OID 1.3.6.1.4.1.2.6.71

○ NT Event Source

Generic Trap Type:

☑ Cold Start ☑ Authentication Failure

☑ Warm Start ☑ EGP Neighbor Loss

☑ Link Down ☑ Enterprise Specific ID: *

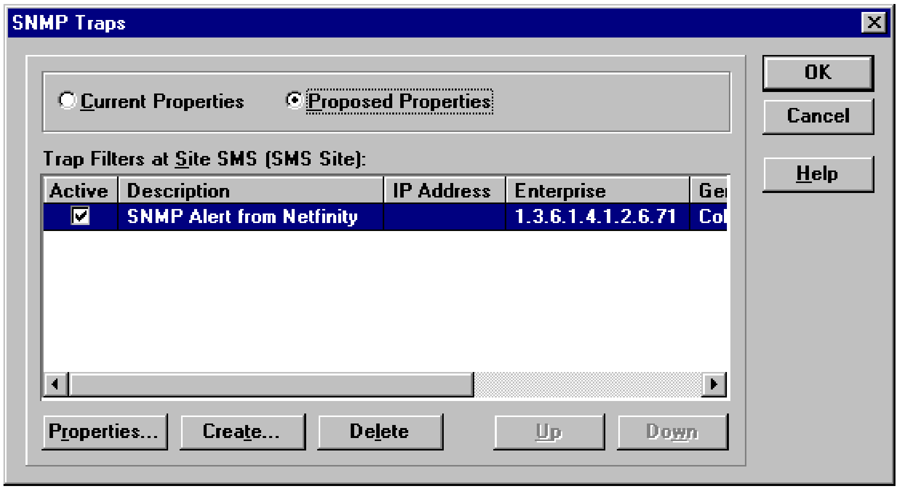
☑ Link Up

Perform this action:

● Write to Database ○ Discard

Figure 147. SNMP Trap Filter for Netfinity Managers OID number

8. You will now see the proposed filter as seen in Figure 148.



SNMP Traps

○ Current Properties ● Proposed Properties

Trap Filters at Site SMS (SMS Site):

Active	Description	IP Address	Enterprise	Ge
☑	SNMP Alert from Netfinity		1.3.6.1.4.1.2.6.71	Co

Figure 148. SNMP Trap Filter setup for an OID number

9. Select **OK**
10. Then save the settings.

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.

7.1.5.4 Sending Netfinity Manager Alerts Via Event Log and SNMP

The Integration with Systems Management Server SMS Version 1.2 provides an Event to Trap translator and a SNMP trap receiver. These two can be used to periodically scan the event log and send alerts received in it to the SNMP community. The Event to Trap translator must be configured to look for Netfinity Manager as the NT event source. As SNMP uses the Internet protocol then TCP/IP must be installed on the client and server.

Does SMSService user have the correct rights?

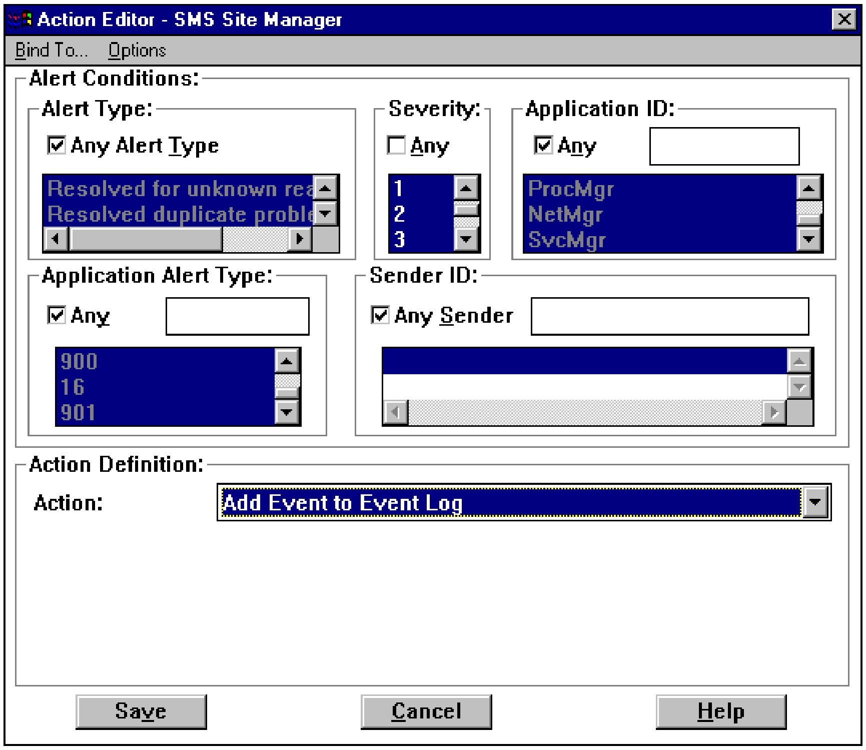
When installing the client under Windows NT the SMSService user needs to have administrative rights on the domain where the client logs on to. If the client authenticates at the same domain controller as the SMS server then there is no problem but if the client is on another domain then the SMSService user needs to have administrative rights on that domain. This can be done using either trust relationships or identical users and passwords.

What the following sets up is that when Netfinity Manager writes an event to the Windows NT event log, it is translated into an SNMP trap. An SNMP trap is an SNMP packet sent from one machine to another. The SMS server should then pickup that packet and log the event.

Follow these steps on the client:

1. Start **Control Panel**.
2. Double-click on the **Network** icon.
3. Select the **Services** tab.
4. Select the **Traps** tab and add you community name. A *Community* is a administrative group of systems. The group take part in authentication of messages and have the name as part of the SNMP packet.
5. Add the address of the system that you want to forward the SNMP alerts to the **Trap Destinations** section.
6. Close the SNMP properties and the Network box.
7. Restart the SNMP service in the services icon. The machine does not need to be rebooted.
8. Open **Alert Manager** in Netfinity Manager.
9. Click the **Action** button to open the Action list window.
10. To setup a new Action click on the **New** button.
11. Set the alert conditions you require for an alert to be logged in the event log.
12. Set the action to **Log alert in event Log**.
13. Save the action.

The client is now configured to log to the NT event log.



Alert Conditions:

Alert Type: ☑ Any Alert Type
Resolved for unknown rea
Resolved duplicate proble

Severity: □ Any
1
2
3

Application ID: ☑ Any
ProcMgr
NetMgr
SvcMgr

Application Alert Type: ☑ Any
900
16
901

Sender ID: ☑ Any Sender

Action Definition:

Action: Add Event to Event Log

Figure 149. Action Editor Setup to Log events to the NT Event Log

Now on the SMS server we need to do the following three things:

1. Set up the SNMP service on the Server
2. Setup in the SMS Site properties for the client to scan for a key word in the NT Event Log.
3. Setup the SMS Event to Trap Translator to trigger a SNMP event on a keyword appearing in the NT event log.

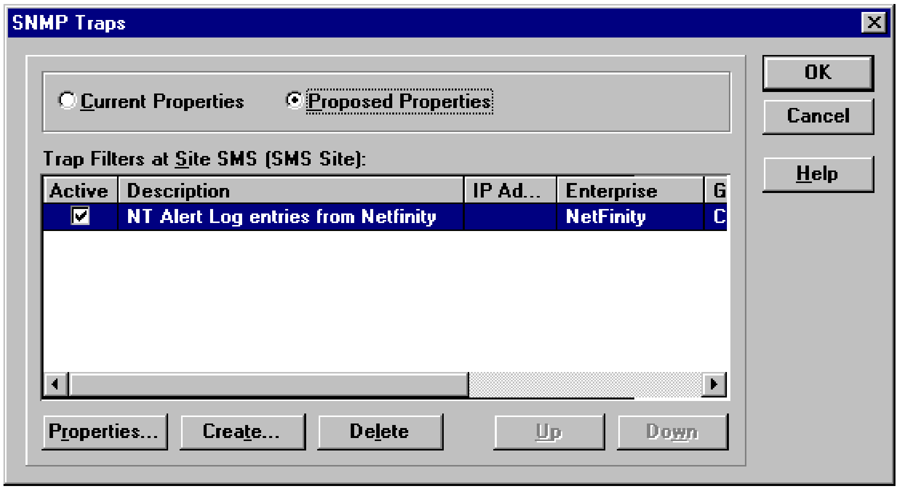
To setup the SNMP service follow these steps:

1. Start **Control Panel**.
2. Double-click on the **Network** icon.
3. Select the **Services** tab.
4. Select the **Traps** tab and add you community name.
5. Restart the SNMP service in the services icon. The machine does not need to be rebooted.

This now allows any SNMP alerts to be received by the NT server.

On the client the CCM needs to be setup to monitor the NT event log and convert any NT event log entry in to an SNMP alert and then on the server we need to setup a filter to accept these alerts if it matches a particular keyword. This is done in two stages first we setup the keyword:

1. Open up the SMS console and open the site view
2. Select the SMS Site and then the client in that domain.
3. Select **File** → **Properties...**. This will bring up the Site properties window.
4. Click on the **SNMP Trap** icon to bring up the TRAP file You can see this window in Figure 150 on page 195. This window also show the filter after setup.



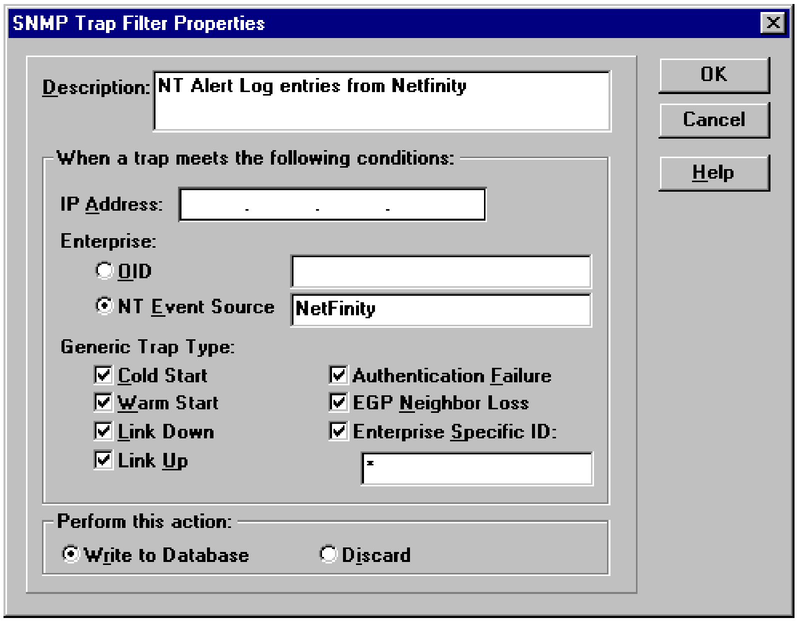
○ Current Properties ● Proposed Properties

Trap Filters at Site SMS (SMS Site):

Active	Description	IP Ad...	Enterprise	G
☑	NT Alert Log entries from Netfinity		NetFinity	C

Figure 150. SNMP Trap Filter setup for a keyword

5. Select **Proposed Properties** and then select **Create...**. This will bring up the windows as seen in Figure 147 on page 192.



Description: NT Alert Log entries from Netfinity

When a trap meets the following conditions:

IP Address: . . .

Enterprise:

○ OID

● NT Event Source: NetFinity

Generic Trap Type:

☑ Cold Start ☑ Authentication Failure
☑ Warm Start ☑ EGP Neighbor Loss
☑ Link Down ☑ Enterprise Specific ID: *
☑ Link Up

Perform this action:

● Write to Database ○ Discard

Figure 151. SNMP Trap Filter for Netfinity Manager as a keyword

6. Give the Filter a description and then set the **NT Event Source** to **NetFinity**.

   Note: The keyword *NetFinity* must be entered exactly. The word comes from the source field in the NT event log.

7. Select **OK** to save these settings and the **OK** on the filter screen. Select **OK** on the site properties window to save the settings.

Now that the keyword has been set we need to tell the CCM to scan the NT event log.

1. Open up the SMS console and open the site view.
2. Select the SMS domain and then the client in that domain that you will to configure.

3. Select **File** → **Properties....** This brings up the Personal Computer properties Window. This windows is seen in Figure 152 on page 196

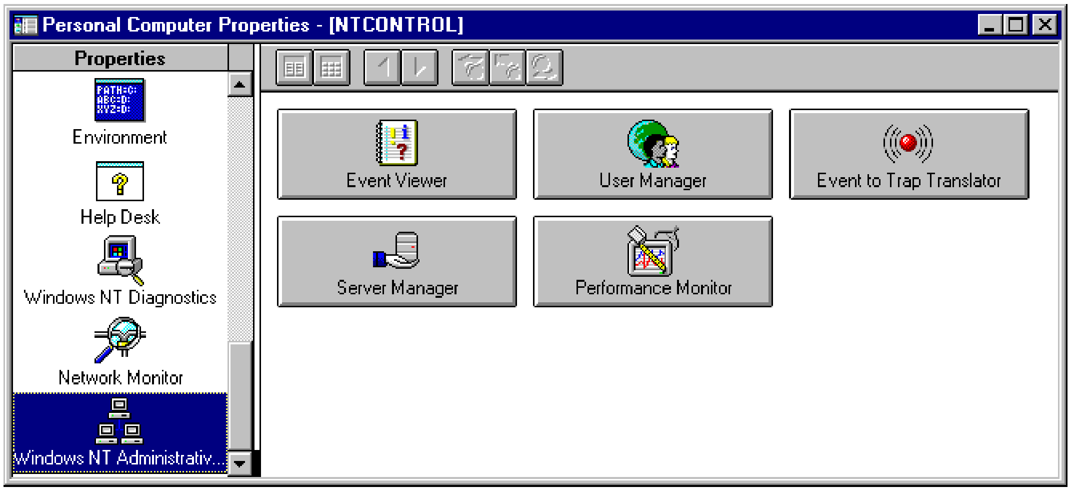
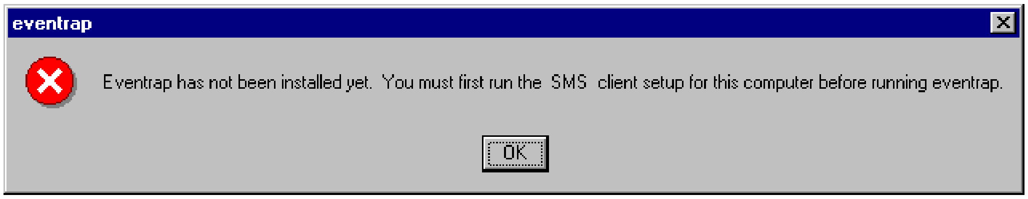


Figure 152. SMS Personal Computer Properties

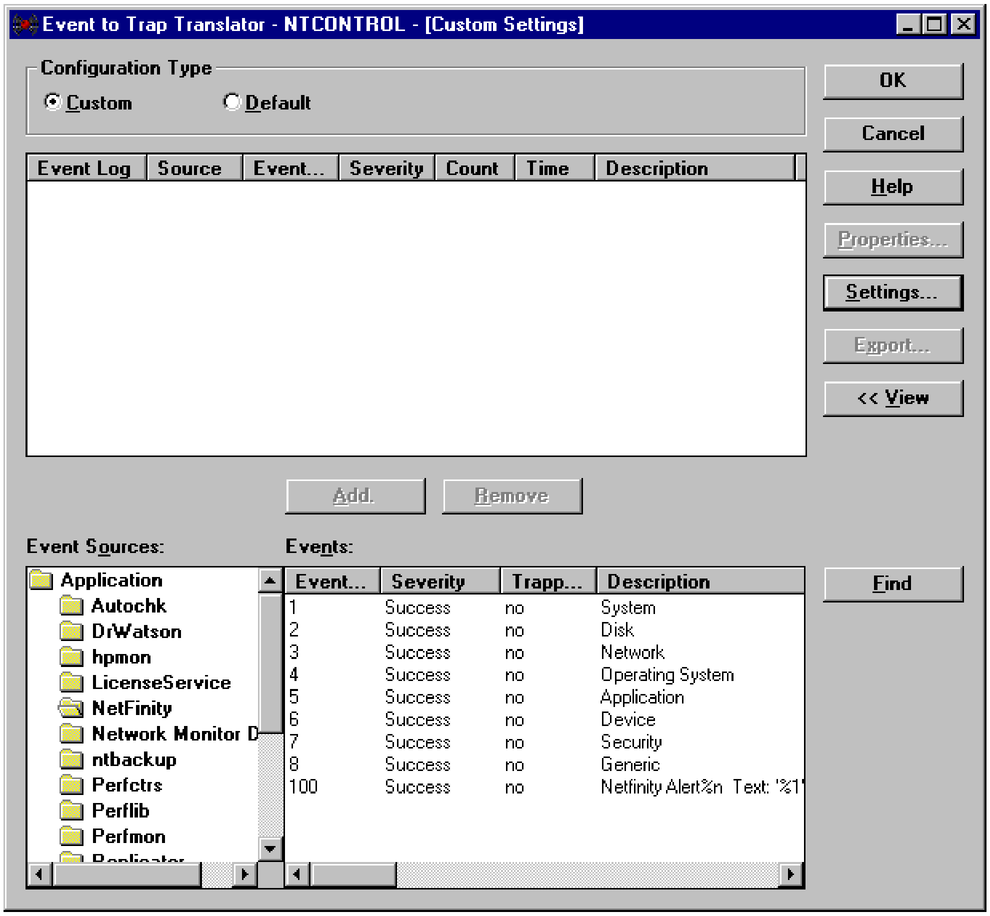
4. Select **Windows NT Administration Tools** property and then select **Event to Trap Translator**. If you get the message seen in Figure 153 then you have selected a system in another NT server domain. You will need to setup security across the two domains so that the CCM can be run. See the Microsoft SMS on-line documentation for details on how to set this up.


eventrap

Eventrap has not been installed yet. You must first run the SMS client setup for this computer before running eventrap.

Figure 153. Error when CCM has incorrect permissions

5. Select the **Custom** radio button. If you have the correct permissions you will you will see a window similar to Figure 154 on page 197



Event to Trap Translator - NTCONTROL - [Custom Settings]

Configuration Type

● Custom ○ Default

Event Log	Source	Event...	Severity	Count	Time	Description

Event Sources:

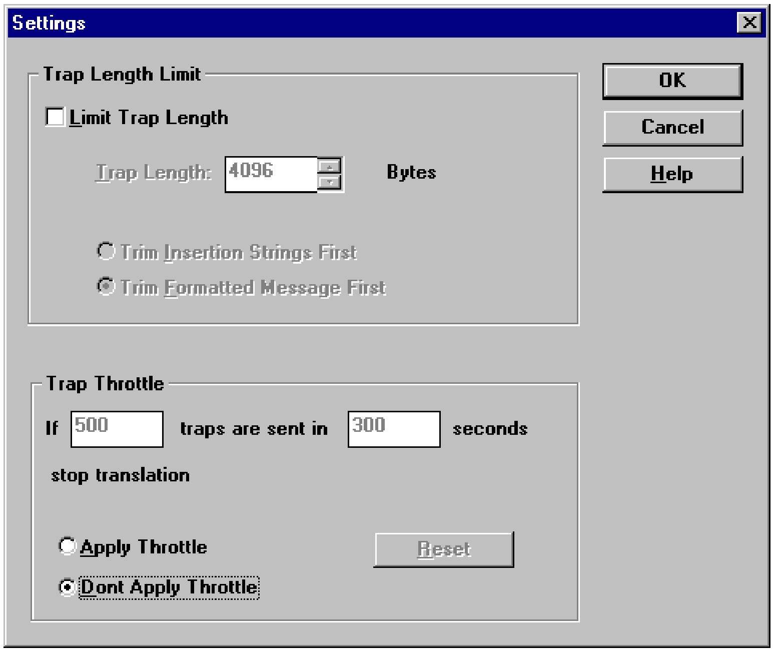
- Application
  - Autochk
  - DrWatson
  - hpmon
  - LicenseService
  - NetFinity
  - Network Monitor D
  - ntbackup
  - Perfctrs
  - Perflib
  - Perfmon
  - Replicator

Events:

Event...	Severity	Trapp...	Description
1	Success	no	System
2	Success	no	Disk
3	Success	no	Network
4	Success	no	Operating System
5	Success	no	Application
6	Success	no	Device
7	Success	no	Security
8	Success	no	Generic
100	Success	no	Netfinity Alert%n Text: '%1'

Figure 154. The Event to Trap Translator

6. Select the **Settings...** button. This will give you a dialog box similar to Figure 155 on page 198.
7. Ensure that ***Don't Apply Throttle*** is selected.



Trap Length Limit

☐ Limit Trap Length

Trap Length: 4096 Bytes

○ Trim Insertion Strings First

● Trim Formatted Message First

Trap Throttle

If 500 traps are sent in 300 seconds

stop translation

○ Apply Throttle

● Dont Apply Throttle

Figure 155. The Event to Trap Translator

8. Select **Edit** and in the right hand box select **Event Sources** → **Application** → **Netfinity**. This will bring up a list on the right-hand side of the screen that shows all of our possible events.
9. Select all of the events then select **Add.**.
10. Select **OK** to save.

Now when Netfinity receives an alert it will log it in the clients local Window NT Event Log and the CCM will pick up the Netfinity keyword and send a SNMP alert to the SMS site manager, which in turn will log the event.

Appendix A. Special Notices

This publication is intended to help customers, business partners and IBMers to successfully implement a server management environment using IBM Netfinity Manager and the Advanced Systems Management Adapter on Netfinity Servers. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM Netfinity Manager and Advanced Systems Management Adapter. See the PUBLICATIONS section of the IBM Programming Announcement for IBM Netfinity Manager and the Advanced Systems Management Adapter for more information about what publications are considered to be product documentation.

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

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

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

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, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

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

IBM®

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

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

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

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

Other company, product, and service names may be trademarks or service marks of others.

Appendix B. Related Publications

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

B.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How to Get ITSO Redbooks" on page 203.

- *Integrating LAN Managment Tools with TME 10 LAN Access*, SG24-2118
- *Clustering and High Availability Guide for IBM Netfinity and IBM PC Servers*, SG24-4858
- *IBM Netfinity and PC Server Technology and Selection Reference*, SG24-4760
- *NetFinity V5.0 Command Line and LMU Support*, SG24-4925
- *NetFinity V5.0 Database Support*, SG24-4808
- *Windows NT Systems Management*, SG24-2107

B.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	**Subscription Number**	**Collection Kit Number**
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

B.3 Other Publications

These publications are also relevant as further information sources:

- *Advanced Systems Management Adapter Installation Instructions*, 05L1467. Also available as D3KT2MST.PDF from `http://www.pc.ibm.com/us/searchfiles.html`

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at `http://www.redbooks.ibm.com/`.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type `GOPHER.WTSCPOK.ITSO.IBM.COM`
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type the following command:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1998
  ```

  For a list of product area specialists in the ITSO: type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Web Site on the World Wide Web**

  `http://w3.itso.ibm.com/redbooks/`

- **IBM Direct Publications Catalog on the World Wide Web**

  `http://www.elink.ibmlink.ibm.com/pbl/pbl`

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to `announce@webster.ibmlink.ibm.com` with the keyword `subscribe` in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** — send orders to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications
Publications Customer Support
P.O. Box 29570
Raleigh, NC 27626-0570
USA

IBM Publications
144-4th Avenue, S.W.
Calgary, Alberta T2P 3N5
Canada

IBM Direct Services
Sortemosevej 21
DK-3450 Allerød
Denmark

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to `softwareshop@vnet.ibm.com`

- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com/
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to `announce@webster.ibmlink.ibm.com` with the keyword `subscribe` in the body of the note (leave the subject line blank).

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name   Last name

Company

Address

City   Postal code   Country

Telephone number   Telefax number   VAT number

□ Invoice to customer number

□ Credit card number

Credit card expiration date   Card issued to   Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

List of Abbreviations

AC	alternating current
ANSI	American National Standards Institute
APC	American Power Conversion Corp.
API	application programming interface
APPC	advanced program-to-program communication
ASMA	Advanced Systems Management Adapter
ATA	AT Attachment
BIOS	basic input/output system
CA	Computer Associates
CD	compact disk
CD-ROM	compact disk read only memory
CNE	Certified NetWare Engineer
COM	communications port
CPU	central processing unit
CRLF	carriage return line feed
CTS	clear to send
DC	direct current
DIMM	dual inline memory module
DMI	Desktop Management Interface
DTR	data terminal ready
ECC	error checking & correction
ECC-P	error checking & correction - parity
EDO	extended data output
EMEA	Europe/Middle East/Africa
EOS	ECC on SIMM
GB	gigabyte
GUI	graphical user interface
HEX	hexadecimal
HP	Hewlett Packard
HTML	Hypertext Markup Language
I/O	input/output
ICSM	IBM Cluster Systems Management
IDE	integrated drive electronics
IIS	Internet Information Server
IP	internet protocol
IPC	interprocess communication
IPX	Internetwork Packet eXchange
IRQ	interrupt request
ISA	industry standard architecture
ITSO	International Technical Support Organization
KB	kilobyte
LAN	local area network
LAPM	Link Access Procedure for Modems
LCD	liquid crystal display
LED	light emitting diode
LMU	LAN Management Utilities
LU	logical unit
MAPI	messaging application programming interface
MB	megabyte
MCSE	Microsoft Certified Systems Engineer
MIB	management information base
MMX	multimedia extensions
MNP	Microcom Networking Protocol
MPM	Multi-platform Manager
NC	normally closed
NLM	NetWare loadable module
NMI	non-maskable interrupt
NMVT	network management vector transport
NO	normally open
O/S	operating system
ODBC	open database connectivity
OID	object identifier
OS	operating system
PCI	peripheral component interconnect
PDF	portable document format
PFA	predictive failure analysys
POST	power-on self test

PS	PostScript
PSE	Professional Server Expert
RAID	redundant array of independent disks
RAM	random access memory
ROM	read-only memory
RTS	ready to send
RWC	remote workstation control
SCSI	small computer system interface
SCU	system configuration utility
SMART	self-monitoring and reporting technology
SMP	symmetric multiprocessing
SMS	System Management Server
SN	serial number
SNA	systems network architecture
SNMP	simple network management protocol
SSA	serial storage architecture
SSL	secure sockets layer
TAP	telocator alphanumeric protocol
TCP/IP	transmission control protocol/internet protocol
TME	Tivoli Management Environment
UDP	user datagram protocol
UPS	uninterruptible power supply
URL	universal resource locator
VAC	volts, alternating current
VDC	volts, direct current
VIM	vendor independent messaging
VPD	vital product data

Index

ITSO Redbook Evaluation

Netfinity Server Management
SG24-5208-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction ____________

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

____

____

____

____

What other redbooks would you like to see published?

____

____

____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

____

____

____

____

____

Netfinity Server Management **SG24-5208-00**

SG24-5208-00
Printed in the U.S.A.