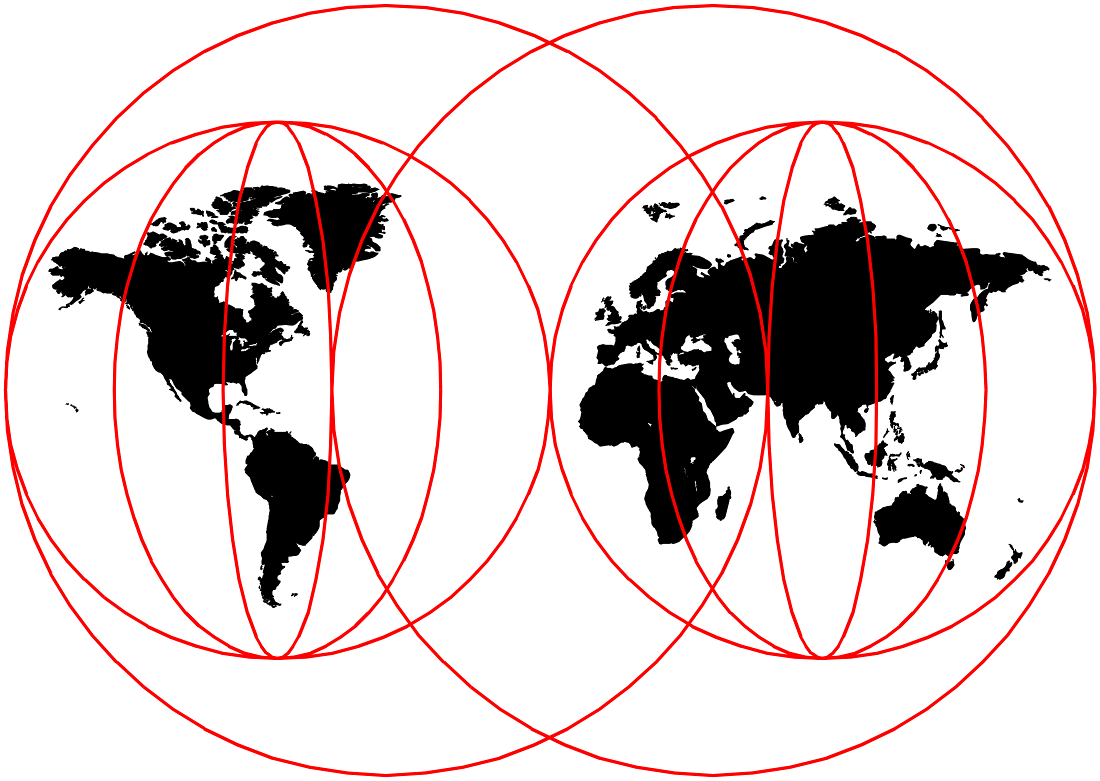
Netfinity Server Management

David Watts, Bernd Baeuml, Sutikno Lukito



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5208-01

International Technical Support Organization

SG24-5208-01

Netfinity Server Management

June 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, “Special Notices” on page 275.

Second Edition (June 1999)

This edition applies to the following IBM products:

- Netfinity Manager Version 5.20.4
- Netfinity Advanced System Management PCI Adapter
- Netfinity Advanced System Management Processor
- Advanced Systems Management Adapter
- Netfinity 3000, 5000, 5500, 5500 M10, 5500 M20, 7000 and 7000 M10

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 second edition redbook describes how to use the management hardware and software that is shipped with IBM Netfinity servers. In particular, it covers Netfinity Manager Version 5.2, the Advanced System Management PCI Adapter, the Advanced Systems Management Adapter and the management hardware that is integrated into Netfinity servers.

The book explains each of the functions of Netfinity Manager as they apply 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 management 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 System Management devices that are available for Netfinity systems. We describe the Advanced System Management PCI Adapter, the integrated Advanced System Management Processor and the Advanced Systems Management ISA Adapter. We show how to configure them to send alerts and to let you dial into the servers to perform remote diagnostics and recovery. We also describe the new RS-485 interconnect function which lets you connect through this serial link, to send and receive alerts and to allow the sharing of modems and LAN connections among servers.

For each of our currently available server systems, we describe the system status indicators and management functions. We also explain how to install the Advanced Systems Management Adapter.

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.

This redbook will help you to tailor and configure Netfinity Manager and the Advanced System Management devices in IBM’s servers and will show you 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 manages residencies and produces redbooks on IBM Netfinity Servers. His most recent publications include *Implementing Netfinity Disk Subsystems* and *Netfinity Performance Tuning with Windows NT 4.0*. 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 has worked for IBM for the past 10 years.

Bernd Baeuml is the Market Simulation and Stress Test Team Lead for IBM Netfinity server development based in Greenock, Scotland. He has three years of experience with IBM hardware and software. He holds 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. Bernd was co-author of the first edition of this redbook.

Sutikno Lukito is a PC/NW System Services Specialist in Indonesia. He has five years of experience in software and hardware for both IBM Servers and Networking. He has worked at IBM for three years. He has PSE, MCSE, and CNE qualifications. His areas of expertise include Windows NT Server and Novell Intranetware.

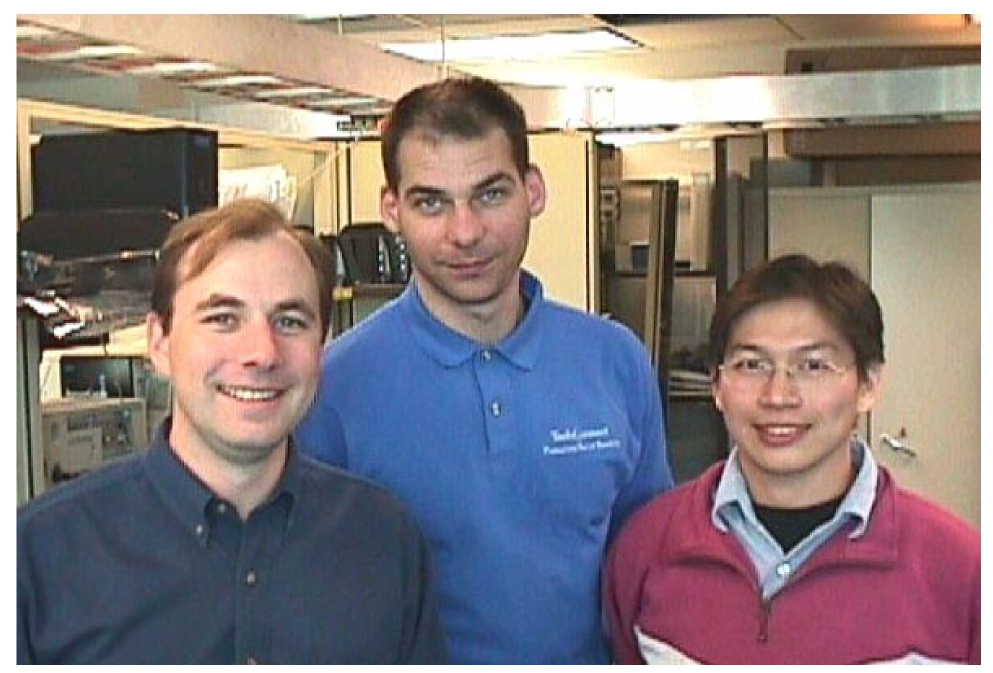


Figure 1. The Team: David, Bernd and Sutikno

Thanks to the following people from the ITSO, Raleigh for their invaluable contributions to this project:

Jakob Carstensen, Netfinity Products Specialist
Gail Christensen, Senior Editor
Barry Nusbaum, Management Products Specialist
Steve Russell, Netfinity Products Specialist
Shawn Walsh, Editor

Thanks to the following IBMers:

Kelly Anderson, Netfinity Information Development, Raleigh
Carl Bennett, World Wide Marketing Product Manager, Raleigh
Charlie Brown, Capacity Manager Test, Raleigh
Paul Chenger, Netfinity Technology Center, Raleigh
Stuart Dalgleish, Netfinity Server Development Test Manager, Greenock
George Diatzikis, Capacity Manager Test, Raleigh
George Gillenwater, World Wide Market Simulation Team Lead, Raleigh
Denise Holland, Product Education Leader for Servers, PC Institute, Raleigh
Angela Keung, Engineering Software Server FVT, Raleigh
David Laubscher, Netfinity Technology Center Manager, Raleigh
Wade Mahan, Netfinity Manager Test and Support, Raleigh

Ted Mazanec, World Wide Netfinity Brand Marketing, Raleigh
Gregg McKnight, Netfinity Performance Lab, Raleigh
Olaf Menke, IBM SWAT Netfinity Pre Sales Support, Germany
Gregg Primm, Netfinity Information Development, Raleigh
Sandra Raynor, Netfinity Information Development, Raleigh
James Rix, Netfinity Information Development, Raleigh
Marcio Spieker, Netfinity Manager ASM Test, Raleigh
Spiros Teleoglou, ASM Development Manager, Raleigh
Marco Trivella, Netfinity Product Planner, Raleigh
James VerVaecke, Netfinity Manager ASM Test, Raleigh

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 293 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an internet note to `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 and anything that keeps them from being productive. 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 management tools that have no common characteristics and little to no integration.

All they want is to be able to spend more time managing their business and less time managing their 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.
3. Provide seamless integration with leading enterprise and workgroup managers, for a comprehensive solution and a 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 systems are the Advanced System Management processors and adapters for remote monitoring and problem management, and ServerGuide to simplify installation and setup.

This redbook will concentrate on these products, explaining how they can be used to maximize your ability to manage your servers and the users they support. We describe the functions of:

- IBM Netfinity Manager
- Advanced System Management PCI Adapter
- Advanced System Management Processor
- Advanced Systems Management Adapter
- The management components of the IBM Netfinity systems

We then provide example scenarios of how these products work together to provide a solid server management platform.

For the integration of Netfinity Manager into a Tivoli environment, see *Integrating LAN Management Tools with Tivoli LAN Access*, SG24-2118. For the integration of Netfinity Manager with the IBM Universal Management Agent (UMA), see *Universal Management Agent: Functions and Integration*, SG24-5294. Future redbooks will cover the integration of Netfinity Manager with enterprise managers such as SMS and Intel LANDesk.

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 Server systems. 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 your 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. If you want a machine to be *manageable* remotely, or if you 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 Netfinity system. One license of the manager code and 10 licenses of the Client Services are included.

You can also download the latest version of Netfinity Manager from:

`http://www.pc.ibm.com/us/netfinity/smtools2.html`

or use the following path:

Go to `http://www.pc.ibm.com/support`
Select **Server** from the Select a server pulldown
Click on **Downloadable files**
Click on **Netfinity Manager**

What Do I Install on My Servers?

If you plan to do any management of the servers using the Advanced System Management processor or adapter installed in the server, then you will need the manager code. If you don't plan this and you don't plan to do any administration work from the server console, then Client Services is sufficient.

IBM Netfinity Manager and Client Services for Netfinity Manager (Client Services) are both split into 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:

- Advanced System Management Support
- Capacity Manager
- Remote Workstation Control
- Update Connector Manager
- World Wide Web Enhancement

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 11.

During the installation of Client Services, only the base services necessary to control the installed hardware are installed. 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 11, we go into detail about each of the functions. As this book is concerned for the most part with the management of servers, Netfinity Manager is the side of Netfinity that we concentrate upon.

2.1.1 IBM Netfinity Manager

Netfinity Manager is the managing portion of the system. In the 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:

- Advanced System Management Support
- Capacity Manager
- Remote Workstation Control
- Update Connector Manager
- World Wide Web Enhancement

For further details on all the Netfinity Manager functions, see 2.3, “Functions” on page 11.

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 his/her 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 and 98
- Windows NT 3.51 and 4.0

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

- OS/2 Warp V3.0, and later
- OS/2 Warp Server (including the SMP version)
- Windows 95 and 98
- Windows NT 3.51 and 4.0
- NetWare 3.12, 4.1, 4.11 and 5.0
- Windows 3.x
- SCO UnixWare 7

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)

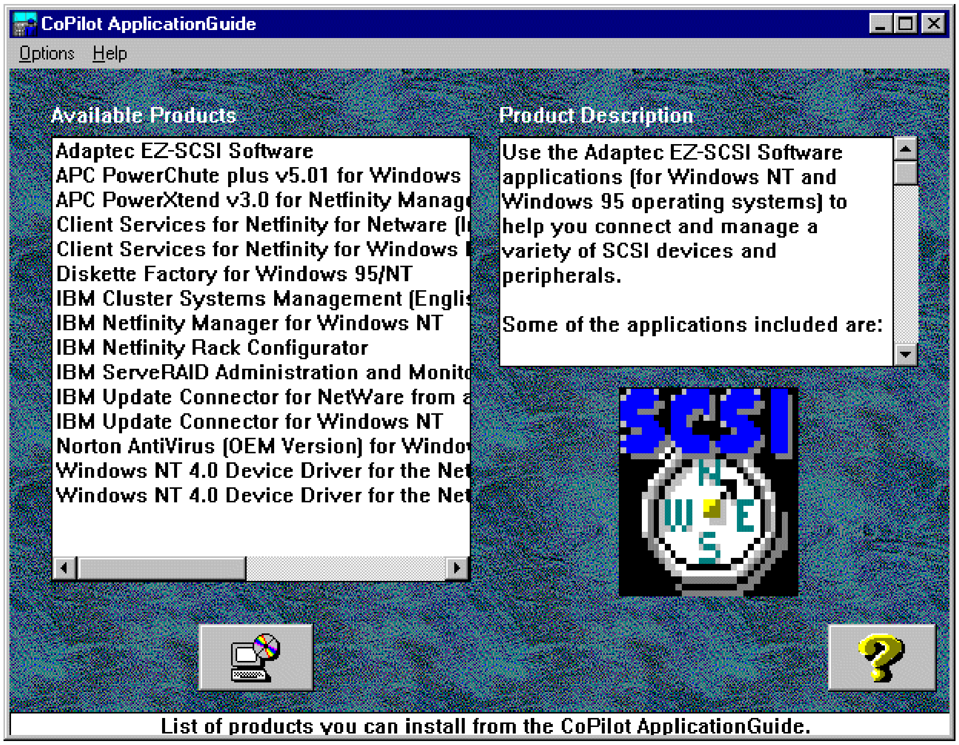
This section describes how to install Netfinity Manager, Client Services and Netfinity Manager plug-in for the Advanced Systems Management Adapter for each of the following operating systems:

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

The installation processes for Windows NT and OS/2 Warp are basically the same and will be handled together. See the README files accompanying the software for information about installing Netfinity Manager on other operating systems.

2.2.1 Windows NT and OS/2 Warp

Netfinity Manager is supplied on the ServerGuide Co-Pilot ApplicationGuide CD-ROM. Insert the CD-ROM and run SCW95.EXE for Microsoft Windows NT 4.0 and SCOS2.EXE for OS/2 Warp. The CD-ROM starts automatically in Microsoft Windows NT 4.0. The first screen lets you choose a language for displayed messages. The next screen is the main installation window (Figure 2). Select the option according to your operating system and click the button in the lower left corner.



Adaptec EZ-SCSI Software
APC PowerChute plus v5.01 for Windows
APC PowerXtend v3.0 for Netfinity Manage
Client Services for Netfinity for Netware (I
Client Services for Netfinity for Windows I
Diskette Factory for Windows 95/NT
IBM Cluster Systems Management (Englis
IBM Netfinity Manager for Windows NT
IBM Netfinity Rack Configurator
IBM ServeRAID Administration and Monit
IBM Update Connector for NetWare from a
IBM Update Connector for Windows NT
Norton AntiVirus (OEM Version) for Windo
Windows NT 4.0 Device Driver for the Net
Windows NT 4.0 Device Driver for the Net

Use the Adaptec EZ-SCSI Software applications (for Windows NT and Windows 95 operating systems) to help you connect and manage a variety of SCSI devices and peripherals.

Some of the applications included are:

List of products you can install from the CoPilot ApplicationGuide.

Figure 2. CoPilot ApplicationGuide Main Installation Screen in Microsoft Windows NT 4.0

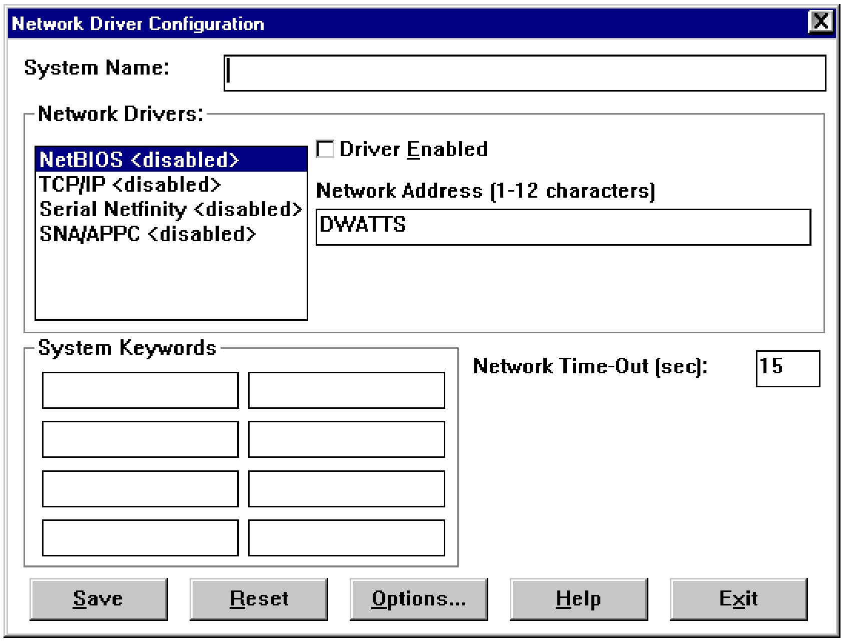
Alternatively, you can install Netfinity Manager from the file browser or command prompt.

You will find the program code in

```
<CD-ROM>:\NETFIN\<your-language>\<your-OS>\NETFINST.EXE
```

2.2.1.1 Network Driver Configuration

After installation, Figure 3 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 3. Network Driver Configuration

This window 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 dial-up 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 automatically in the Network Address field. To change this default name, enter a new address. However, this address must be unique to the 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.

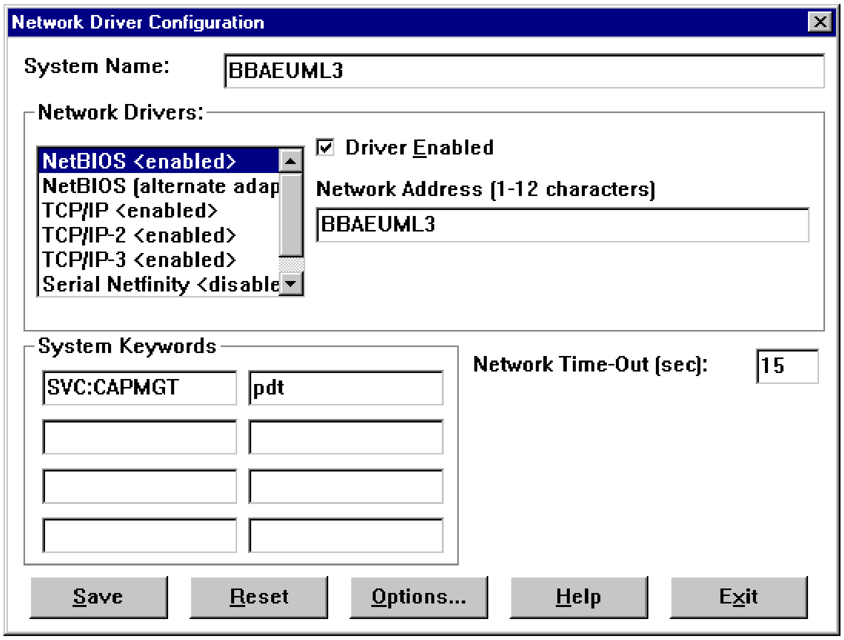
  When enabling the Serial Netfinity driver, identify the system with a Unique Machine Dialup Name. This name can be up to 32 characters long, and must be unique to the system. If this name is not unique, it can prevent remote Netfinity Managers from using the Serial Connection Control service to access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

- **More than one network adapter**

  If your system contains more than one network adapter, Netfinity Manager will only work with the first two or four drivers in the binding order:

  – NetBIOS: Netfinity Manager only works with the first two network drivers in the binding order of the NetBEUI protocol. All other network drivers in the binding order are ignored.

  – TCP/IP: Netfinity Manager only works with the first four network drivers in the binding order.



Network Driver Configuration

System Name: BBAEUML3

Network Drivers:

- NetBIOS <enabled>
- NetBIOS (alternate adap
- TCP/IP <enabled>
- TCP/IP-2 <enabled>
- TCP/IP-3 <enabled>
- Serial Netfinity <disable

☑ Driver Enabled

Network Address (1-12 characters): BBAEUML3

System Keywords: SVC:CAPMGT pdt

Network Time-Out (sec): 15

Figure 4. Multiple Network Adapters

Figure 4 shows a configuration for three network adapters under Microsoft Windows NT 4.0 at installation time.

The system has two network adapters (one Ethernet, one token-ring) and a modem installed. The token-ring adapter was installed after the modem and Ethernet adapter. Therefore the default binding order was:

1. Ethernet
2. Modem
3. Token-ring

Since Netfinity Manager supports only the first two networks in the binding order for NetBIOS, token-ring was ignored. To correct this we opened **Control Panel -> Network -> Bindings** and adjusted the order of the listed protocols so that the first two were the ones we want to access via NetBIOS.

- **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 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.

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 remove all accesses from the <PUBLIC> user.

> **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 box remains checked, <PUBLIC> users (that is, those users not having a user ID and password) will still have the ability to change their security access to all other functions.

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 from 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 the **Install** button.
6. When prompted, change your installation drive to your mapped network drive and change the directory name to NETFIN.
7. When prompted, select the Client Services network interfaces you want enabled on your NetWare server.

   Note: Do *not* enable **Serial Netfinity**. Serial connections on 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 manually issue the two commands in step 8.

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 issue the following two commands:

   ```
   search add <vol>:netfin
   load netfbase.nlm
   ```

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

```
LOAD NFCONFIG.NLM
```

2.2.3 SCO UnixWare

To install Client Services for Netfinity Manager on SCO UnixWare 7, issue the following command:

```
pkgadd -d CDDriverName
```

where CDDriverName is your CD-ROM, for example /dev/cdrom/c1b0t0l0. When prompted, select the Netfinity package.

For more information, see the README.SCO file on the CD-ROM.

2.3 Functions

The Netfinity Manager main window consists of a set of icons that constitute the user interface component of Netfinity Manager and provide an interface to the base services that perform all the interactions with the hardware and communications drivers.

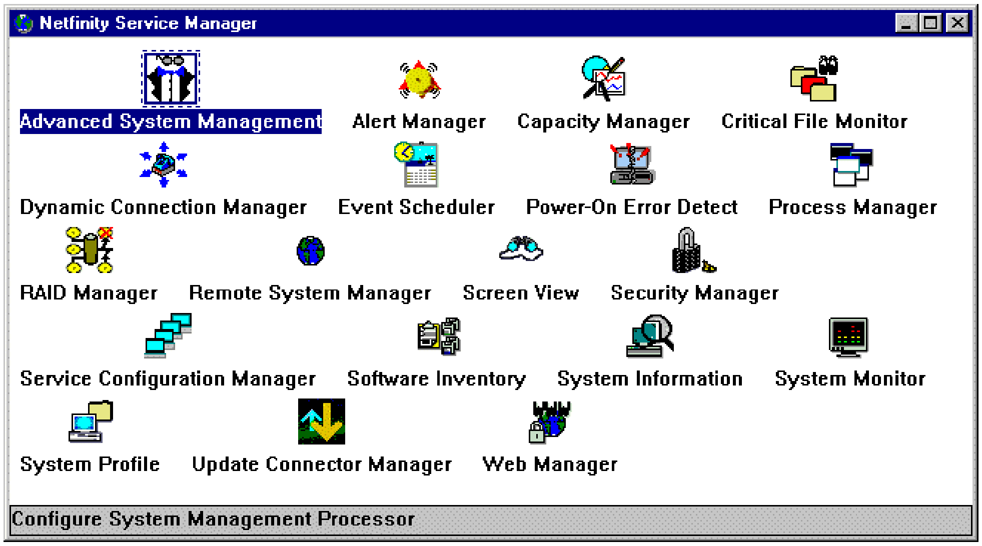


Figure 5. A Typical Netfinity Manager Window

The functions that are available in a standard installation are briefly discussed below. 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 in PDF format in the DOCS directory of the Netfinity Manager CD-ROM:

- NFMGRCR.PDF -- Netfinity Manager Command Reference
- NFMGRQB.PDF -- Netfinity Manager Quick Beginnings
- NFMGRUG.PDF -- Netfinity Manager User's Guide
- NFSVCNW.PDF -- Client Services for Netfinity for NetWare User's Guide
- NFSVCQB.PDF -- Client Services for Netfinity Quick Beginnings
- NFSVCUG.PDF -- Client Services for Netfinity User's Guide
- ASMUPDT.PDF -- Advanced System Management Information Update

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

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

INF files can be viewed without additional software under OS/2. The viewer for Windows (XVIEW) can be obtained from the Web by going to the following URL and searching on XVIEW:

```
http://www.pc.ibm.com/support
```

2.3.1 Advanced System Management

Advanced System Management

The Advanced System Management service (recently renamed from Service Processor Manager) enables communication between Netfinity Manager and the Advanced System Management processors and adapters. 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 time-outs, 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 System Management processor or adapter.

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 4, "Integrating Netfinity Manager with Netfinity Servers" on page 101.

Note: This icon only appears if you select **Advanced System Management Support** during Netfinity Manager installation.

2.3.2 Alert Manager

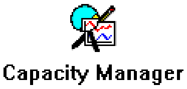
The Alert Manager is an extensible facility that allows receiving and processing of application-generated alerts. A predefined set of alert profiles is available to monitor the subsystems of the servers (for example RAID alerts, PFA alerts, ECC memory monitors).

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 a simple network management protocol (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 25.

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 can 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 Management's functions, making it especially simple to learn and understand this service.

Notes:

1. 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.
2. Capacity Management is a new function to Netfinity Manager V5.1. To collect data from a remote system, that system must be running Netfinity V5.1 or higher.

See Chapter 6, “Netfinity Capacity Manager” on page 155 for details on Capacity Manager.

2.3.4 Cluster Management

Cluster Manager

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 administrator consoles you've configured. Double-clicking on this icon starts IBM Cluster Systems Management, IBM's tool for improved MSCS management.

2.3.5 Critical File Monitor

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 Dynamic Connection Control

Dynamic Connection Manager

The Dynamic Connection Manager function enables remote Netfinity Manager managers to access your system through either a phone line and modem, a null modem cable or through the RS-485 connection of the Advanced System Management device in your server. Your system must have a properly installed and configured modem that supports at least 9600 bps for the function to work.

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

Dynamic Connection Manager is a replacement for the Serial Connection Control function of earlier versions of Netfinity Manager. However, if you don't select **Advanced System Management Support** during installation, you'll get Serial Connection Control instead, which lets you connect to modems and null modems only.

Dynamic Connection Manager is discussed in detail in Chapter 4, "Integrating Netfinity Manager with Netfinity Servers" on page 101.

2.3.7 ECC Memory Setup

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.

This service supports only specific implementations of ECC. Currently, only the PC Server 704 and the Netfinity 7000 are supported.

2.3.8 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 it requires a valid incoming user ID and password. See 2.7, "Netfinity Manager Security Implications" on page 48 for further details.

2.3.9 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.

2.3.10 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 for 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 led 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.

2.3.11 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 25 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.

2.3.12 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.

2.3.13 Remote Session

Remote Session

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

2.3.14 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:

   `http://www.pc.ibm.com/us/software/netfinity`

   See 2.6, “Netfinity Rack Configurator” on page 45 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.

2.3.14.1 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 automatically discover LAN-attached client workstations running Netfinity Manager. 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.

2.3.14.2 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 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 respond 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. Additions to the TCPADDR.DSC take effect immediately. You do not need to restart Netfinity Manager. The next discovery operation will use the new entries in the file.
4. These two examples are valid definitions within the IBM Intranet only.

2.3.14.3 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 configurations.

Table 1. System-Defined Keywords

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
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

Keyword	Explanation
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.

2.3.15 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 such as 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, such as serial connections through a modem. We recommend that you use at least a 14.4 kbps modem.

Modem Not Supported

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

2.3.16 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 and creates less network overhead.

2.3.17 Security Manager

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 remove all accesses from the <PUBLIC> user. 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.

Note: If you are working remotely through Remote Systems Manager and you modify the <PUBLIC> user ID to remove its accesses, you should create another ID *before* you change <PUBLIC>.

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.

2.3.18 Serial Connection Control

Serial Control

When you select Advanced System Management Support during Netfinity Manager installation, Serial Connection Control is replaced by Dynamic Connection Manager, which provides network and RS-485 connectivity as well as the serial connectivity provided by Serial Connection Control. See 2.3.6, “Dynamic Connection Control” on page 14 for more information.

2.3.19 Service Configuration Manager

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 any 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.

2.3.20 Service Processor Manager

Service Processor

The Service Processor Manager was renamed to Advanced System Management in Netfinity Manager Version 5.10.4. See 2.3.1, “Advanced System Management” on page 12 for more information.

2.3.21 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 Information Tool functions from the command line using the NFSYSICL command. See Chapter 11 of *Netfinity Manager Command Reference* for details.

2.3.22 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 these are NT functions. 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 36 for more information on the UPS extensions. Also see Chapter 5, “Management Functions in Netfinity Servers” on page 127 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.

2.3.23 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 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 functions. This enables you to do remote system management over the Internet, without having to install Netfinity Manager.

Note: The Remote Workstation Control and many 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.

2.3.24 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 the current range of Netfinity or PC Servers.

- DMI Browser

  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

  Power-On Error Detect

  The Power-On Error Detect service is available only 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.

- 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 by 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 available only on Micro Channel systems that 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 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, for example, 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 full list of alerts generated by the base Netfinity Manager functions can be found in Appendix J “Netfinity Alerts” of the *Netfinity Manager User’s Guide*. A full list of alerts generated by the Advanced System Management PCI Adapter and Advanced System Management Processor can be found in Appendix A, “Advanced System Management Alerts” on page 265.

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 heart of the alerting function 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, carries out the appropriate action.

To start Alert Manager, double-click its icon in the Netfinity Manager Main Window. You will then see Figure 6 which also doubles as the alert log.

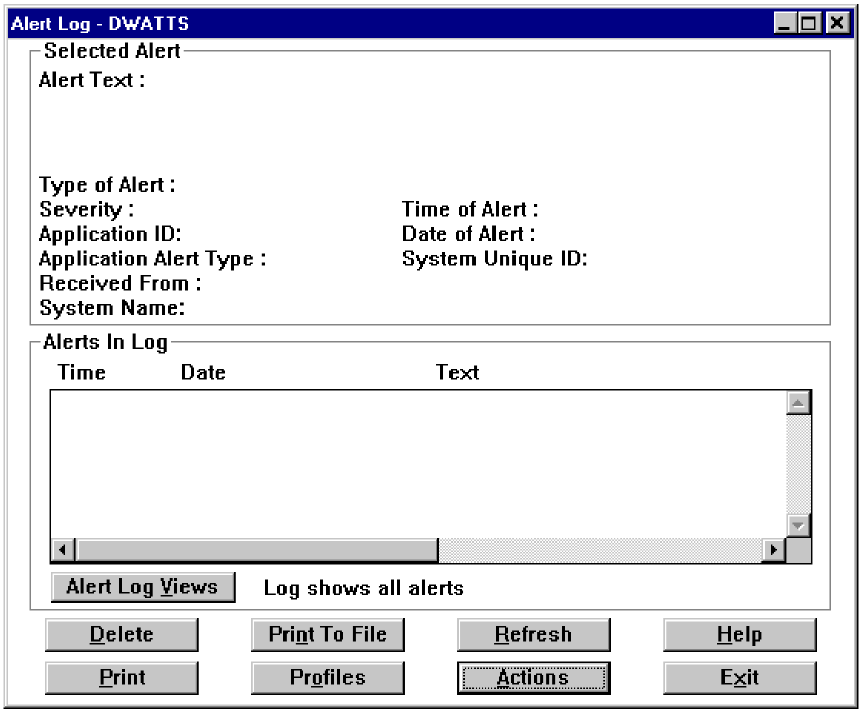


Figure 6. Alert Manager: Main Window

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 is 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 an 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*).

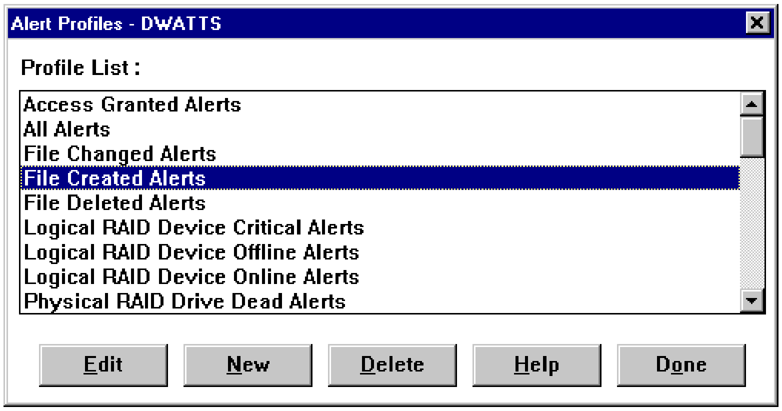
There is no significant difference between these two methods except that defining a profile before binding it to an action gives you a little more control over the alerts and allows you to give each action a name. If you plan to have multiple actions as a result of a single alert, it will be easier if 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 27. The second is described in 2.4.3, “Defining an Action from an Alert Using a Condition” on page 32.

2.4.2 Defining an Action from an Alert Using a Profile

From the main window, click the **Profiles** button. You will then see Figure 7. 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 appear here also.

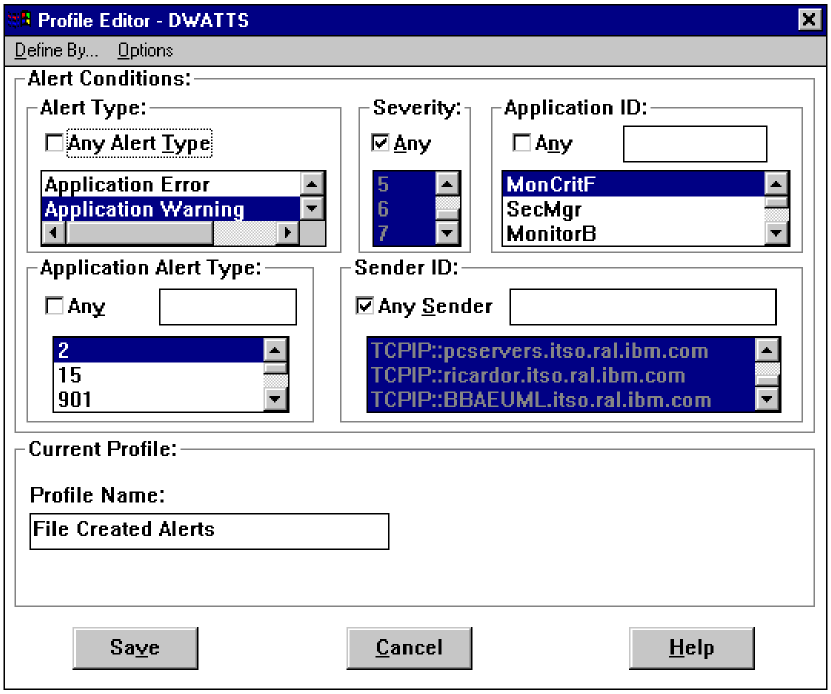
See “Predefined Alert Profiles” in Chapter 2 of *Netfinity Manager User’s Guide* for a description of the predefined profiles.



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 7. Alert Manager: List of Defined Profiles

Here you can work with an existing profile or create new ones. Select the **File Created Alerts** profile and click **Edit**. The Profile Editor window, shown in Figure 8, now appears.



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 8. 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

The profile editor shown in Figure 8 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 check box to select all Alert types.

Severity

These have values 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 normal conditions.

For example, if you want to know what the alert values are when a system exceeds a temperature threshold, set up the alert 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 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. 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
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
ServeProc	IBM Advanced System Management 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 of 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 workstation's 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

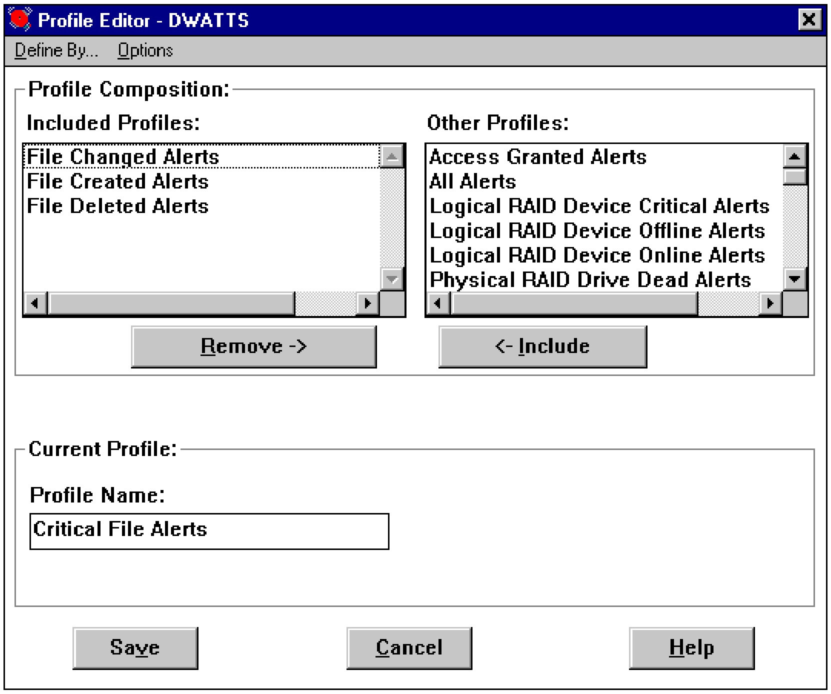
This is the name of the profile. This can be up to 64 characters in length. We advise that you make this name meaningful and describe the alert profile you have just set up.

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 28, you also can use the Profile Editor to create a profile based on *multiple profiles*. This has the effect of funneling 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 9 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

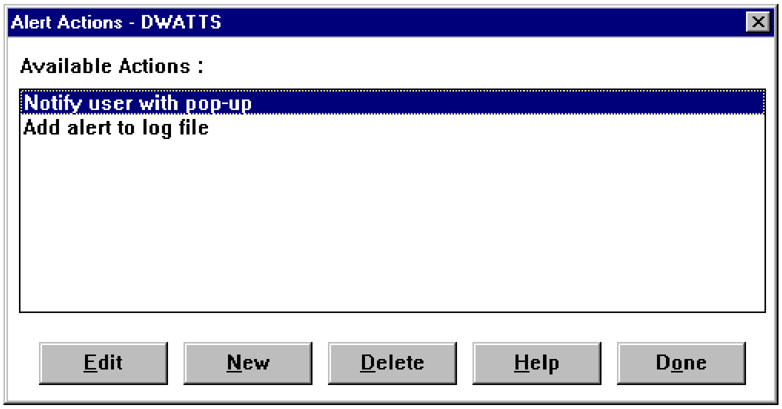
Figure 9. Alert Manager: Profile Editor by Profile Composition

Select the profiles you want to include, then click the **Include** button. Give the new profile a name of up to 64 characters, then click **Save** to save the profile, then **Yes** to confirm the save. Your new profile will then appear 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 the **Actions** button and Figure 10 will appear:



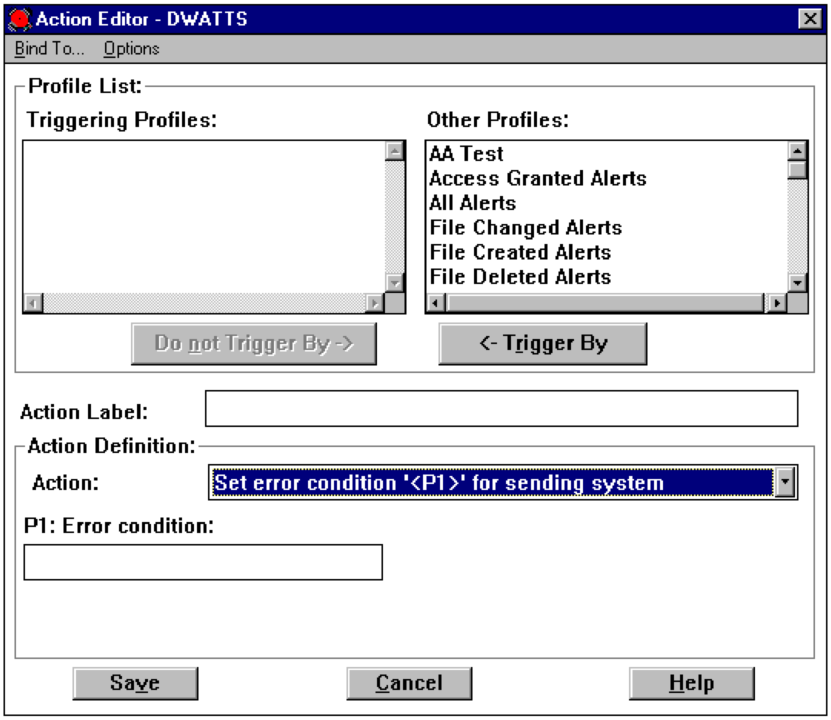
Available Actions :

Notify user with pop-up
Add alert to log file

Figure 10. Alert Manager: Alert Actions

You will see that two actions are defined. These two (as shown in Figure 10) 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 32. For now, click the **New** button.

The Action Editor window now appears. Click **Bind To... -> Profiles**. Figure 11 appears:



Action Editor - DWATTS

Profile List:

Triggering Profiles:

Other Profiles:

AA Test
Access Granted Alerts
All Alerts
File Changed Alerts
File Created Alerts
File Deleted Alerts

Action Label:

Action Definition:

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

P1: Error condition:

Figure 11. Alert Manager: Action Editor Using Profiles

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

Now, specify a name for the action you are about to set (up to 22 characters), then the specific 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 33.

Save the action by clicking **Save**, then confirm the save by clicking **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 26, a second and 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 27.

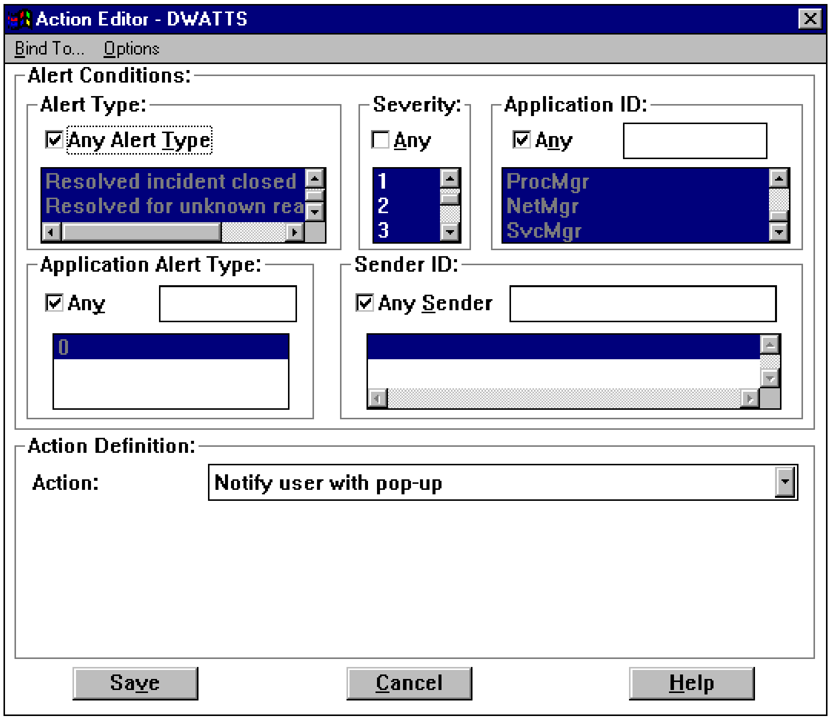
Even though this method is quicker, it does offer some disadvantages:

- You are not able to give the alert a name.
- Using profiles is easier 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 the **Actions** button. You will be presented with the list of currently defined actions as shown in Figure 10.

Select the action **Notify user with pop-up** and click the **Edit** button. Figure 12 appears.

Note: If you see Figure 11 instead, click **Bind To... -> Alert Conditions** and the window should appear.



☑ Any Alert Type

Resolved incident closed
Resolved for unknown rea

☐ Any

1
2
3

☑ Any

ProcMgr
NetMgr
SvcMgr

☑ Any

0

☑ Any Sender

Action: Notify user with pop-up

Figure 12. 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 28 except that instead of specifying a profile name, you specify an alert condition.

In the window in Figure 12, the action is to “Notify user with pop-up”, and in this case, no additional parameters are required. See 2.4.4, “Alert Actions” on page 33 for a complete description of all the actions available.

Once you select the appropriate action, click **Save**, then confirm the save by clicking **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) lists all actions that can be set to occur on the server itself. The second table (Table 6) 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 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 a 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 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

With the “Execute a command” action, you can add parameters to the command to pass information from the alert itself. These parameters are:

%TXT	Alert text
%TIM	Alert time
%DAT	Alert date
%SEV	Alert severity
%SND	Sender (for example, NETBIOS::SERVER1)
%APP	Application ID
%AT	Application alert type
%P1-%P9	Alert specific strings. See Appendix J of *Netfinity Manager User’s Guide* for the use of these for specific alerts.

Table 6 lists all the actions that involve sending an alert to some other system:

Table 6. Actions Available with Netfinity Manager – Remote

Action	**Description/Prerequisites**
Forward alert to another Netfinity workstation	Available on all systems.

Action	Description/Prerequisites
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/95/98: requires the SNMP service • Not available on Windows 3.1 For NT, install SNMP from Services in Control Panel. For 95/98, install from the Windows CD-ROM: \tools\reskit \netadmin\snmp for Windows 98 and \admin\nettools\snmp for Windows 95.
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/95/98: requires the SNMP service • Not available on Windows 3.1
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
Send alert as TCP/IP mail	Sends a text-only e-mail 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 e-mail message. Requires OS/2 with TCP/IP V2.0 or later.
Send to e-mail via VIM interface	Uses Vendor Independent Messaging (VIM) to generate an alert. Requires: • VIM-compliant system (for example, Notes or cc:Mail) • OS/2 or Windows NT or Windows 95
Send alert as e-mail 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	Converts 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 4.2.6.5, “System Alerts” on page 120 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 that allow the 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 control either a UPS connected to the system on which the software is being installed, 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 its 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

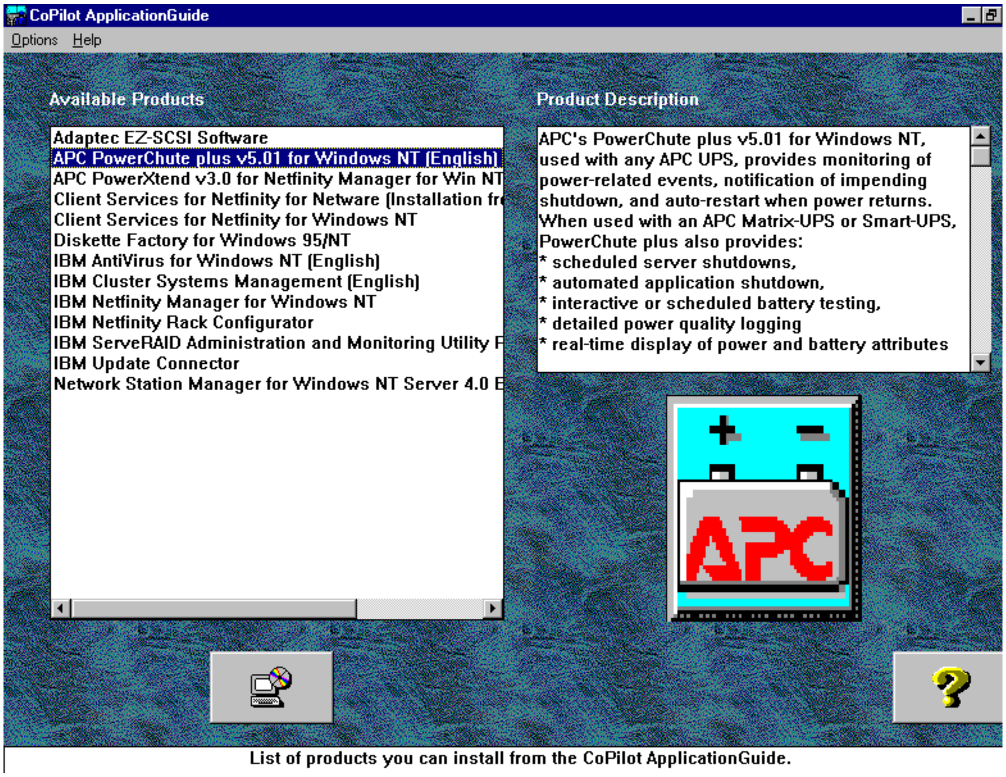
PowerChute and PowerXtend must be installed on both the Netfinity Manager and any machine whose UPS information you want to manage via Netfinity Manager. PowerChute must be installed before installing PowerXtend.

Note: Before starting the installation make sure the UPS is connected to a COM port on the server. If you have an Advanced Systems Management Adapter installed also, 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 start automatically. For OS/2, insert the CD-ROM and run `OS2SC.CMD`. Figure 13 appears for Windows systems and a similar window appears for OS/2:



Available Products

- Adaptec EZ-SCSI Software
- APC PowerChute plus v5.01 for Windows NT (English)
- APC PowerXtend v3.0 for Netfinity Manager for Win NT
- Client Services for Netfinity for Netware (Installation fr
- Client Services for Netfinity for Windows NT
- Diskette Factory for Windows 95/NT
- IBM AntiVirus for Windows NT (English)
- IBM Cluster Systems Management (English)
- IBM Netfinity Manager for Windows NT
- IBM Netfinity Rack Configurator
- IBM ServeRAID Administration and Monitoring Utility F
- IBM Update Connector
- Network Station Manager for Windows NT Server 4.0 E

Product Description

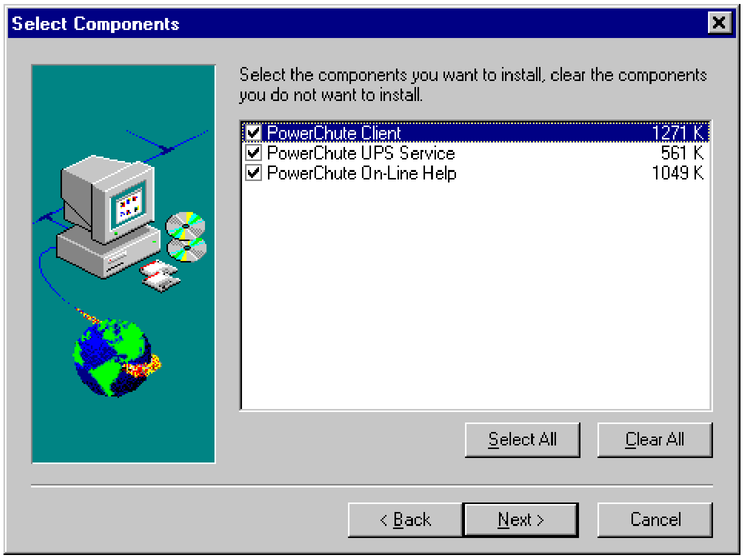
APC's PowerChute plus v5.01 for Windows NT, used with any APC UPS, provides monitoring of power-related events, notification of impending shutdown, and auto-restart when power returns. When used with an APC Matrix-UPS or Smart-UPS, PowerChute plus also provides:
* scheduled server shutdowns,
* automated application shutdown,
* interactive or scheduled battery testing,
* detailed power quality logging
* real-time display of power and battery attributes

List of products you can install from the CoPilot ApplicationGuide.

Figure 13. ServerGuide Installation of PowerChute

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

If you are installing the PowerChute software on the server you would normally take the Typical installation path. However, you can choose the Custom installation path, which lets you configure PowerChute as shown in Figure 14:



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 14. Selecting Components in a Custom Installation

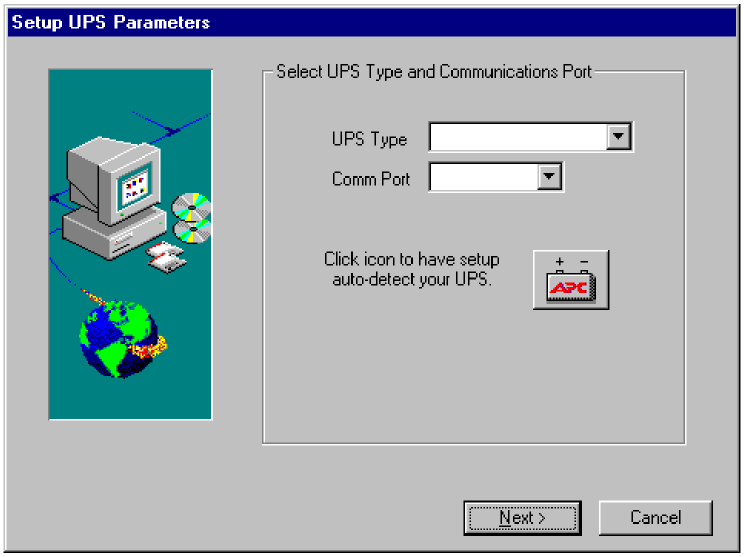
Select the options based on your requirements:

- 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 want to manage only 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 **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 15 appears, prompting you to specify what type of UPS you have and to which COM port you have it attached.


Setup UPS Parameters

Select UPS Type and Communications Port

UPS Type

Comm Port

Click icon to have setup auto-detect your UPS.

Figure 15. Selecting Components in a Custom Installation

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

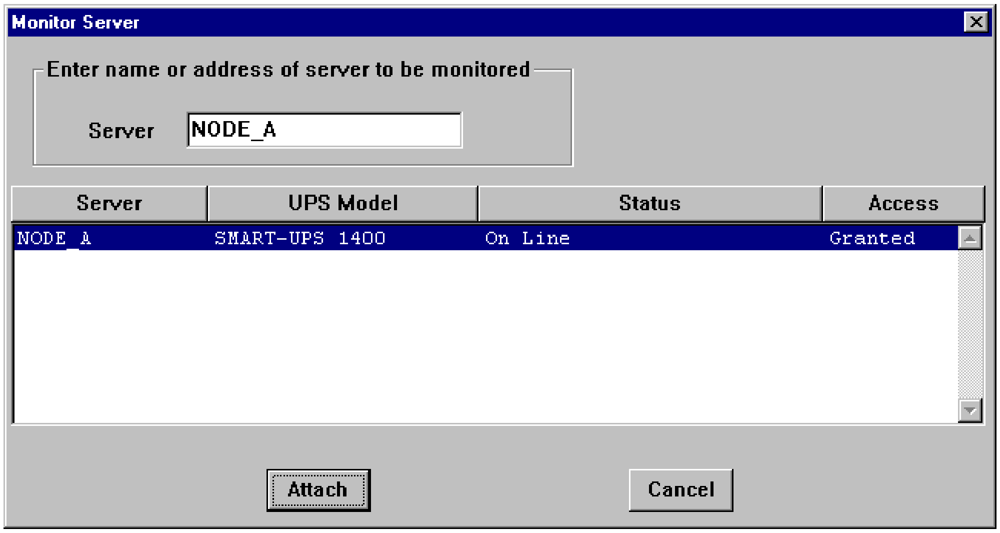
2.5.2 Installing PowerXtend

Once the installation of PowerChute is complete you can then use ServerGuide to install PowerXtend by selecting it from the CoPilot window in Figure 13.

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.

2.5.3 PowerChute

Starting PowerChute displays a window, Figure 16, which lets you choose to which UPS you wish to connect. 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 **Attach**.

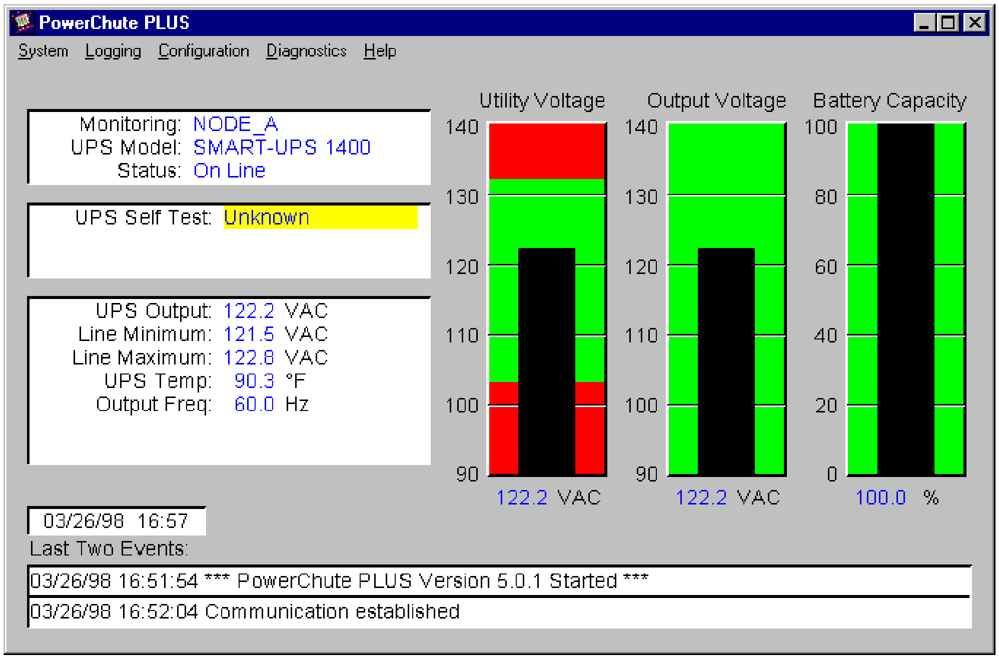


Server: NODE_A

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

Figure 16. Selecting a UPS to Access

When you click **Attach**, Figure 17 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

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

Figure 17. PowerChute Main Window

From here you can control directly 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, and 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 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 connection block for sensors that require power.

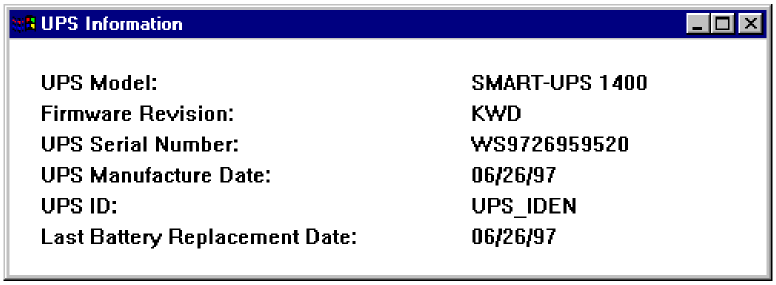
For more information about the Measure-UPS device, see Appendix B of the *PowerChute plus User’s Guide*.

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

PowerXtend supplies another icon on the Netfinity Manager main window that you can use to display information about the UPS. When you double-click the icon, Figure 18 appears showing details about the UPS connected to this system:



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 18. UPS Information Window

2.5.5.2 System Monitor Enhancements

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

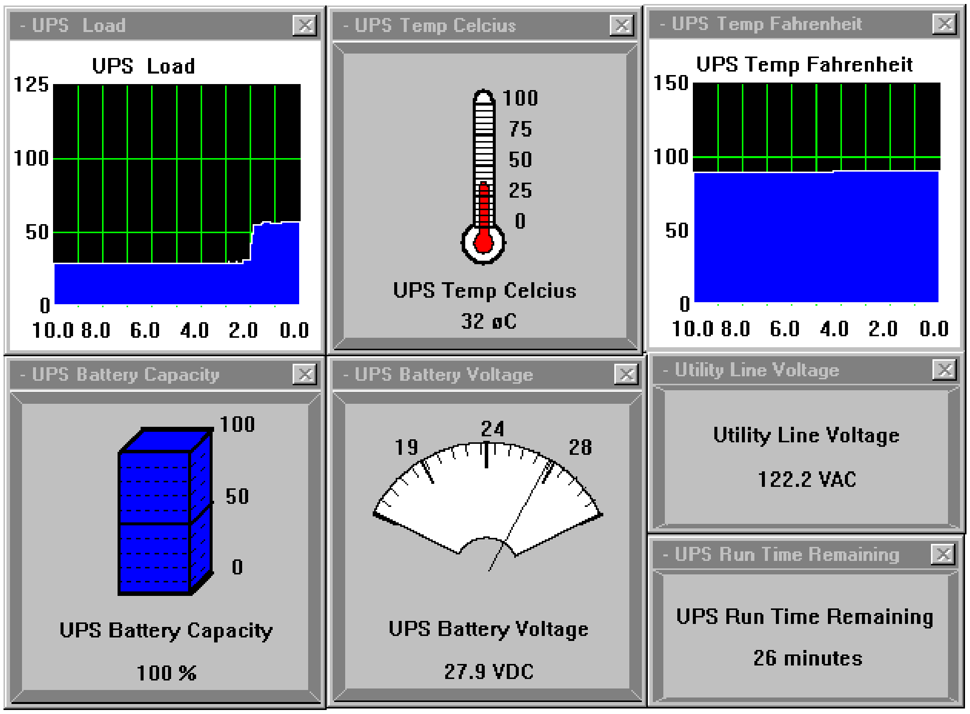


Figure 19. UPS Monitoring Data Displayed by System Monitor

- 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 19, 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 20:

- 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.

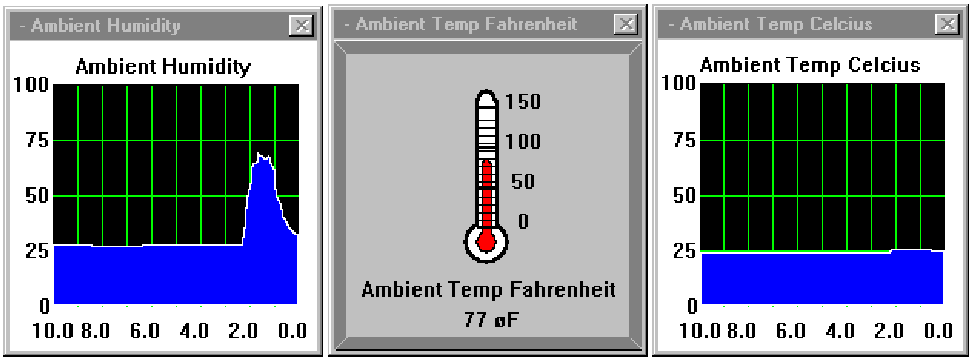


Figure 20. Additional Monitors Using the Measure-UPS Device

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 shows all the alert types generated by the application ID “PwrChute”:

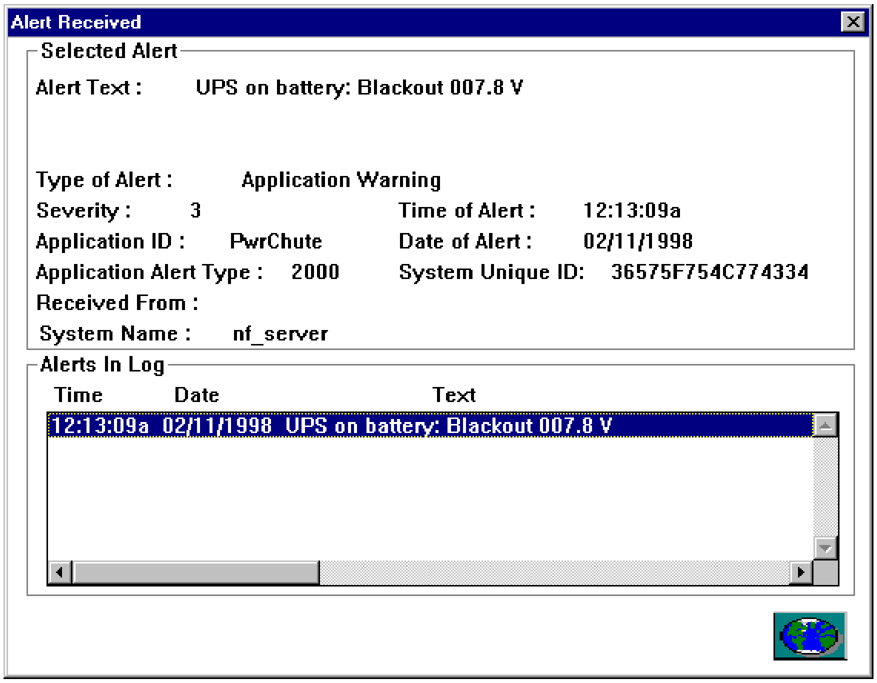
Table 7. Application Alert Types Generated by PowerChute and PowerXtend

Type	Description
1000	PowerChute Started
1001	PowerChute Stopped
1002	Communication Established
1003	Power Restored
1004	UPS Self-Test Passed
1005	Administrative Shutdown
1006	Shutdown Canceled
1007	UPS Return From Low Battery
1009	UPS Battery No Longer Needs Replacing
1010*	Contact Normal

Type	Description
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 Canceled
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 (*) occur only 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 21:



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 21. UPS Alert Displayed by Netfinity Alert Manager

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

Warning: Do not configure Netfinity Manager to issue this action if PowerChute is already configured to automatically 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” set on by default. 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 occurs only via Netfinity Manager.

2.5.5.4 Event Scheduler Enhancements

PowerXtend supplies two additional events that 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 scheduled, 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 issues a message that the requested service is not available on that server.

2.6 Netfinity Rack Configurator

This stand-alone utility lets you specify 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 define connections to other components also and select the correct cables needed for the connection. You can create either 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/software/netfinity
```

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 Copilot window, select **IBM Netfinity Rack Configurator** and click 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

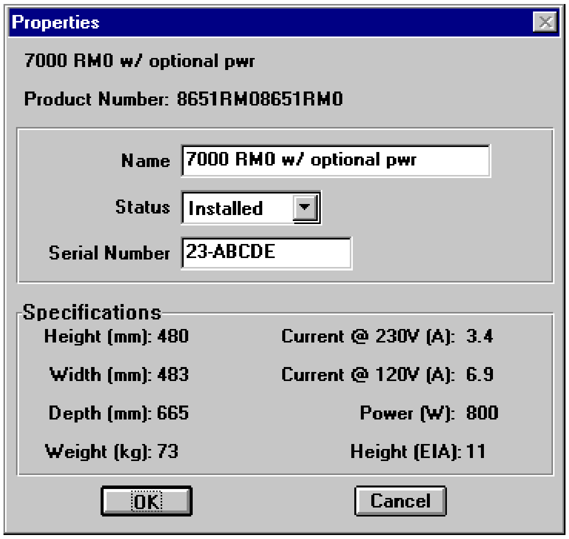
Note: Before creating the Netfinity files, you *must* have a rack configuration that has been created, validated, and built. See the program documentation for more information.

To create the Netfinity files, perform the following steps:

1. Ensure your server component has these settings (see Figure 22):

   – 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.



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

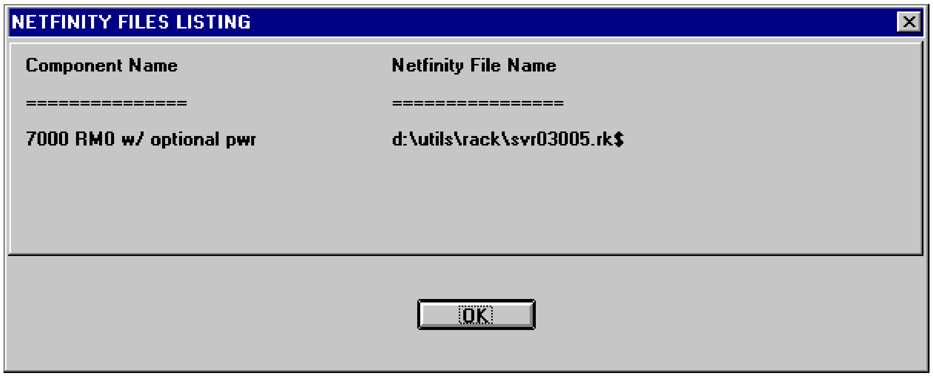
Figure 22. Server Properties Window

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. Click **Suite -> Name** in the main window.

   – Summary Info – This option allows you to set different properties for your rack configuration, such as collection name, customer name, etc. Use **Files -> Summary Info** to add this information.

3. Create the Netfinity files by selecting **Tools -> Create Netfinity Files** in the main window. A separate file is created for each server defined in the rack configuration (see Figure 23):



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

Figure 23. Sample Export File Created

Figure 24 shows a sample export file created for Netfinity 7000.

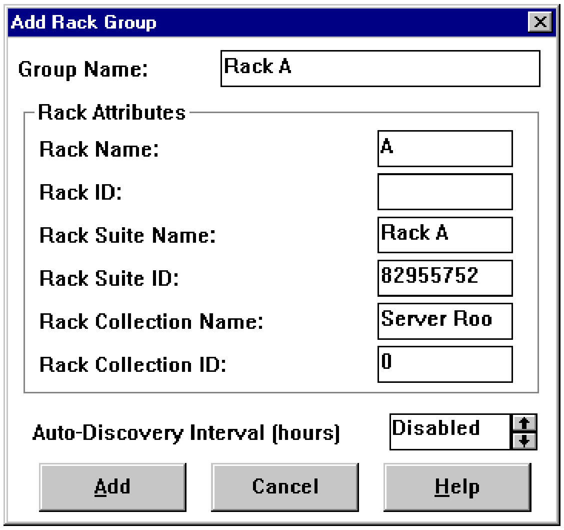
```
#========================SVR03005.RK$========================#
#
# Rack Interface File for:
#
#       COLLECTION:    “Server Room Building A”
#       RACK SUITE:    “Rack A”
#       RACK:          “A”
#       COMPONENT:     “7000 RMO w/ optional pwr”
#       COMPONENT SN: 23-ABCDE
#
# Please copy 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=8651RMO
ComponentSerialNumber=23-ABCDE
ComponentWidth=483
ComponentHeight=480
ComponentDepth=665
ComponentName=”7000 RMO w/ optional pwr”
```

Figure 24. 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 **Group -> Add Rack Group** in the Remote System Manager window.
3. Figure 25 appears.



Add Rack Group

Group Name: Rack A

Rack Attributes

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 25. Adding a Rack Group in Netfinity

4. Use the entries in the export file (Figure 24) to fill in the required fields in Figure 25.

   – 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 25	Entry in Export File (Figure 24 on page 47)
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. Click **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.

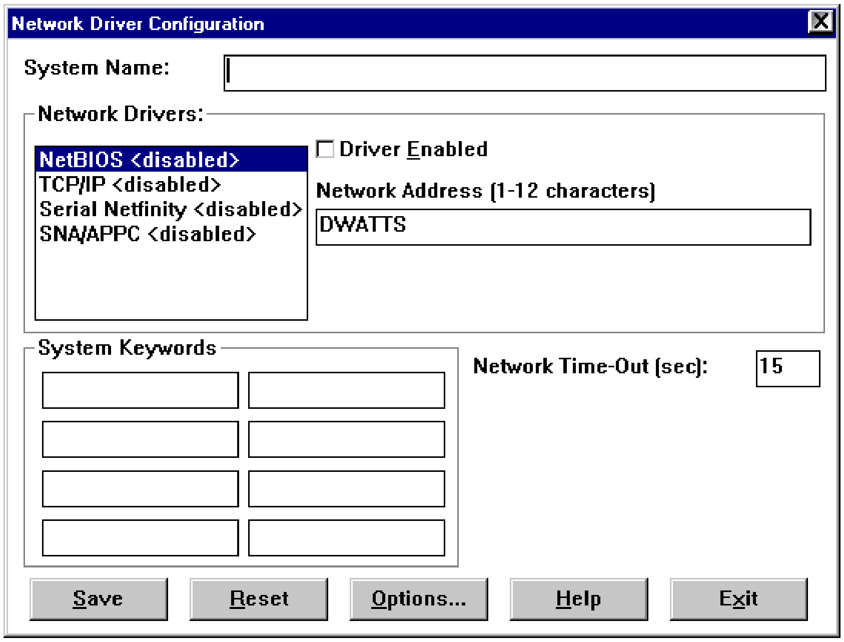
2.7 Netfinity Manager Security Implications

This section describes what security implications there are when 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 26 appears, giving you the opportunity to select and configure the network protocols available to Netfinity Manager. 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.



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

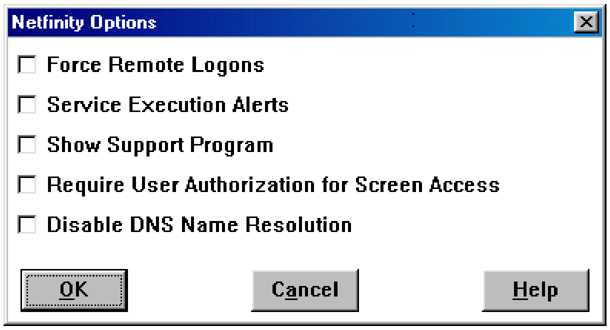
System Keywords

Network Time-Out (sec): 15

Figure 26. 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 to allow some machines 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 **Options...** This window can be seen in Figure 27:



Netfinity Options

☐ Force Remote Logons
☐ Service Execution Alerts
☐ Show Support Program
☐ Require User Authorization for Screen Access
☐ Disable DNS Name Resolution

Figure 27. Netfinity Driver Options

The Netfinity Options window contains five 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 log on manually each time to any remote system that you want to access. 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 shut down 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.

- Disable DNS Name Resolution

  If you turn on this setting, Netfinity Manager will not translate the IP address into IP names via the DNS. Instead, only the dotted IP address will be displayed in the Remote Systems Manager.

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 user ID/password combination to give access to your system to authorized users. Each user ID can have access to one or more Netfinity Manager functions. You can also use Security Manager to configure pre-set user IDs for your access to other Netfinity Manager systems.

Authentication is split into two parts:

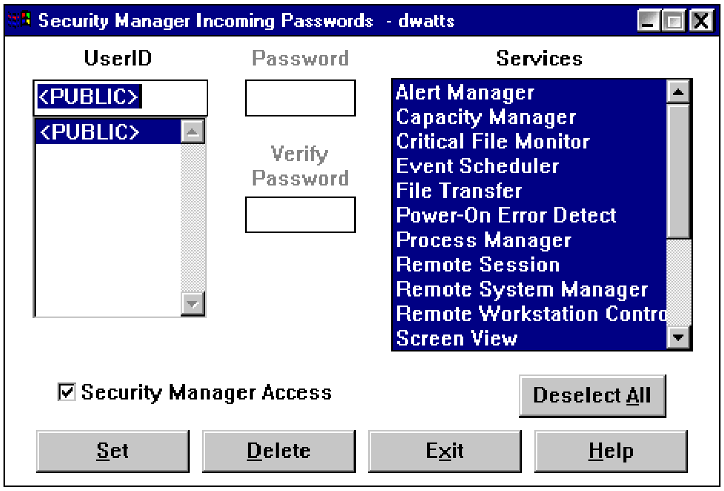
- Incoming user ID/password combinations
- Outgoing user ID/password combinations

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 57 for details.

2.7.2.1 Incoming User IDs

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



Security Manager Incoming Passwords - dwatts

UserID

<PUBLIC>

<PUBLIC>

Password

Verify Password

Services

- 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 28. Incoming Passwords

After installing Netfinity Manager, the <PUBLIC> user ID will have full access to all services, as shown in Figure 28. 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 **Set**. Failure to do so will make your system susceptible to intentional or unintentional damage.

2.7.2.2 Outgoing User IDs

This is where you set user ID/password combinations to access other Netfinity Manager systems. Initially, only the default user ID exists and is set to <PUBLIC> as shown in Figure 29:

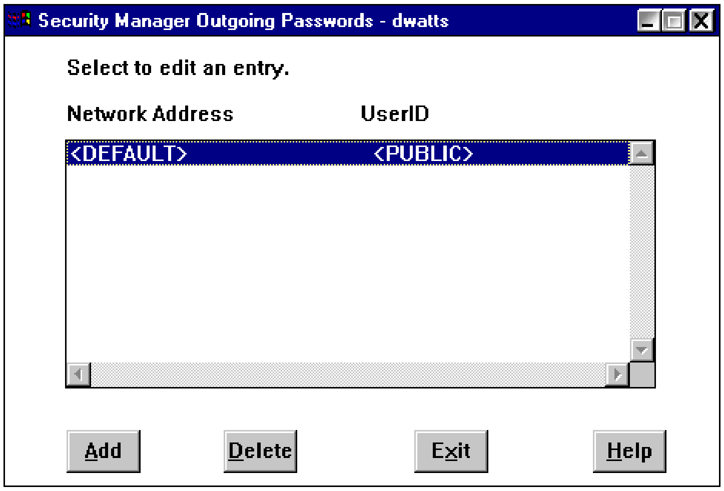


Figure 29. Initial Outgoing Passwords

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

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

1. Logging on via Remote Systems Manager

   From Remote System Manager, open the desired group and right-click the desired remote system. A pop-up window as shown in Figure 30 appears:

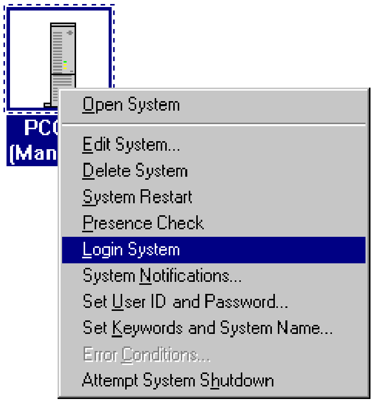


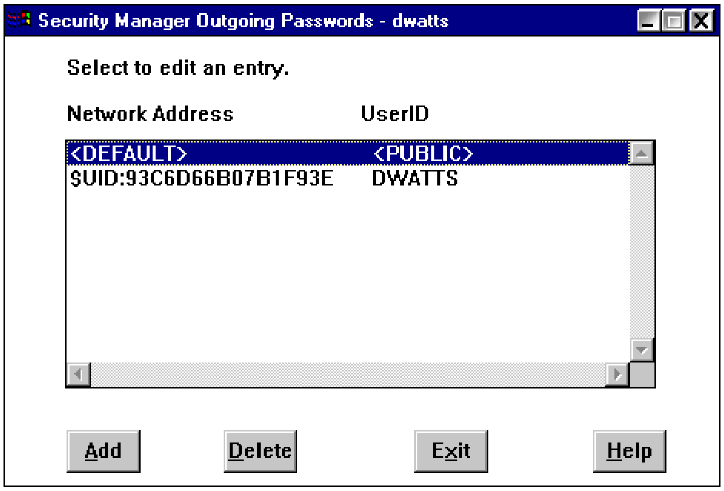
Figure 30. Logging On to a Remote System

   Click **Login System** and you will be prompted to enter a user ID and password. The 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** per 2.7.1, “Network Driver Configuration” on page 49, then you will also be prompted:

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

   If you click **Yes**, then an entry will be added to your Outgoing Passwords list, as in Figure 31:



Security Manager Outgoing Passwords - dwatts

Select to edit an entry.

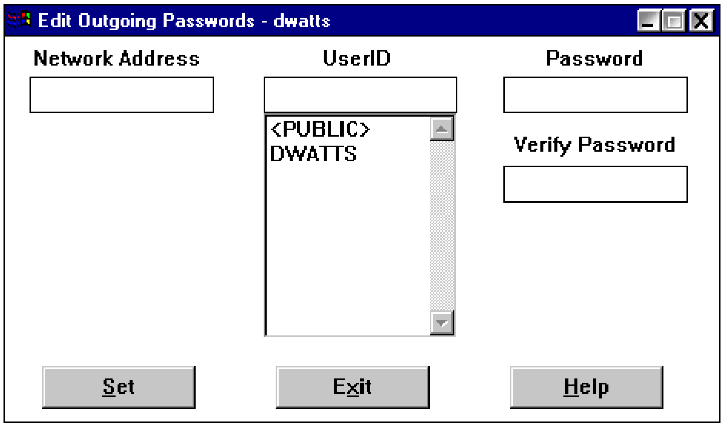
Network Address	UserID
<DEFAULT>	<PUBLIC>
$UID:93C6D66B07B1F93E	DWATTS

Figure 31. Outgoing Password Added during a Manual Logon

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

2. Adding an Entry to the Outgoing Passwords List

   From the Outgoing Passwords window (Figure 31), click **Add**. You will then see Figure 32.



Edit Outgoing Passwords - dwatts

Network Address

UserID

<PUBLIC>
DWATTS

Password

Verify Password

Figure 32. Adding an Outgoing Password Manually

From here you can type in the address of the system you want to access, and a user ID and password that match an incoming user ID 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 **Set** then **Exit**.

2.7.2.3 Password Storage and Transmission

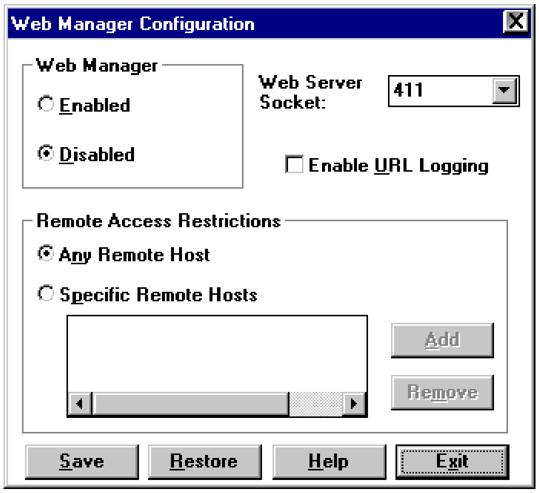
Incoming and outgoing passwords are stored in files in the Netfinity Manager directory. They are SECIN.INI and SECOUT.INI respectively. These files have the user IDs and machine IDs in plain text, but the passwords are scrambled.

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 33.


Web Manager Configuration

Web Manager
○ Enabled
● Disabled

Web Server Socket: 411

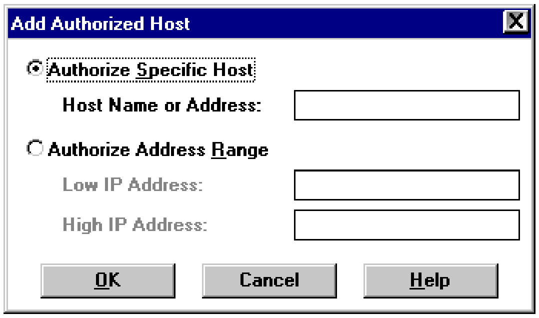
□ Enable URL Logging

Remote Access Restrictions
● Any Remote Host
○ Specific Remote Hosts

Figure 33. Web Manager Security

When enabled, all authorized systems running a Web browser, can access the Netfinity 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 specific TCP/IP addresses or ranges of addresses. To specify the TCP/IP addresses, click **Specific Remote Hosts** and Figure 34 appears:


Add Authorized Host

● Authorize Specific Host
Host Name or Address:

○ Authorize Address Range
Low IP Address:
High IP Address:

Figure 34. 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 **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 log all accesses from browsers also by clicking **Enable URL Logging**. Selecting this check box 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 two-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.

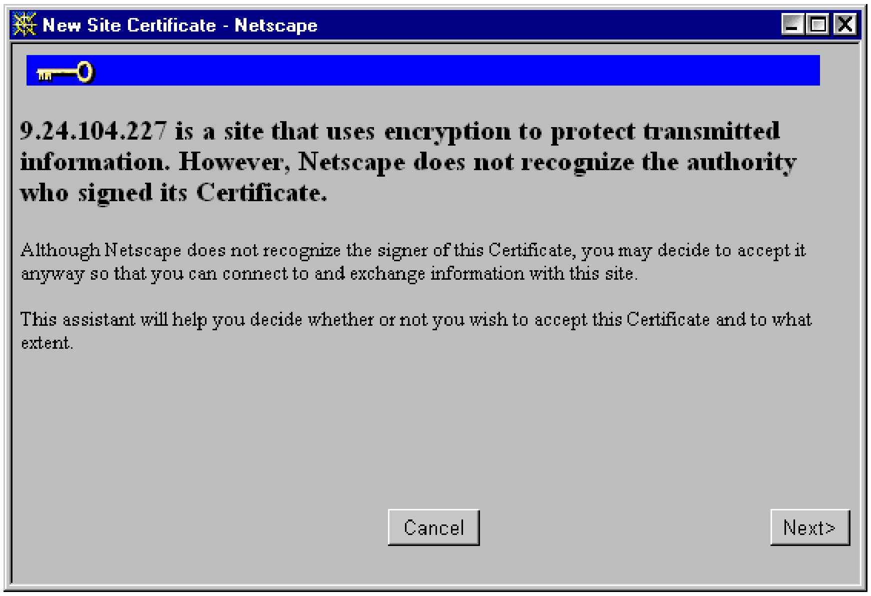
The logging action takes care to remove passwords from the log that are entered through the security service. However, this does not prevent a user from entering a password and having it logged by other services, such as while setting up an alert action to export alerts to a database.

2.7.3.1 Secure User Access

Normally, users would access the Netfinity system via the unsecured 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 to which you are connecting. If you are using Netscape Navigator, the following window will appear:



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 35. Setting Up an SSL Encryption Certificate

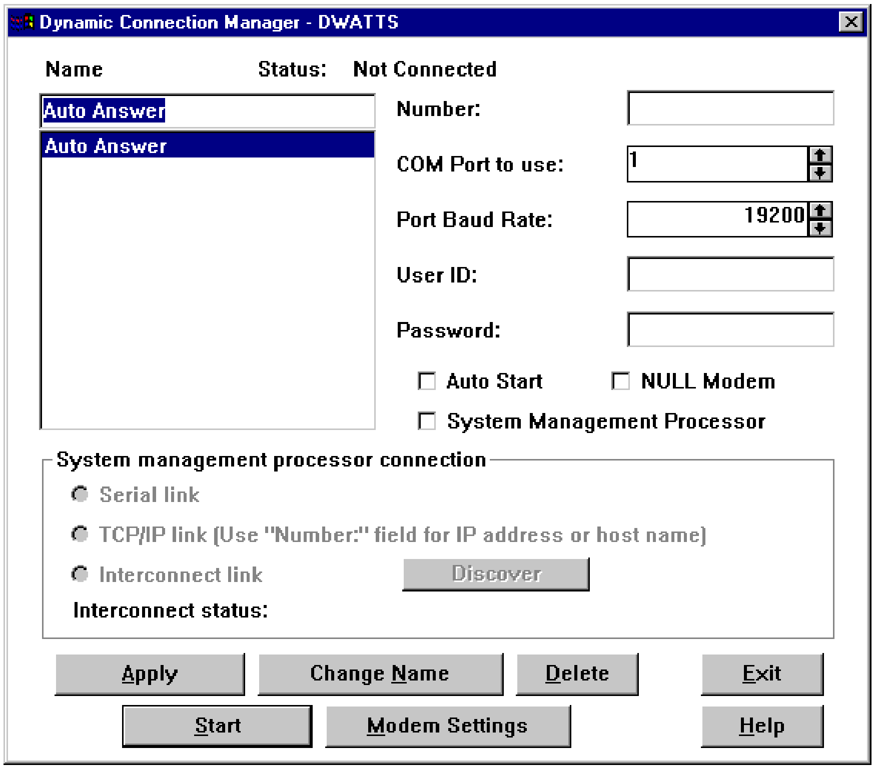
The encryption used is of Export Grade (that is, using a 40-bit encryption key). Follow the instructions on the screen to complete the security certificate issuance.

2.7.4 Serial Access

The Dynamic Connection Manager function allows you to set up user IDs that can be used to dial out to other Netfinity Manager systems. It also enables you to configure the local system to let other systems dial into it.

Dynamic Connection Manager is a replacement for the Serial Connection Control function of earlier versions of Netfinity Manager. However, if you don’t select **Advanced System Management Support** during installation, you’ll get Serial Connection Control instead, which lets you connect to modems and null modems only.

First we describe 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 Dynamic Connection Manager function (or Serial Control if you do not have Dynamic Connection Manager). You will see Figure 36:



Dynamic Connection Manager - DWATTS

Name: Auto Answer

Auto Answer

Status: Not Connected

Number:

COM Port to use: 1

Port Baud Rate: 19200

User ID:

Password:

☐ Auto Start ☐ NULL Modem

☐ System Management Processor

System management processor connection

○ Serial link

○ TCP/IP link (Use "Number:" field for IP address or host name)

○ Interconnect link

Interconnect status:

Figure 36. Netfinity Manager Serial Control

Select **Auto Answer** 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 user ID and password into the appropriate field, then click **Apply** to save the settings, then **Start**. If Serial Control can connect successfully to the modem, it sets the status at the top of the window to `Waiting for Call`.

Note: If you wish to have Auto Answer always started and available, click **Auto Start** in Figure 36. However, this will prevent the modem from 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 use the user ID/password combination you just entered. All users will have to share this user ID/password.

To connect to another Netfinity Manager system with Auto Answer enabled, you use Dynamic Connection Manager (or Serial Control) and create a new entry with the appropriate phone number and COM port. For more information about Dynamic Connection Manager, see 4.1, “Dynamic Connection Manager” on page 103.

Once remote users are connected, they would use Remote Systems Manager to access other Netfinity Manager systems. The remote users will still need a valid user ID and password that is in the Incoming Passwords list of any of the systems they want to access. This includes the system they dialed in to 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

We recommend that 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 available only with Netfinity Manager Version 5.0 or later and is only necessary when using the original IBM ServeRAID SCSI Adapter. It is not required when using newer ServeRAID adapters such as the ServeRAID II (V2.30 BIOS or later) or ServeRAID-3H/3L.

When you have only 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 40.

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

1. Double-click **Event Scheduler**. Figure 37 appears:

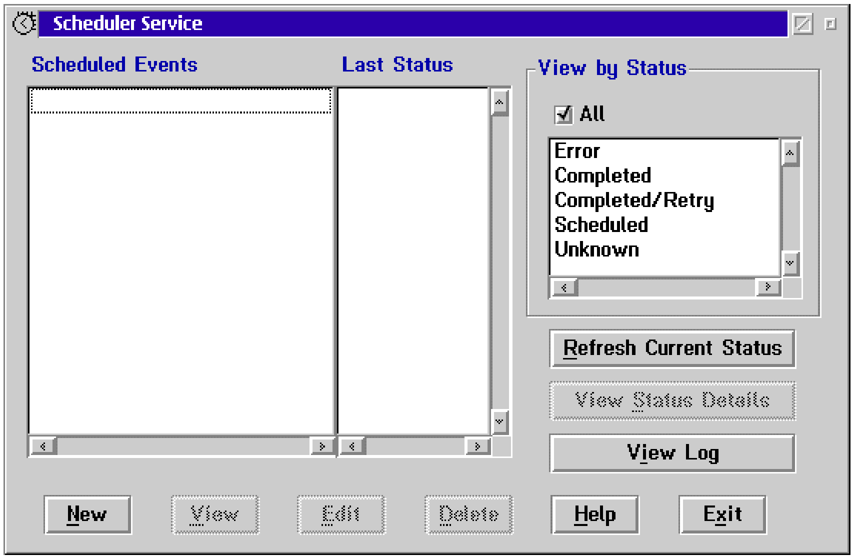
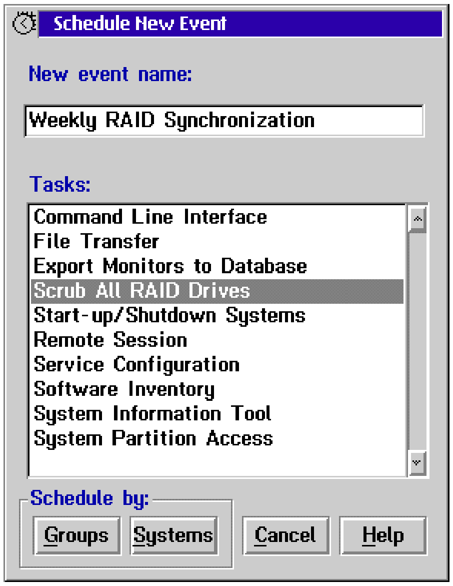


Figure 37. Event Scheduler Main Window

2. Click **New**. Figure 38 appears:



New event name: Weekly RAID Synchronization

Tasks: Scrub All RAID Drives

Figure 38. Creating a New Scheduled Event

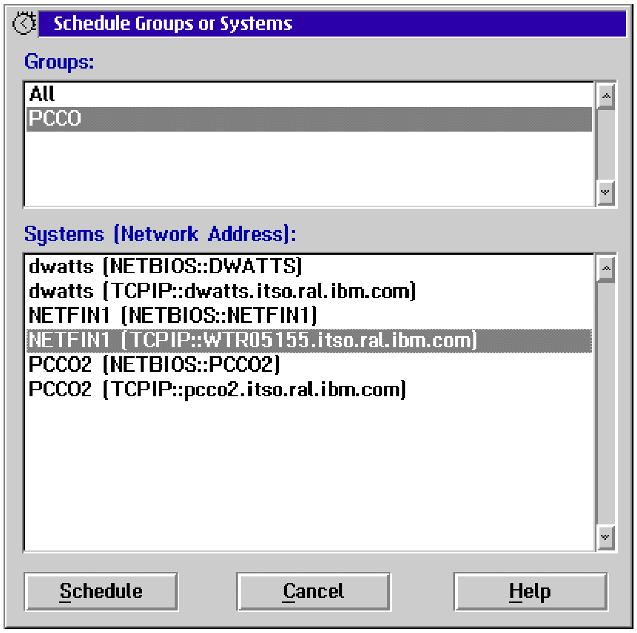
We recommend that you perform a RAID scrub every week.

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

4. Click **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 **Systems** and Figure 39 appeared:



Schedule Groups or Systems

Groups:

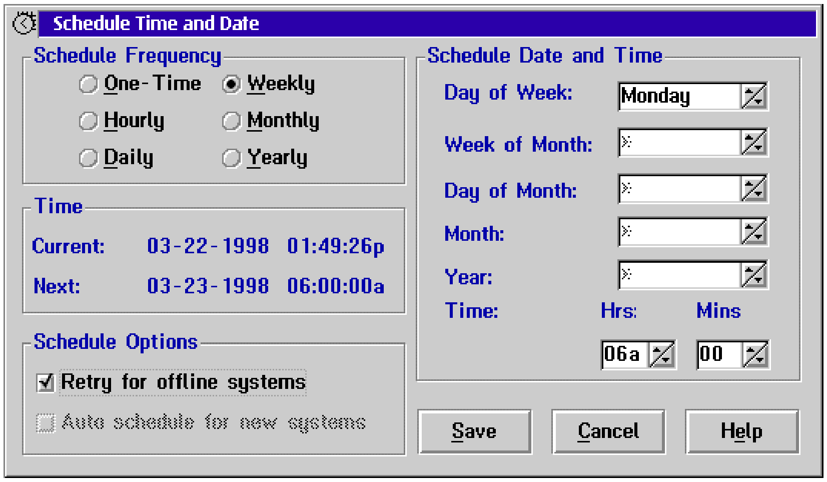
All
PCCO

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 39. Selecting the System to Schedule

5. Select the system or systems you want to schedule and click the **Schedule** button. In this case, this is the local server on which we are working. Figure 40 appears.



Schedule Time and Date

Schedule Frequency

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

Time

Current: 03-22-1998 01:49:26p
Next: 03-23-1998 06:00:00a

Schedule Options

☑ Retry for offline systems
□ Auto schedule for new systems

Schedule Date and Time

Day of Week: Monday
Week of Month:
Day of Month:
Month:
Year:
Time: Hrs: 06a Mins: 00

Figure 40. 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 39) you should also click **Retry for offline systems** to ensure network failures do not impact your RAID scrub schedule.

7. Click **Save**. Figure 41 appears:

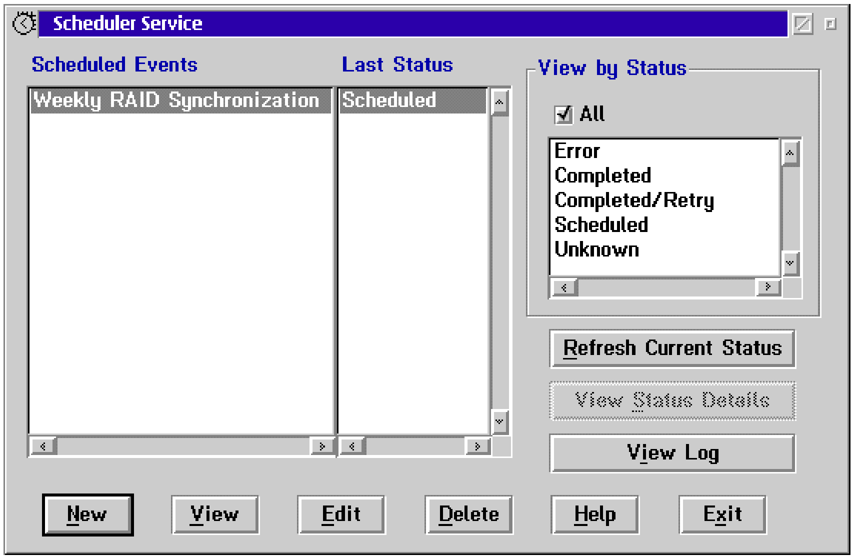


Figure 41. Scheduled Events

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

If you wish to view the status of previously run scrubs, click **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 on which you are defining the schedule. 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 **Security Manager**. Figure 42 appears:

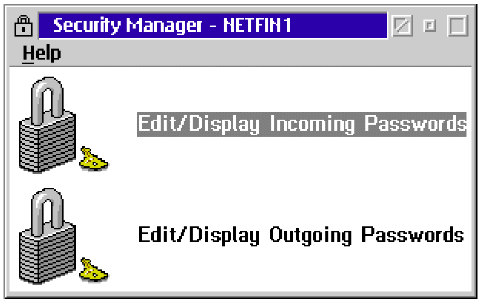
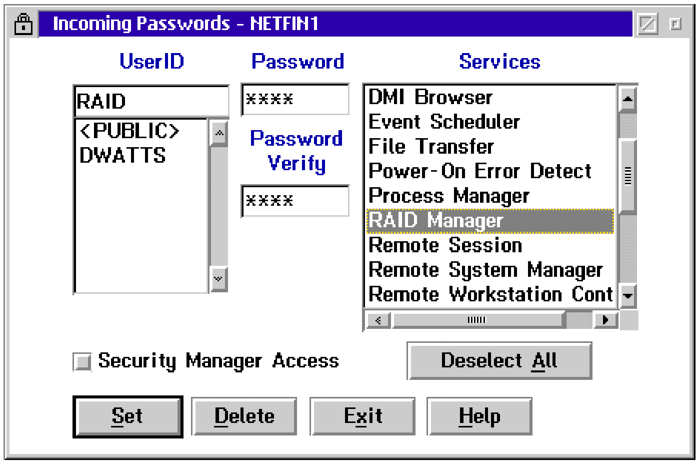

Security Manager - NETFIN1
Help
Edit/Display Incoming Passwords
Edit/Display Outgoing Passwords

Figure 42. 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 steps:

1. Double-click **Edit/Display Incoming Passwords**. Figure 43 appears:



UserID: RAID

<PUBLIC>
DWATTS

Password: xxxx

Password Verify: xxxx

Services:

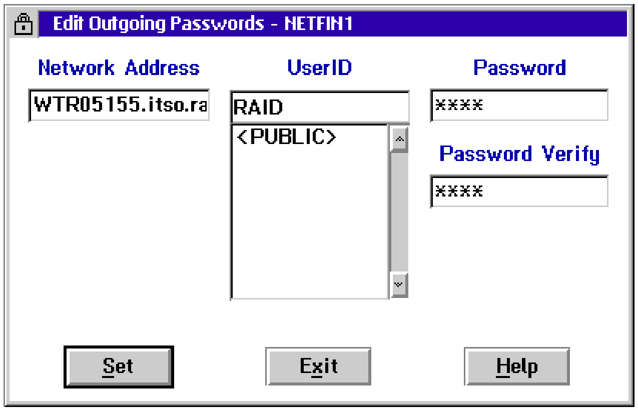
DMI Browser
Event Scheduler
File Transfer
Power-On Error Detect
Process Manager
RAID Manager
Remote Session
Remote System Manager
Remote Workstation Cont

□ Security Manager Access

Figure 43. Defining Incoming Passwords

2. Set up a user ID and password to allow access to the RAID Manager as shown in Figure 43. This is the service that performs the RAID scrub. Click **Set**.

3. Double-click **Edit/Display Outgoing Passwords**, then click **Add**. Figure 44 appears:



Network Address: WTR05155.itso.ra

UserID: RAID

<PUBLIC>

Password: xxxx

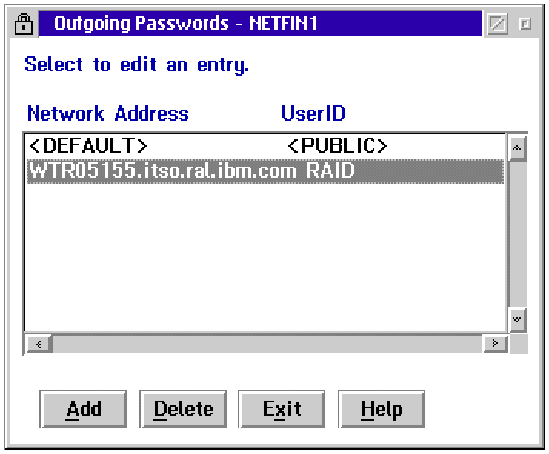
Password Verify: xxxx

Figure 44. 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 39. The user ID and password you type in must match those in Figure 43.

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

5. Click **Set**. A window similar to Figure 45 appears:



Outgoing Passwords - NETFIN1

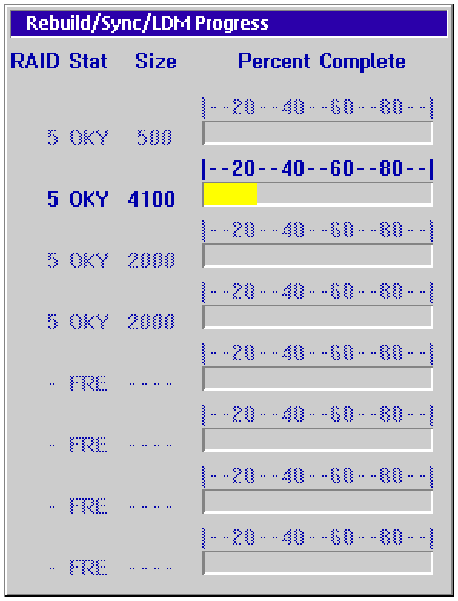
Select to edit an entry.

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

Figure 45. Outgoing Passwords Set

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

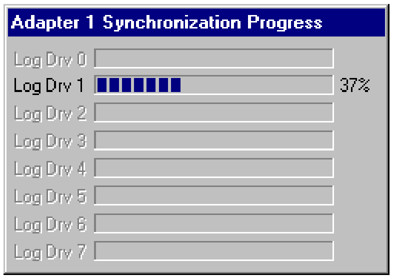
When the scheduled time arrives, the scrub will begin. If you wish you can view the progress of the scrub using the ServeRAID Administration Utility either locally (on Windows NT, OS/2 or NetWare servers) or remotely (using a Windows NT or Windows 95 client) as shown in the following windows:



Rebuild/Sync/LDM Progress

RAID	Stat	Size	Percent Complete
5	OKY	500	
5	OKY	4100	
5	OKY	2000	
5	OKY	2000	
-	FRE	----	
-	FRE	----	
-	FRE	----	
-	FRE	----	

Figure 46. 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 47. Progress Indicator – Windows NT

Chapter 3. Advanced System Management Hardware

The need for minimum server down time has led to more and more sophisticated management tools. One approach is the deployment of devices that allow you to access and manage your server at any time, at any place and in a secure manner.

Maximum up time and constant access to business-critical servers and applications are achievable by implementing features as followed:

- Remote BIOS/firmware upgrades
- Software independence using common programs like Web browsers or Telnet clients as access interfaces
- Remote server power control
- Automated notification process in case of problems
- Built-in recovery features in case of memory or CPU failure
- More than one option for access to the device — combination of LAN, WAN, modem and serial connections
- Monitoring server startup (POST) and running diagnostics tools remotely
- Independent power supply

With the current generation of management devices, server management goes one step further. Not only one server but a chain of servers can be managed from a centralized access connection, whether your server has power.

There are currently three types of these management adapters and processors available from IBM:

- *Advanced System Management PCI Adapter*, standard with the Netfinity 7000 M10 and available as an option on selected servers.
- *Advanced System Management Processor*, integrated in the Netfinity 5000 and 5500 family of servers.
- *Advanced Systems Management Adapter*, an ISA adapter standard with the Netfinity 7000 and available as an option on other selected servers.

Table 9 lists the Netfinity servers that support the ASM processor and adapters:

Table 9. Supported IBM Netfinity Servers

	Advanced System Management PCI Adapter	**Advanced System Management Processor**	**Advanced Systems Management Adapter**
Netfinity 3000	No	No	Supported as an option
Netfinity 3500	No	No	Supported as an option
Netfinity 5000	Supported as an option	Integrated	No
Netfinity 5500 family (5500, 5500 M10 and 5500 M20)	Supported as an option[1]	Integrated	No
Netfinity 7000	No	No	Standard
Netfinity 7000 M10	Standard	No	No

Note:
1 Netfinity 5500 models 8660-1xU and 8660-4xU are not supported.

For the latest information about supported servers, see:

http://www.pc.ibm.com/us/netfinity/serverproven

Each of Advanced System Management devices provides similar functionality, although the Advanced System Management PCI Adapter and the Advanced System Management Processor offer increased connectivity options. Table 10 compares the features of the three devices:

Table 10. Comparison Matrix

Function	**Advanced System Management PCI Adapter**	**Advanced System Management Processor**	**Advanced Systems Management Adapter**
Bus Interface	32-bit PCI adapter	ISA device (integrated)	ISA adapter
Netfinity Manager Support	Yes	Yes	Yes
RS-485 Connectivity	Yes	Yes	No
Network Connectivity	Ethernet; Token-ring (optional)	None	None
Remote Access	Web browser, Telnet, Serial	Web Browser[1], Telnet[1], Serial	Serial
External Power Supply	Standard with the adapter if purchased separately, optional on the 7000 M10.	No	Optional on some models, required on others
Dial-in and Dial-out user IDs	12	12	6
Dedicated COM ports	Yes[3]	Yes	Yes
COM ports sharable between OS and device	Yes (Port 1/COM 3)	Yes (Port A/COM 1)	No[2]

Notes:

1 Web browser and Telnet access only via an ASM PCI adapter when both the adapter and the processor are on the same RS-485 ASM interconnect bus.

2 Although the Advanced Systems Management Adapter User’s Guide states that the COM port can be shared, this is no longer supported. See 3.5.2, “ASM ISA Adapter COM Ports” on page 89.

3 When the ASM PCI adapter is installed in a system with an ASM processor, the COM ports on the ASM PCI adapter are disabled.

3.1 Advanced System Management PCI Adapter

The Advanced System Management PCI Adapter (ASM PCI adapter) is currently the most advanced service processor in the family of management adapters and processors IBM offers. The adapter is standard in the Netfinity 7000 M10 and can be purchased as an option for selected servers including the Netfinity 5000 and 5500 family (except Netfinity 5500 8660-1xU and 8660-4xU). For supported systems see Table 9 on page 63.

When you order the ASM PCI adapter as an option (part 01K7209 in the U.S.), it contains the adapter plus additional cables and software. See 3.1.3, “Ordering the Adapter Separately” on page 67 for details.

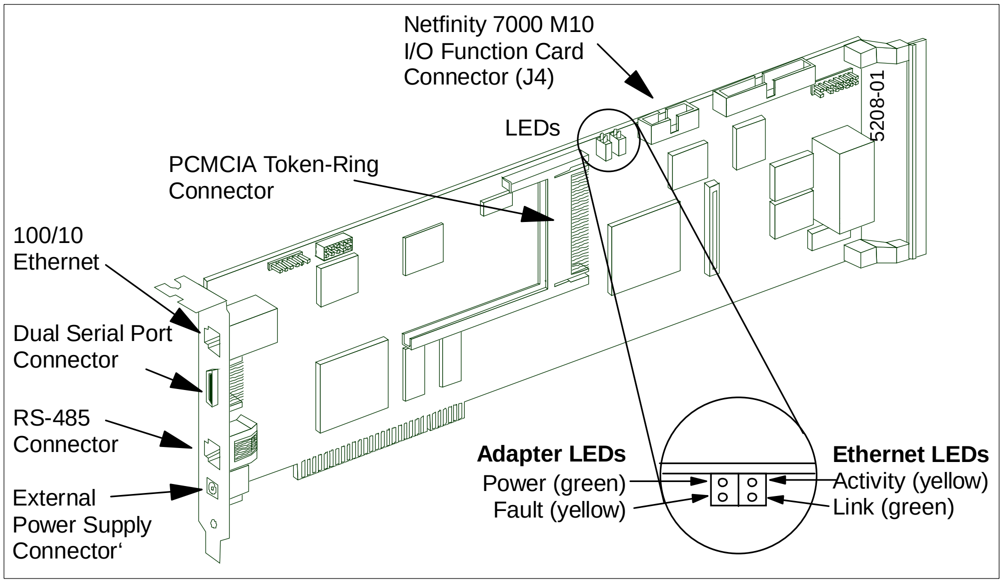


Figure 48. Advanced System Management PCI Adapter

The ASM PCI adapter has the following specifications (see Figure 48):

- Full-length adapter
- 32-bit PCI interface
- Integrated PowerPC 403 RISC processor
- Connector for 56-watt external AC adapter
- RS-485 interconnect bus interface
- Serial connection for modem or other serial devices
- 10/100 Ethernet interface
- Token-ring PCMCIA interface
- Four LEDs for Ethernet and Operation status

The RS-485 interconnect is discussed in detail in 3.4, “ASM Interconnect Network” on page 80.

3.1.1 Comparison of Features

Compared to the ASM processor integrated in the Netfinity 5000 and 5500 servers, and the ASM ISA adapter in the Netfinity 7000, the Advanced System Management PCI Adapter offers new features such as:

- Management over your LAN or WAN through:
  - 10/100 Ethernet port
  - Optional Turbo16/4 token-ring PCMCIA adapter
- Remote manageability through:
  - Telnet session
  - Web browser interface
  - RS-485 ASM interconnect bus
- PCI interface
- Generate unique SNMP traps

As an option installed in Netfinity 5000 and 5500 servers, the following capabilities are added:

- LAN connectivity through the 10/100 Ethernet port or optional token-ring connection
- Remote update of System BIOS and ASM processor firmware over LAN, modem and RS-485 ASM interconnect bus.
- Manage remotely from:
  - Telnet session
  - Web browser
- Generate unique SNMP traps

See 3.4, "ASM Interconnect Network" on page 80 for more information on RS-485 connectivity.

3.1.2 Adapter LEDs

The LEDs on the adapter are shown in Figure 49. You see two pairs of LEDs. One pair for operational status, one pair for Ethernet status. Table 11explains the functions of each LED.

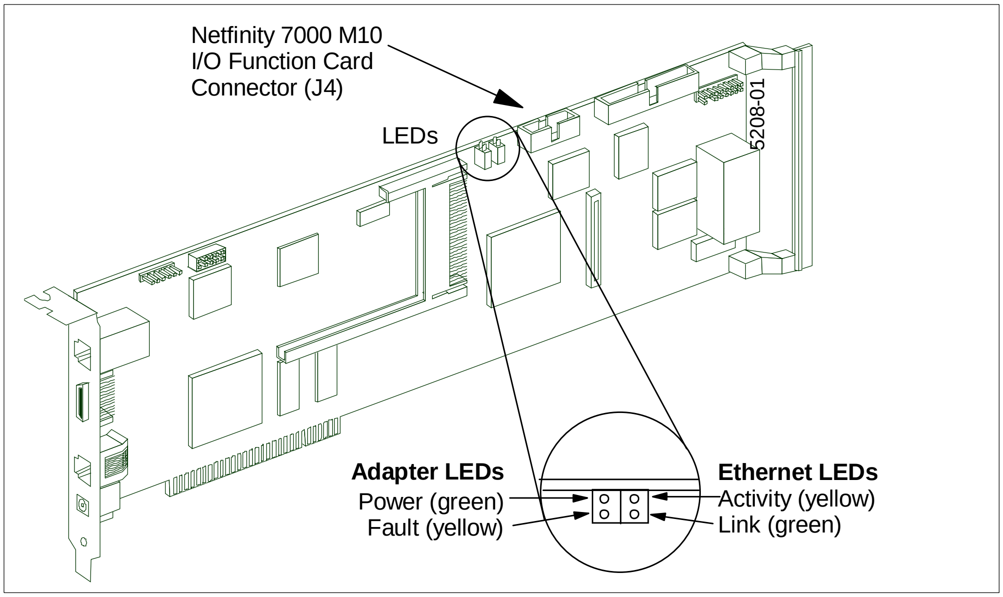


Figure 49. ASM PCI Adapter LEDs

Table 11. ASM PCI Adapter LED Functions

LED	Function
Adapter Power (green)	Remains lit if power is being supplied to the adapter.
Adapter fault (yellow)	Indicates problems with the Advanced System Management PCI Adapter processor. If lit, get your adapter serviced.
Ethernet activity (yellow)	Blinks when Ethernet activity is low and remains steady when activity is high. It does not indicate Token-Ring or RS-485 activity.
Ethernet link (green)	If lit, a logic link on the Ethernet network has been established. It does not indicate Token-Ring or RS-485 link status.

3.1.3 Ordering the Adapter Separately

The ASM PCI adapter is shipped standard with the Netfinity 7000 M10. For other supported servers such as the 5000 and 5500/5500 M10/5500 M20 servers, you can order the adapter as an option. As an option, it is supplied with a number of additional components as shown in Figure 50 on page 67.

In the United States, the part number for the option is 01K7209. For part numbers in other countries, see the appropriate product announcement at:

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

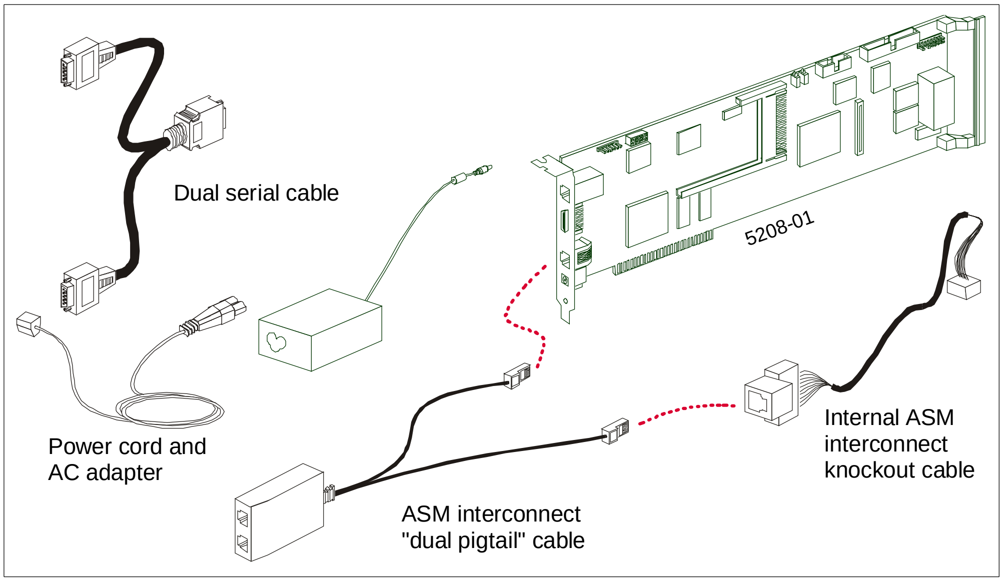

Dual serial cable
5208-01
Power cord and AC adapter
Internal ASM interconnect knockout cable
ASM interconnect "dual pigtail" cable

Figure 50. Advanced System Management PCI Adapter Option

The Advanced System Management PCI Adapter option includes the following components:

- The adapter as described in 3.1, “Advanced System Management PCI Adapter” on page 64.
- Internal ASM interconnect knockout cable, making the ASM connection on the Netfinity 5000/5500 system board available externally through a knockout on the server’s casing for use in the RS-485 network.
- ASM Interconnect “dual pigtail” cable, connects both the ASM processor integrated on the Netfinity 5000/5500 system board (via the knockout cable) and the ASM PCI adapter (RJ-11 connector) into the ASM interconnect bus. The cable has two RJ-45 sockets for connection to other servers on the ASM interconnect bus.
- Dual port cable, for serial connectivity. This cable provides two 9-pin RS-232C ports for modem connections dedicated to access the adapter for dialing in or sending out alerts. One of the ports, labeled “Modem”, can be shared between the adapter and the operating system and the other, labeled “COM_AUX”, is available only to the adapter.
- External 56-watt AC adapter (ThinkPad-style) and power cord. This power supply ensures the ASM PCI adapter has power even when the server does not. We recommend you connect the AC adapter to a UPS for improved availability. The AC adapter can also be ordered separately by ordering part number 83H6739.

- Advanced System Management CD-ROM, for upgrading and configuring the ASM devices.
- Netfinity Manager version 5.20.4 CD-ROM, includes updated designs for the ASM PCI adapter and ASM processor.

The Netfinity 7000 M10 has the ASM PCI adapter installed as standard. Also included with the server is the dual-ported serial cable. The interconnect cable and knockout cables are included in the interconnect cable kit as explained in 3.1.5, “Interconnect Cable Option” on page 68. An AC adapter can be purchased separately by ordering the ThinkPad 56W AC Adapter (83H6739).

3.1.4 Token-Ring Option

The ASM PCI adapter has a 10/100 Ethernet port integrated on the card so that the adapter can be directly connected to your LAN for remote access and alert transmission.

If you use a token-ring network, you can purchase the Netfinity Advanced System Management Token-Ring Connection, part 36L9654.

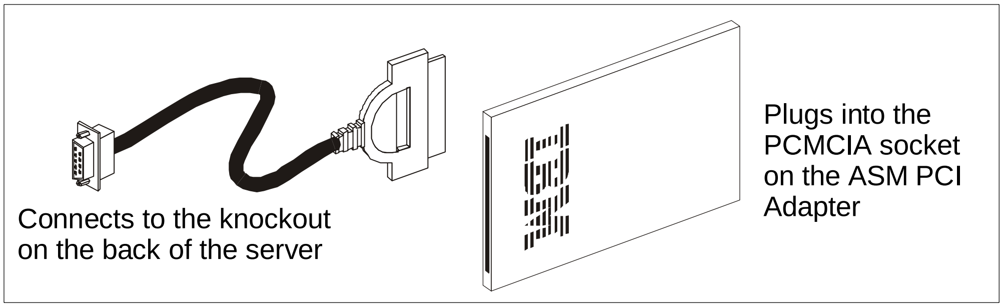

Connects to the knockout on the back of the server
Plugs into the PCMCIA socket on the ASM PCI Adapter

Figure 51. Advanced System Management Token-Ring Option

This option provides the following parts (see Figure 51):

- 16/4 token-ring PCMCIA
- 9-pin D-shell cable assembly
- Netfinity Manager 5.20.4 CD-ROM
- ASM PCI adapter firmware update

The PCMCIA card is inserted into the Type II slot on the ASM PCI adapter (see Figure 54 on page 70). The cable is then connected to it and routed to the knockout at the rear of the server. You will need an additional cable to connect the DB9 connector to your LAN. See the *Advanced System Management PCI Adapter Installation Instructions* for more details.

Note: Once the token-ring option is installed, the Ethernet port is automatically disabled.

3.1.5 Interconnect Cable Option

As standard, Netfinity servers are not capable of connecting to the ASM interconnect bus. To achieve this, you will need one of the following:

- Advanced System Management PCI Adapter, purchased separately (as part 01K7209 in the U.S.) as described in 3.1.3, “Ordering the Adapter Separately” on page 67.

- Advanced System Management Interconnect Cable Kit, part 03K9309, for use on servers where the ASM PCI adapter is standard (such as the Netfinity 7000 M10) or the ASM processor is integrated (such as the Netfinity 5000 and 5500).

Notes:

1. If you obtain the ASM PCI adapter as an option, you do not need the interconnect cable kit as well, as the equivalent cables are already included.
2. The Netfinity 5500 models 8660-1xU and 8660-4xU do not support the interconnect cable kit nor connectivity to the ASM interconnect bus.

Figure 52 on page 69 shows the Advanced System Management Interconnect Cable Kit:

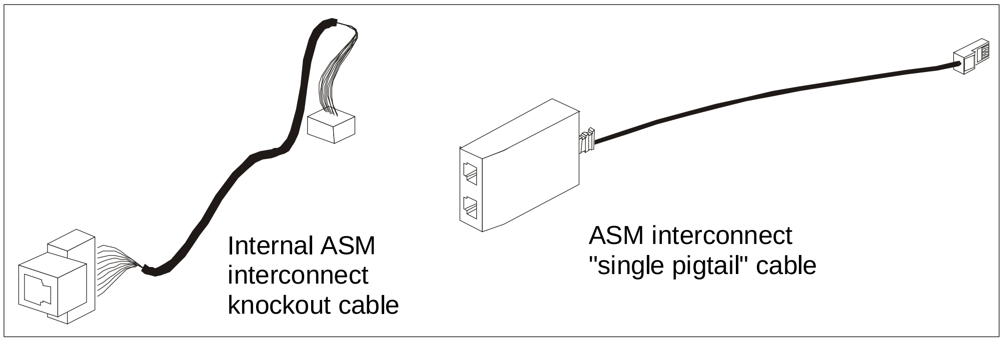


Figure 52. Advanced System Management Interconnect Cable Kit

This kit provides the necessary cables to interconnect an installed ASM processor or ASM PCI adapter with other servers. It includes the following components as shown in Figure 52:

- Internal ASM Interconnect knockout cable, making the ASM connection on the Netfinity 5000/5500 system board available externally through a knockout on the server's casing for use in the RS-485 network.

  Note: This cable is not needed when used with the Netfinity 7000 M10.

- ASM Interconnect "single pigtail" cable, connects the ASM processor (via the knockout cable) or the ASM PCI adapter into the ASM interconnect bus. The cable has two RJ-45 sockets for connection to other servers on the ASM interconnect bus.
- Advanced System Management CD-ROM
- Netfinity Manager V5.20.4 CD-ROM

For information on how to use the interconnect cable kit, See 3.4, "ASM Interconnect Network" on page 80.

3.1.6 Installation in the Netfinity 7000 M10

The ASM PCI adapter comes pre-configured with your Netfinity 7000 M10. However, if you remove it and wish to reinstall it, follow these steps:

1. Open the Netfinity 7000 M10 and install the card into the ASM PCI adapter slot (see Figure 53 on page 70).

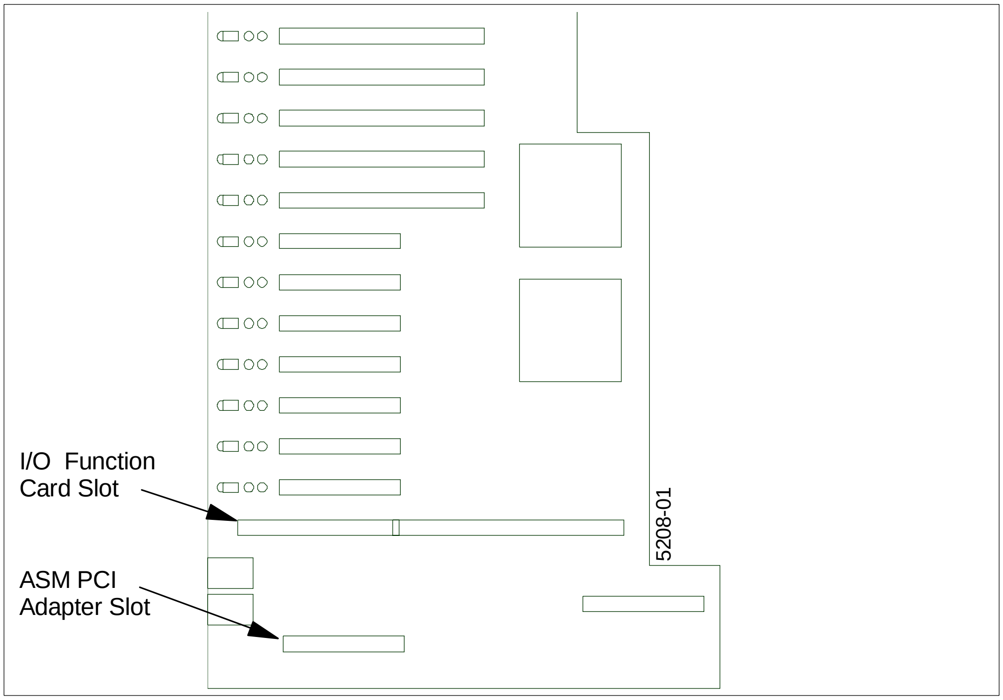


Figure 53. Netfinity 7000 M10 I/O Board

2. Connect the supplied ribbon cable from the 12-pin connector J4 on the ASM PCI adapter to the Netfinity 7000 M10 I/O Function Card's ASM PCI adapter connector (see Figure 54). The ribbon cable used is the one that was connected to the adapter when it was originally installed in the server.

   This ribbon cable is used to supply power to the ASM PCI adapter even when the system is powered off and power to the PCI slots is removed.

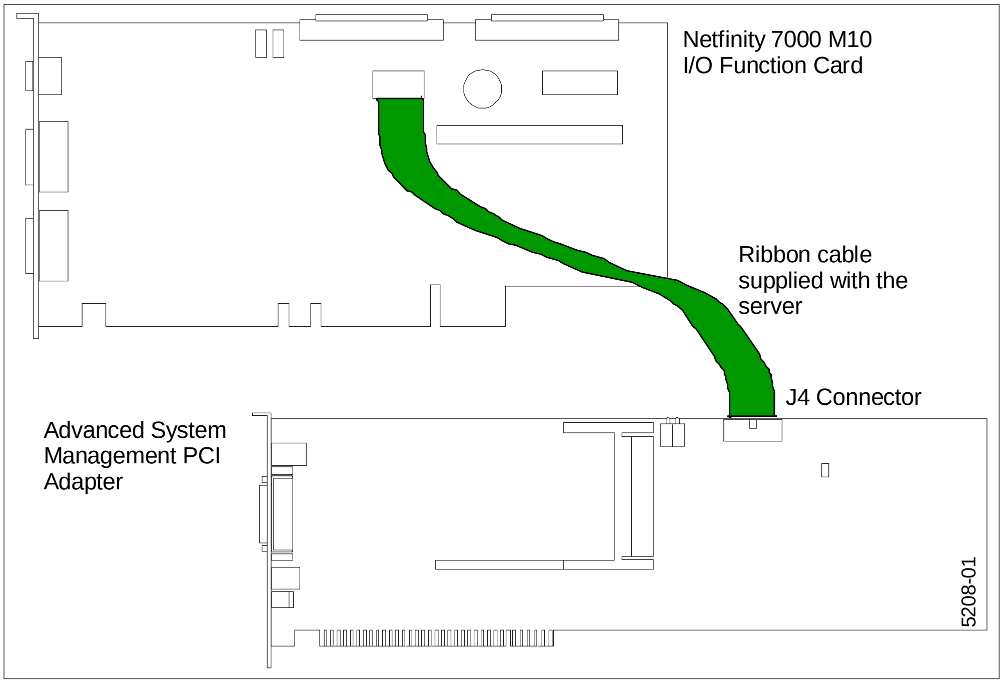

Netfinity 7000 M10 I/O Function Card
Ribbon cable supplied with the server
J4 Connector
Advanced System Management PCI Adapter
5208-01

Figure 54. Connecting the I/O Function Card to the ASM PCI Adapter

The Netfinity 7000 M10 includes both the ASM PCI adapter and the dual-ported serial cable. The interconnect cable and knockout cables are included in the interconnect cable kit as explained in 3.1.5, “Interconnect Cable Option” on page 68. An AC adapter can be purchased separately by ordering the ThinkPad 56W AC Adapter (83H6739).

3.1.7 Installation in the Netfinity 5000 and 5500 Servers

The ASM PCI adapter is available as an option for the Netfinity 5000 and 5500 servers. When installed in one of these servers, it gives you LAN connectivity via the Ethernet port and optional token-ring port on the adapter.

Note: The ASM PCI adapter is not supported in the Netfinity 5500 models 8660-1xU and 4xU.

To install the adapter follow these steps:

1. Shut down your server.
2. Insert the ASM PCI adapter into any PCI slot. See your server’s user guide for any placement recommendations.
3. Remove the knockout (**1** in Figure 56).
4. Connect the internal ASM interconnect knockout cable to your server’s system board and to the knockout on the rear casing of your server:

   – On the Netfinity 5000, connect the cable from the J35 connector on the system board to the knockout on the server casing (see Figure 55).

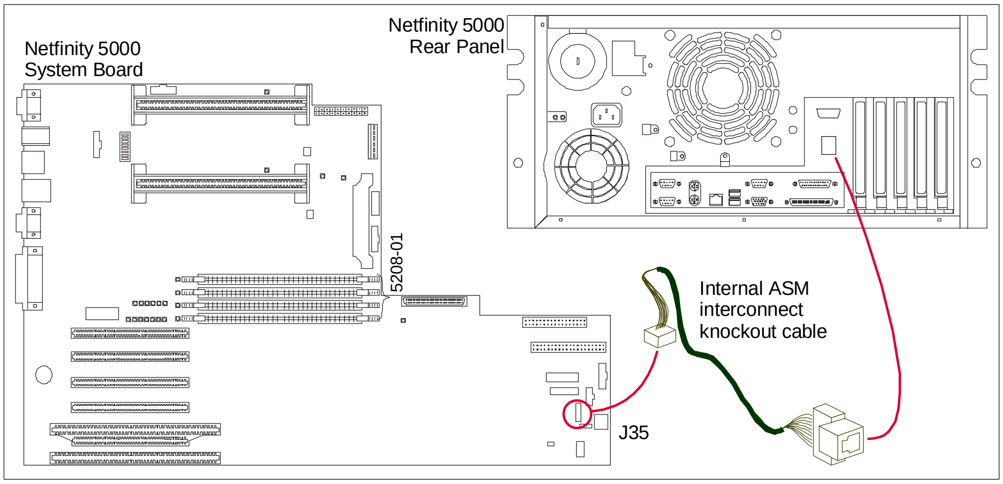


Figure 55. Netfinity 5000

   – On the Netfinity 5500 connect the cable from the J27 connector (**2** in Figure 56) to the knockout on the server (**1** in Figure 56).

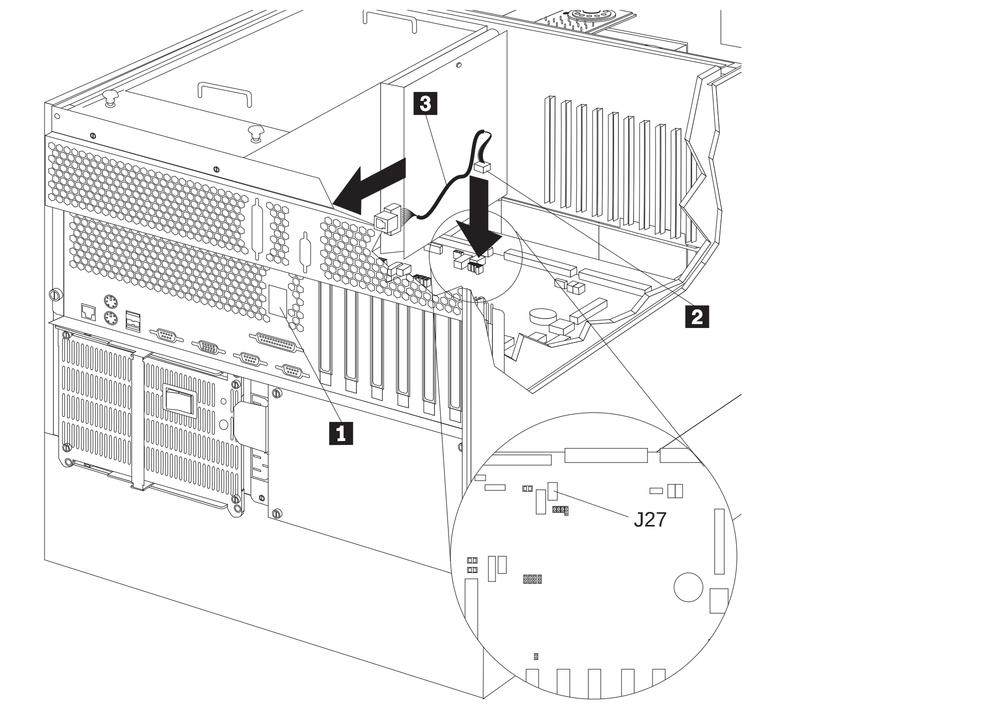


Figure 56. Netfinity 5500 Connections

5. Connect the dual pigtail ASM interconnect cable to both the ASM PCI adapter and the ASM processor as shown in Figure 57:

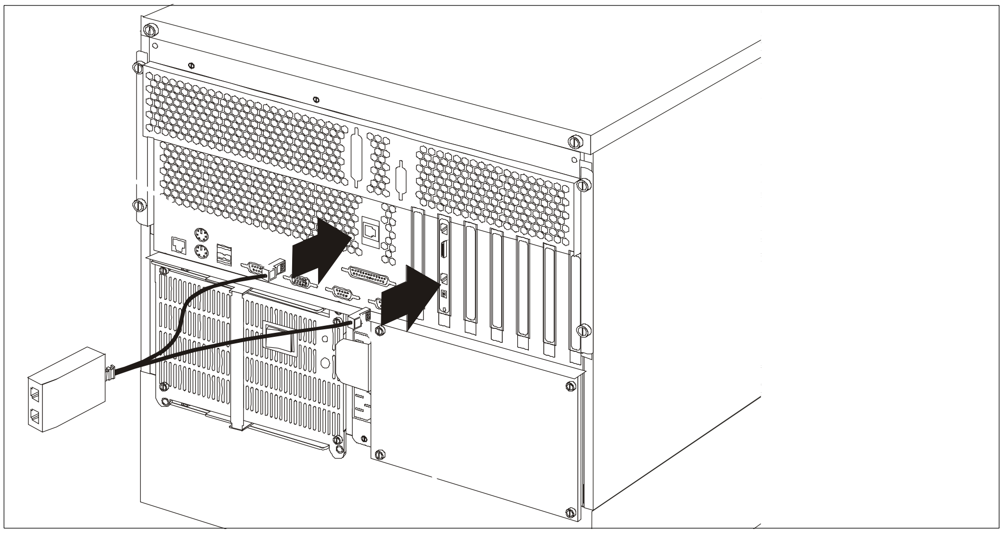


Figure 57. Connecting the ASM PCI Adapter and ASM Processor Together

For how to use the ASM interconnect bus option and how to set up your RS-485 network, see 3.4, “ASM Interconnect Network” on page 80.

6. Plug the AC adapter into the ASM PCI adapter and connect it to a power socket. The AC adapter is needed to provide continuous power to the adapter even when the server is powered off.

3.2 Advanced System Management Processor

The integrated Advanced System Management Processor offers strong local and remote management of the server. It is currently integrated into the following servers:

- Netfinity 5000
- Netfinity 5500
- Netfinity 5500 M10
- Netfinity 5500 M20

Collectively, we will refer to these as the Netfinity 5000/5500 servers.

The ASM processor has the following specifications:

- Powered by a PowerPC 403GA 32-bit RISC microprocessor
- Self-contained SRAM, non-volatile RAM, real-time clock, UART serial port processor and I^2C controller
- Interface to LM78 environmental monitoring processor
- Five I^2C buses 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)
- Upgradable through flash update
- COM port B, shared with operating system after boot
- COM port C, dedicated management COM port

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

- Additional dial-out alerts: VRM failure, PFA alert, non-critical voltage alert
- Remote diagnostics 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

In addition, extended features are available when the ASM processor is used with the Advanced System Management Interconnect Cable Kit:

- Allows multiple management processors to be interconnected
- Allows sharing of available resources (LAN, modem)
- Forwards alerts over ASM interconnect bus to available modem/LAN resource
- Connects up to 12 service processors

For more information about the Advanced System Management Interconnect Cable Kit, see 3.1.5, “Interconnect Cable Option” on page 68.

Older Models of the Netfinity 5500

Netfinity 5500 models 8660-1xU and 8660-4xU do not support the Advanced System Management Interconnect Cable Kit nor connection to the ASM interconnect bus.

3.2.1 Installing an ASM PCI Adapter in a Netfinity 5000/5500

See 3.1.7, “Installation in the Netfinity 5000 and 5500 Servers” on page 71 for details of this procedure.

If you install an Advanced System Management PCI Adapter into the Netfinity 5000/5500 you will have two ASM devices working together in the one server. The ASM PCI adapter acts as an Ethernet or token-ring network gateway, or as a shared modem resource.

In this configuration, the ASM processor generates all the alerts, timeouts and other system management information. This data is then relayed to the ASM PCI adapter using the ASM interconnect bus between the two. The adapter then forwards the information to other systems on the LAN, or uses its modem to forward the data using a serial connection.

Key Concept

If you install an ASM PCI adapter into a Indefinite 5000/5500 system, the two ASM devices will act as follows:

- The ASM processor generates all management data
- The ASM PCI adapter acts only as a network gateway (or shared modem resource)

It is important to understand how the tasks are divided when configuring the combined management functions. For example, any alerts configured on the ASM PCI adapter will be ignored.

Because the ASM interconnect bus allows connectivity of multiple ASM PCI adapters and ASM processors through the RS-485 ports, it is only necessary to have an ASM PCI adapter in one system on the ASM interconnect bus. You simply access the other systems through the interconnect bus.

A note about the AC adapter: The AC adapter is required when you install the ASM PCI adapter in a Netfinity 5000/5500 system. This is because the server does not supply power to the PCI slots when the system is powered off. Therefore, to connect to the ASM PCI adapter through its ports (for example, the Ethernet port) to power up the server, you must have the AC adapter connected.

3.3 Configuring your ASM PCI Adapter and ASM Processor

In order to configure your ASM PCI adapter for the first time, you can use either Netfinity Manager or the DOS-based installation utility. If you plan to use Netfinity Manager, you will need to install the ASM device drivers first then install (or reinstall Netfinity Manager).

3.3.1 Device Drivers

Device drivers are supplied on the Advanced System Management CD-ROM for the following operating systems:

- Windows NT 3.51 or 4.0
- OS/2 Warp
- Novell NetWare
- SCO UnixWare

Note: For information on how to install drivers for the Advanced Systems Management Adapter, see 3.5.4, “Device Drivers” on page 92.

Before you start check the IBM Web support page for the latest version for the configuration utility disk and device drivers:

`http://www.pc.ibm.com/support`

Select **Server** from **Select a Brand**.
Select your server from **Select your family**.
Click **Downloadable Files**.
Click **Advanced System Management**.

The ASM processor uses the same utilities as ASM PCI adapter. Some of the options are not available due to differences in function and features. For example, no network settings are available for the ASM processor.

An IBMCOMx.SYS driver is also installed on systems with the ASM PCI adapter (for example, the Netfinity 7000 M10) which enables the serial interface of the ASM PCI adapter to be shared between the adapter and the operating system. After the driver is installed, an additional COM port is added to your operating system. NetWare does not support shared COM ports so a NetWare version of the driver is not available.

Note: The IBMCOMx.SYS driver is not installed on systems with both the ASM PCI adapter and the ASM processor. It is only for systems with the ASM PCI adapter.

For further details on COM ports see 3.3.5, “COM Ports” on page 79.

As both devices use the same utilities and their features are very similar, we will talk about them together. If there is a difference between them, we will point it out. Unless we do so, consider all statements valid for both the ASM PCI adapter and the ASM processor.

Note: If you plan to install Netfinity Manager, you must install the required device drivers *before* you install Netfinity Manager. If you don’t, you’ll have to reinstall Netfinity Manager. When you install Netfinity Manager, ensure you have **Advanced System Management Support** selected.

3.3.2 IRQ and I/O Address Settings

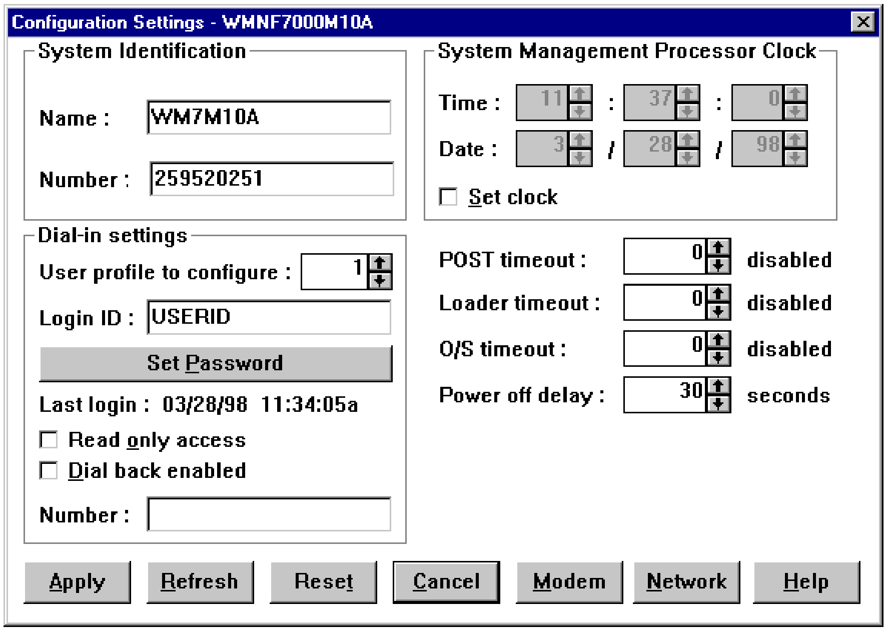
The IRQ and I/O address settings for the ASM PCI adapter are assigned through the PCI bus. You can reserve an IRQ for the card using the Configuration/Setup Utility by pressing F1 during POST.

As the ASM processor is an ISA device you can assign an IRQ to the device, using the Configuration/Setup Utility by pressing F1 during POST. By default, the system allocates resources through “Autoconfigure” but, in order to avoid problems with IRQ sharing we recommend you assign an IRQ such as IRQ 5.

3.3.3 Configuring with Netfinity Manager

Once you have installed the ASM device driver and installed (or reinstalled) Netfinity Manager, you can configure your ASM device through Netfinity Manager:

Start Netfinity Manager.
Click **Advanced System Management.**
Click **Configuration Settings**. Figure 58 appears.



Configuration Settings - WMNF7000M10A

System Identification

Name : WM7M10A

Number : 259520251

System Management Processor Clock

Time : 11 : 37 : 0

Date : 3 / 28 / 98

□ Set clock

Dial-in settings

User profile to configure : 1

Login ID : USERID

Last login : 03/28/98 11:34:05a

□ Read only access

□ Dial back enabled

Number :

POST timeout : 0 disabled

Loader timeout : 0 disabled

O/S timeout : 0 disabled

Power off delay : 30 seconds

Figure 58. ASM Configuration Settings

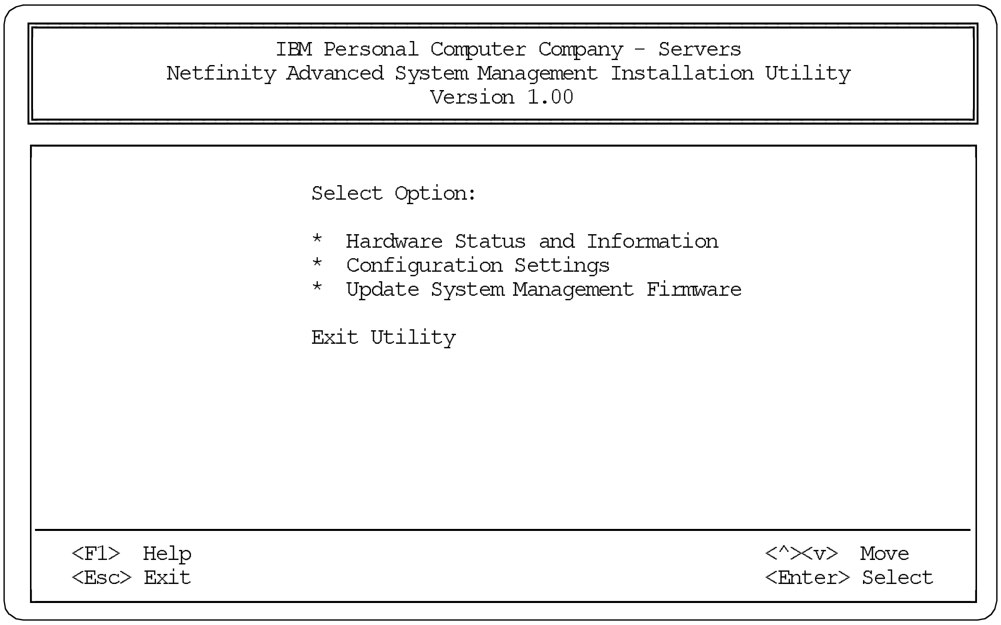
From here you can configure the device. To specify the TCP/IP settings for the ASM PCI adapter, click the **Network** button.

For details see 4.2.3, “Configuration Settings” on page 108.

3.3.4 Configuring with DOS-Based Utility

The DOS-based utility gives you a limited variety of options to configure your ASM PCI adapter. The following options are available:

- Hardware Status and Information
- Configuration Settings
- Update System Management Firmware

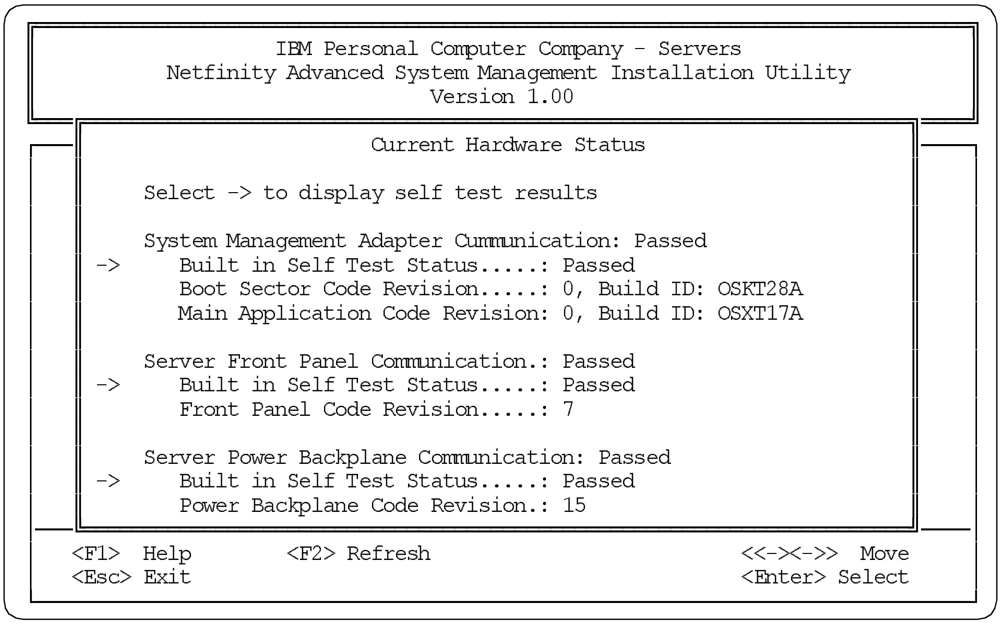


```
                 IBM Personal Computer Company - Servers
          Netfinity Advanced System Management Installation Utility
                               Version 1.00

                        Select Option:

                        *  Hardware Status and Information
                        *  Configuration Settings
                        *  Update System Management Firmware

                        Exit Utility

   <F1>  Help                                        <^><v>  Move
   <Esc> Exit                                        <Enter> Select
```

Figure 59. Advanced System Management PCI Adapter Configuration Startup Screen

3.3.4.1 Hardware Status and Information

If you select **Hardware Status and Information**, a screen similar to Figure 60 appears:



```
                 IBM Personal Computer Company - Servers
          Netfinity Advanced System Management Installation Utility
                               Version 1.00

                          Current Hardware Status

         Select -> to display self test results

         System Management Adapter Cummunication: Passed
   ->       Built in Self Test Status.....: Passed
            Boot Sector Code Revision.....: 0, Build ID: OSKT28A
            Main Application Code Revision: 0, Build ID: OSXT17A

         Server Front Panel Communication.: Passed
   ->       Built in Self Test Status.....: Passed
            Front Panel Code Revision.....: 7

         Server Power Backplane Communication: Passed
   ->       Built in Self Test Status.....: Passed
            Power Backplane Code Revision.: 15

  <F1>  Help        <F2> Refresh                           <<-><->>  Move
  <Esc> Exit                                               <Enter> Select
```

Figure 60. Hardware Status and Information (Netfinity 7000 M10)

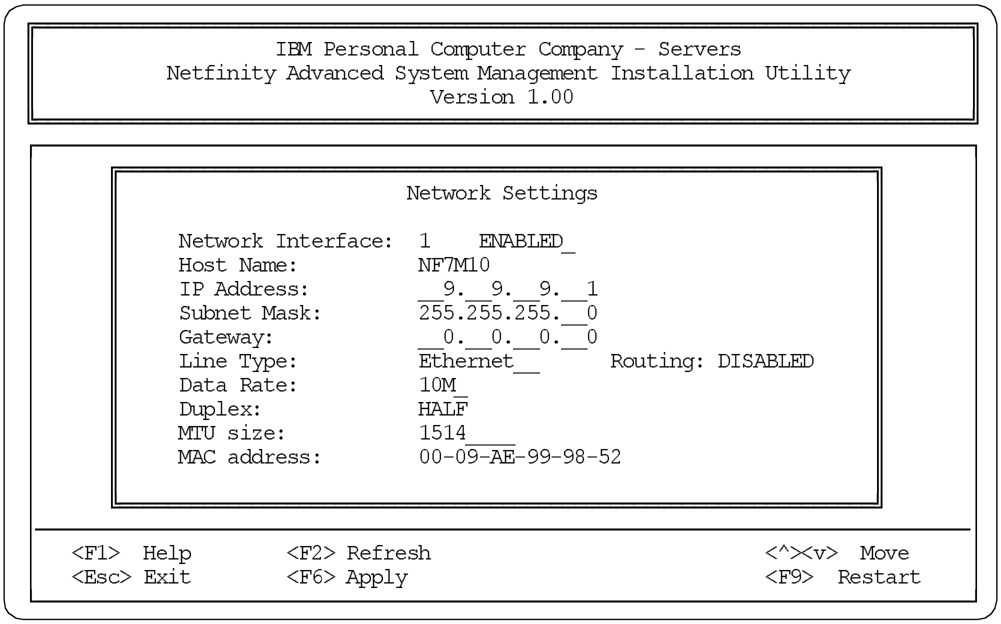
This window displays information about firmware level for the ASM PCI adapter (Netfinity 7000 M10) or ASM processor (Netfinity 5000/5500) or both, if the ASM PCI adapter is installed in the Netfinity 5000/5500. In a Netfinity 7000 M10, as shown in Figure 60, additional information about the front panel, backplane and code level is displayed.

The entries Boot Sector Code Revision and Main Application Code Revision give you information about the current level of firmware. That code will be updated when new features are added or code bugs eliminated. Options marked with -> contain the self test results.

3.3.4.2 Configuration Settings

Selecting **Configuration Settings** from Figure 59 on page 76 produces a window with two options:

- System identification, where you can specify a name and number that identifies your system.
- Network Settings (ASM PCI adapter only), which allows you to enter information to access your system in a TCP/IP network. Selecting this option produces a window similar to Figure 61 on page 78:



```
                    IBM Personal Computer Company - Servers
            Netfinity Advanced System Management Installation Utility
                                 Version 1.00

                              Network Settings

          Network Interface:  1    ENABLED_
          Host Name:          NF7M10
          IP Address:         __9.__9.__9.__1
          Subnet Mask:        255.255.255.__0
          Gateway:            __0.__0.__0.__0
          Line Type:          Ethernet__      Routing: DISABLED
          Data Rate:          10M_
          Duplex:             HALF
          MTU size:           1514____
          MAC address:        00-09-AE-99-98-52

   <F1>  Help       <F2> Refresh                          <^><v>  Move
   <Esc> Exit       <F6> Apply                            <F9>  Restart
```

Figure 61. Network Settings (Advanced System Management PCI Adapter Only)

The settings in the window are as follows. Use the Tab key to navigate from field to field. Depending on the field, either type in the setting or use the left and right arrow keys to select the appropriate one.

- Network Interface. Select your network interface to configure. Interface 1 refers to Ethernet, Interface 2 refers to token-ring.
- Host Name. Type the TCP/IP host name that will be used by the Advanced System Management PCI Adapter.
- IP Address. Type the IP address that will be used by the Advanced System Management PCI Adapter.
- Subnet Mask. Type the subnet mask that will be used by the Advanced System Management PCI Adapter.
- Gateway address. Type the TCP/IP address of the gateway that will be used by the Advanced System Management PCI Adapter.
- Line Type. Use the spin buttons to select the line type that will be used by the Advanced System Management PCI Adapter. Available selections are Ethernet and token-ring. Mark the Routing check box if needed.
- Data Rate. Use the spin buttons to select the data rate that will be used by the Advanced System Management PCI Adapter. Available selections are AUTO, 4M, 16M, 10M, and 100M depending on whether you select Ethernet or token-ring.
- Duplex method. Use the spin buttons to select the duplex method that will be used by the Advanced System Management PCI Adapter. Available selections are AUTO, FULL and HALF.
- MTU size. Type the maximum transmission unit (MTU) value that will be used by the Advanced System Management PCI Adapter.
- MAC address. Type the media access control (MAC) address of the network adapter being used by the Advanced System Management PCI Adapter. The

default value 00.00.00.00.00.00 will indicate the adapter is to use the burnt-in MAC address.

3.3.4.3 Update System Management Firmware

The Update System Management Firmware menu choice from Figure 59 on page 76 lets you update the firmware of your ASM PCI adapter. For the latest version contact your technical support or check the support Web page at:

```
http://www.pc.ibm.com/support
```

Note: All customer-defined user profiles used for accessing the ASM PCI adapter and ASM processor will be reset after you update the firmware. You will need to recreate them after the update. See 4.2.3, “Configuration Settings” on page 108 for information about user profiles.

3.3.5 COM Ports

The COM ports on the ASM PCI adapter and ASM processor can be dedicated to the ASM device or they can be shared between the device and the operating system.

In the modem settings of the Advanced System Management service in Netfinity Manager, you can specify which port to use for dial-in and dial-out. You choice affects the availability of the modem for use by either the Netfinity Advanced System Management PCI Adapter or the operating system. The ports that are available to the system or to the Advanced System Management service vary depending on your hardware configuration.

Note: Shared ports are seen by the operating system when the system is running. Shared ports are seen by the Advanced System Management PCI Adapter or Processor when the machine is starting up or powered off. The shared port will also be seen by the system, but not by the Advanced System Management PCI Adapter or Processor, when started with DOS.

If the system has an Advanced System Management Processor only (currently the Netfinity 5000/5500 servers), Table 12 shows what ports are available to the ASM device and to the operating system:

Table 12. COM Ports on Servers with the ASM Processor Only

Physical Ports (as labeled)	A	B	C
Ports available to ASM	Port 1 shared	N/A	Port 2 dedicated
Ports available to OS	COM 1 shared	COM 2	N/A
N/A means Not Available.			

If the system has an Advanced System Management PCI Adapter only (currently the Netfinity 7000 M10), Table 13 shows what ports are available to the ASM device and to the operating system:

Table 13. COM Ports on Servers with the ASM PCI Adapter Only

Physical Ports (as labeled)	A	B	Modem	COM/AUX
Ports available to ASM	N/A	N/A	Port 1 Shared	Port 2 dedicated
Dedicated ports available to OS	COM 1	COM 2	COM 3 shared[1]	N/A
Note: 1 The ASM device driver must be running for the operating system to see COM3. N/A means Not Available.				

If the system has both an Advanced System Management PCI Adapter and an Advanced System Management Processor (for example, a Netfinity 5000/5500 with an optional ASM PCI adapter), Table 14 shows what ports are available to the ASM devices and to the operating system:

Table 14. COM Ports on Servers with Both ASM Devices

Physical Ports	A	B	C	Modem[1]	COM/AUX[1]
Ports available to ASM	Port 1 shared	N/A	Port 2 dedicated	N/A	N/A
Ports available to OS	COM 1 shared	COM 2	N/A	N/A	N/A
Notes: 1 The serial ports on the ASM PCI adapter are not usable when the adapter is installed in a server with an ASM processor. 2) N/A means Not Available.					

3.4 ASM Interconnect Network

It is now possible to connect the ASM PCI adapters and ASM processors in the Netfinity 7000 M10 and 5000/5500 servers together. This connection, known as the Netfinity Advanced System Management Interconnect Bus allows up to 12 ASM devices to be interlinked.

Note: The ASM interconnect bus is supported by Netfinity Manager 5.20.4 or later.

Older Models of the Netfinity 5500

Netfinity 5500 models 8660-1xU and 8660-4xU do not support connectivity to the ASM interconnect bus.

Once they are connected, you can use the interconnect network to:

- Share LAN connections and modems
- Gain access to remote servers through the network
- Forward alerts between the servers to the outside network

The network is a bus that is formed by connecting RS-485 ports on the ASM PCI adapters and the RS-485 ports of the interconnect cable kit when used with ASM processors.

Examples of where this network is useful is as follows:

- You have a rack of Netfinity servers, but only one of them has a modem attached to it. Using the ASM interconnect bus, an alert from any of the servers in the rack can be transferred to the server with the modem which can then perform actions on that alert.
- Using a Web browser, or Telnet session, you connect to the ASM PCI adapter in one of the Netfinity 7000 M10 servers in your rack, then using the ASM interconnect bus, connect to one of the Netfinity 5500s in your rack to perform actions such as power cycling.

3.4.1 Building the Interconnect Network

The RS-485 connector is available on the ASM PCI adapter and Netfinity 5x00 Servers ASM processor when used with the interconnect cable kit.

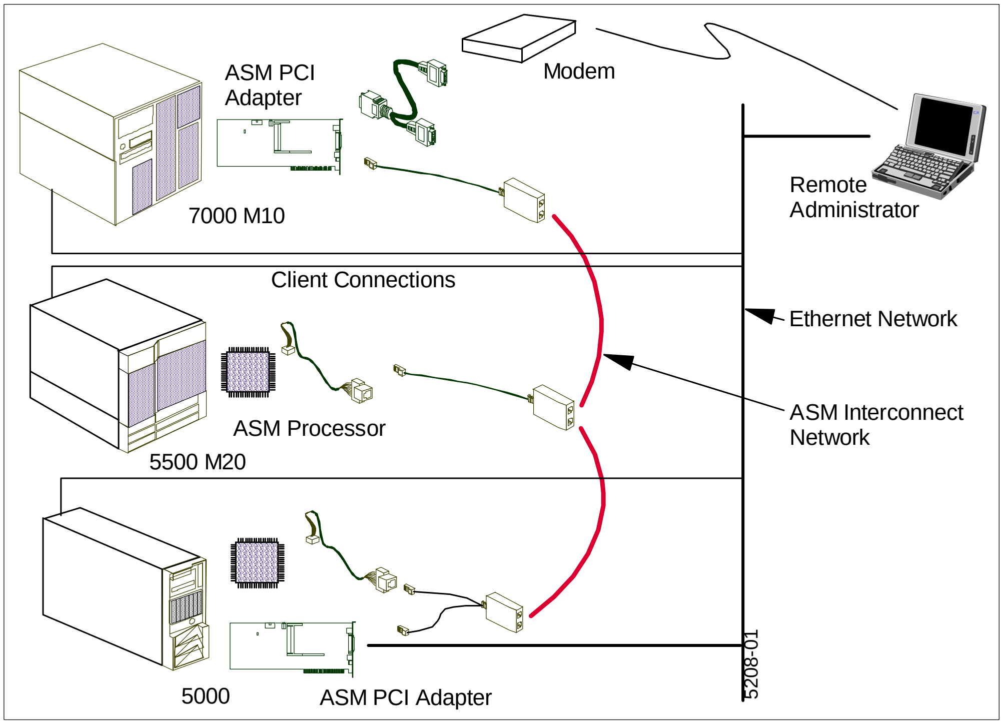


Figure 62. Sample Netfinity Advanced System Management Interconnect Bus

To connect to the ASM interconnect bus, you will need the following components, as shown in Figure 62:

- Unshielded twisted pair cabling with RJ-45 connectors.
- For a Netfinity 7000 M10, you will need the single pigtail interconnect cable. This cable is part of the Advanced System Management Interconnect Cable Kit as described in 3.1.5, “Interconnect Cable Option” on page 68.
- For a Netfinity 5000/5500, you will need both cables from the interconnect cable kit.
- For a Netfinity 5000/5500 with an additional ASM PCI adapter, you will not need any extra hardware, as all cables are supplied with the adapter.

3.4.2 Accessing the Interconnect Network

You can access the ASM interconnect bus through a number of methods as shown in Figure 62:

- Locally at the server, you can connect to the local ASM PCI adapter or ASM processor through Dynamic Connection Manager.
- From a remote Netfinity Manager system which has the Advanced System Management service installed, you can use Remote Systems Manager to connect to the server, then Dynamic Connection Manager to connect to the ASM interconnect bus.
- By connecting the ASM PCI adapters into your Ethernet or token-ring network, you can access the ASM interconnect bus through a Web browser or a Telnet client or through the Dynamic Connection Manager function of Netfinity Manager.
- By connecting any of the ASM devices to a modem, you can dial into the device using Netfinity Manager or an ASCII terminal emulator.

Once you have accessed one of the ASM devices on the interconnect bus, you can then “hop” to any other device on the bus using the Web browser, Telnet client or terminal emulator. All attached ASM devices will be automatically detected.

Note: You cannot log in to a remote ASM device and then “hop” to yet another remote ASM device; only “single-hop” accesses, from local to remote are supported.

3.4.3 Access with Netfinity Manager

Unlike serial and TCP/IP links, the ASM interconnect bus does not require extensive configuration prior to attempting to connect with other ASM devices. To establish an RS-485 interconnect link you can use Netfinity Manager’s Dynamic Connection Manager. To see how to access a remote server, consider the configuration shown in Figure 63.

Note: The LAN connection to the Netfinity 7000 M10 in Figure 63 is directly to its ASM PCI adapter and not to the server’s Ethernet adapter.

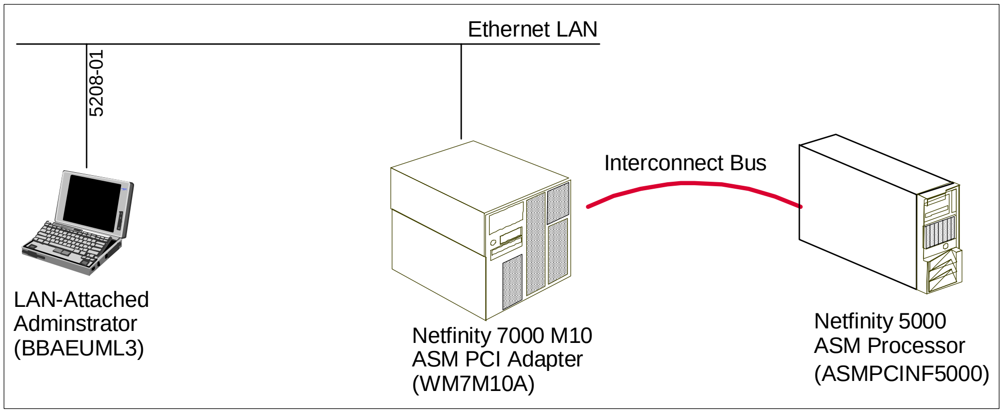
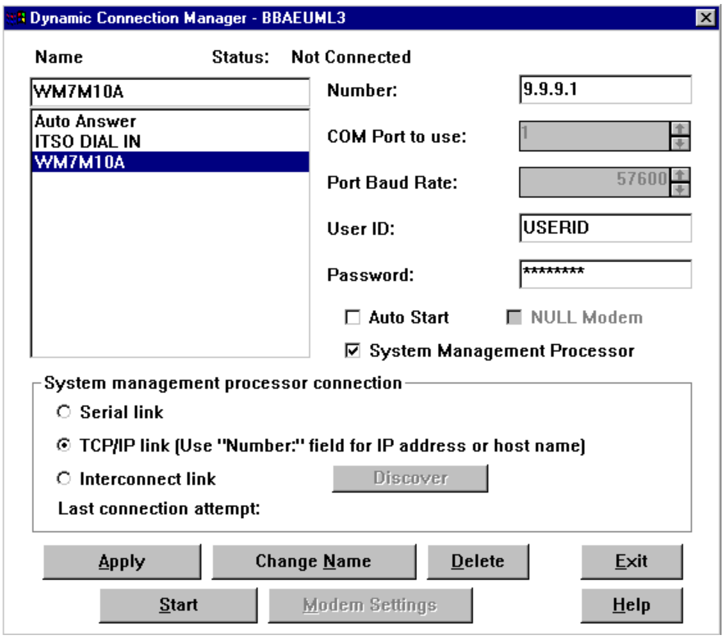


Figure 63. Access a Server through the ASM Interconnect Bus

From the administrator's ThinkPad, we will be directly accessing the ASM PCI adapter in the Netfinity 7000 M10 system via TCP/IP. From there, we connect to the Netfinity 5000 via the ASM interconnect bus. This is achieved as follows:

1. On the ThinkPad start Netfinity Manager and Dynamic Connection Manager. Configure and establish a TCP/IP connection with an ASM PCI adapter in the Netfinity 7000 M10. Fill in the dialog box in a similar fashion to Figure 64.



Dynamic Connection Manager - BBAEUML3

Name: WM7M10A
Status: Not Connected

Auto Answer
ITSO DIAL IN
WM7M10A

Number: 9.9.9.1
COM Port to use: 1
Port Baud Rate: 57600
User ID: USERID
Password: ********

☐ Auto Start ☐ NULL Modem
☑ System Management Processor

System management processor connection
○ Serial link
● TCP/IP link (Use "Number:" field for IP address or host name)
○ Interconnect link
Last connection attempt:

Figure 64. Dynamic Connection Manager

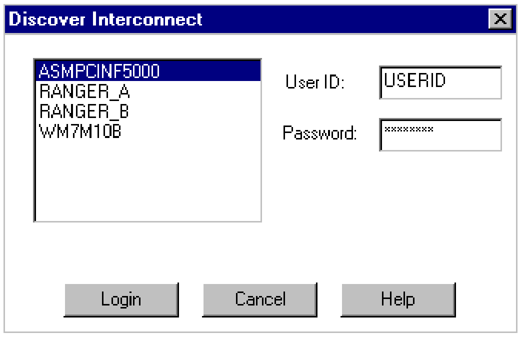
The steps are:

a. Type in a name.
b. Enter the TCP/IP address of the 7000 M10's ASM PCI adapter.
c. Enter the appropriate user ID and password.
d. Click **System Management Processor**.
e. Click **TCP/IP link**.
f. Click **Apply.**

The connection to the ASM PCI adapter should now be established.

2. Now, we want to connect to the Netfinity 5000 system. Click **Interconnect link**.

3. Click the **Discover** button. Figure 65 appears:



Discover Interconnect

ASMPCINF5000
RANGER_A
RANGER_B
WM7M10B

User ID: USERID
Password: ********

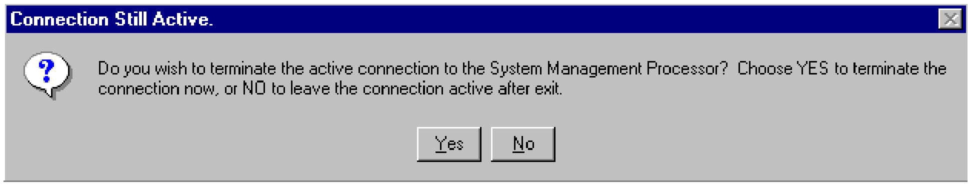
Figure 65. Discover Interconnect

This window shows all the devices on the ASM interconnect bus, other than the one to which you are currently connected (WM7M10A in this example).

4. Select an ASM device from the list displayed.
5. Enter a user ID for logging on to the remote ASM device, type in a user ID and password that will allow access to the remote ASM device. This must match a user ID/password combination that has been configured, using the Advanced System Management service, to allow access to the ASM device.

   The default ID/password is USERID/PASSW0RD. For information on how to configure user ID/password combinations refer to Chapter 4, “Integrating Netfinity Manager with Netfinity Servers” on page 101.
6. Click **Login** to establish the RS-485 link with the selected ASM device.

   Now you can manage and configure the selected ASM device using Advanced System Management. To disconnect the connection, click **Stop** in the Dynamic Connection Manager or Exit from Advanced System Management then click **Yes** when you see the following window:



Do you wish to terminate the active connection to the System Management Processor? Choose YES to terminate the connection now, or NO to leave the connection active after exit.

Figure 66. Connection Still Active

3.4.4 Access with Web Browser/Telnet Client/ANSI Terminal

With Web browser, Telnet client and ANSI terminal emulator applications you can access the ASM interconnect bus via a serial or TCP/IP connection. See 3.6, “Advanced System Management Remote Access” on page 92 for details on how to use these applications with the ASM devices.

Note: This applies only to the ASM PCI adapter and ASM processor. The ASM ISA adapter does not support the ASM interconnect bus.

With the Remote SP Access option (option R in these applications), you can log on to the ASM device and begin a menu-driven session and then log on to other ASM devices, using the first device to talk to the others. After logon, to select the ASM device you will have the same menu to manage and control the Advanced System Management. See 3.6, “Advanced System Management Remote Access” on page 92 for more information.

3.4.5 Sending Alerts Through Shared Resources

You may want to configure an action that sends an alert through the ASM interconnect bus through to a LAN port or modem connected to another server on the bus. This can be configured seamlessly: even though the resource (modem or LAN port) is physically attached to a remote server, the resource appears as being attached to the local server. No additional configuration is required to access the remotely-connected modem or LAN connection.

Each ASM device will have the responsibility of maintaining a table of all active ASM devices and to determine their resources (attached modem, Ethernet or token-ring, firmware level) that are reachable on the interconnect bus.

Each processor and adapter that has a modem, Ethernet, or token-ring connection broadcasts to the other devices on the bus that these resources are available for use by other systems on the ASM interconnect bus. These resources can then be used as ASM Interconnect network resources, enabling any ASM PCI adapter or ASM processor on the interconnect bus to send alerts to a modem or an IP address, even if they do not have a modem or network connection physically attached.

As they generate alerts, the alerts are forwarded to the ASM device on the bus that has the resources necessary to forward the alert. If no system meets the requirements, the alert is not forwarded and is discarded.

If multiple modems or multiple network connections exist on the interconnect bus, you cannot specify which one to use to forward the alert. If an alert is forwarded to another ASM device that is unable to deliver the alert (for example, the modem configured for use has failed or the network cannot resolve the destination IP address), the device will attempt to forward the alert to another system that has the resources necessary to forward the alert as requested. If another system with the necessary resources is not available or the alert still cannot be forwarded it is then discarded.

3.4.6 Implementation Considerations

You should consider the following when implementing an ASM interconnect bus:

- Figure 62 shows the ASM interconnect bus with one Ethernet connection and one modem connection. You may want to consider adding redundant connections to your LAN and to additional modems.
- The network must be set up as a bus, not a ring.
- Only the Advanced System Management PCI Adapter and the Advanced System Management Processor can be connected. The ASM ISA adapter is not supported.
- Up to 12 ASM devices can be connected to the one bus. If a server has both an ASM PCI adapter and an ASM processor, this counts as two.
- The total length of all UTP cables making up the bus can be at most 300 feet.
- To have access to the ASM PCI adapters even when the power to the server room has failed. Use external AC adapters and plug them into a UPS. An AC adapter is included with the ASM PCI adapter option. For the Netfinity 7000 M10, an AC adapter can be ordered separately using part number 83H6739. If you install an ASM PCI adapter in a Netfinity 5000/5500, the AC adapter is required to provide power to the adapter when the server is powered off.
- After you have installed the cables, you must update the firmware of the ASM PCI adapters and ASM processors. Use the Advanced System Management CD-ROM that was shipped with the interconnect cable kit or adapter option or download the latest firmware from:

  `http://www.pc.ibm.com/support`

  Select **Server** from **Select a Brand**.
  Select your server from **Select your family**.
  Click **Downloadable Files**.
  Click **Advanced System Management**.

- Netfinity Manager V5.20.4 or later is required for use of the ASM interconnect bus. You will also need to install the appropriate ASM device driver before you install (or reinstall) Netfinity Manager.

3.4.7 Resolving Problems

If you are having problems connecting ASM PCI adapters and ASM processors via the ASM interconnect bus, check the following:

- Check that all cable connections are firm.
- All cables should be standard UTP. They should not be cross-over cables.
- Cable connections should be server-to-server directly and not via any hubs or switches.
- The ASM interconnect bus must not be connected in a loop.
- Ensure that each ASM device has the latest firmware installed.
- Netfinity 5500 models 8660-1xU and 8660-4xU do not support the ASM interconnect bus.

3.5 The IBM Advanced Systems Management Adapter

The IBM Advanced Systems Management Adapter (part 94G7578) is a full-length ISA card designed to provide comprehensive systems management capability to IBM Netfinity servers.

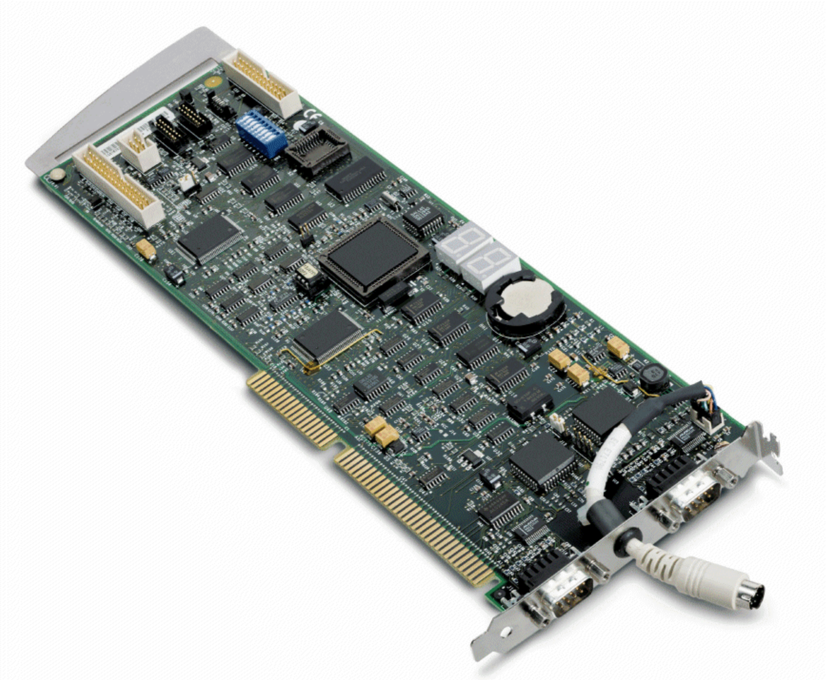


Figure 67. The Advanced Systems Management Adapter

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 I^2C bus of the Netfinity 7000 and other servers for additional systems management functions such as power control, fan, power, security, and temperature monitoring.
- Remote POST Console support on Netfinity 7000 and PC Server 325/330 which echoes text data during system startup to Netfinity Manager or a remote ANSI terminal.

The adapter has two DB9 serial ports, one of which (COM B) supports attachment of a modem for dial-in/dial-out functions. The use of COM A is not supported.

A connector is also provided to connect an external power supply option (part 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. Table 15 lists the servers that require this option:

Table 15. External Power Supply Requirements

Server	External Power Supply Required
Netfinity 3000	Yes
Netfinity 3500	Yes
Netfinity 7000	No

The Advanced Systems Management Adapter can generate the following alerts:

- Operating system hung
- POST sequence timeout
- Loader timeout
- 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 (7000 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 section 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.

3.5.1 Configuration

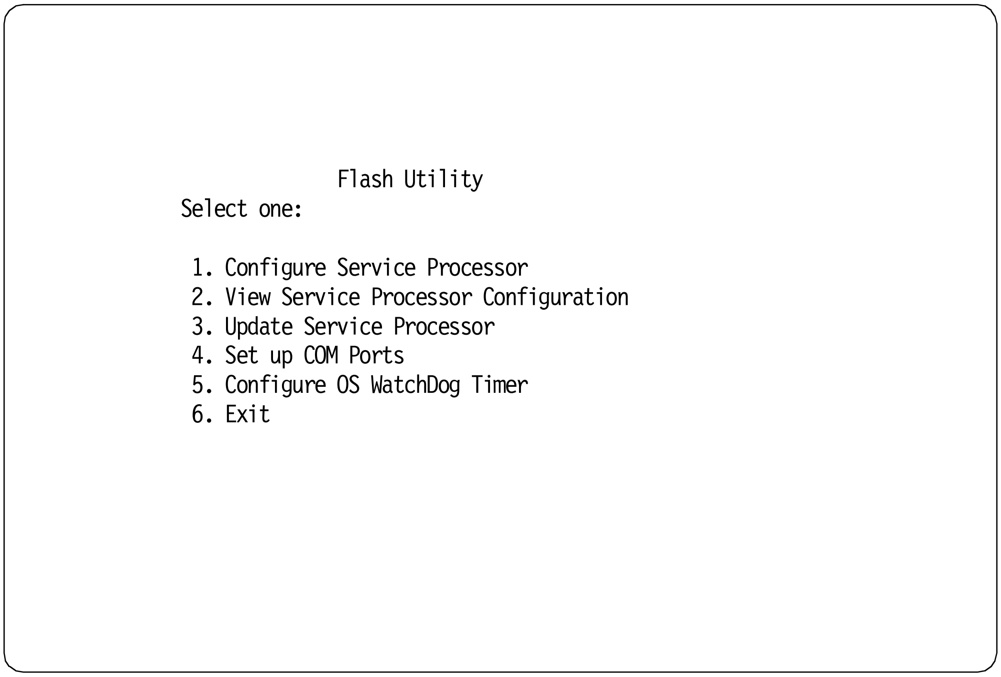
The configuration utility is supplied on diskette with your Advanced Systems Management Adapter. You can also download the latest version from the Web as follows:

`http://www.pc.ibm.com/support`

Select **Server** from **Select a Brand**.
Select your server from **Select your family**.
Click **Downloadable Files**.
Click **Advanced System Management**.

We recommend you use the latest version available.

To start the configuration utility insert the diskette and restart the server. After the welcome screen showing the version number of the utility, you will see Figure 68, 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
```

Figure 68. 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 16 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 16. 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	

Notes:

[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 addresses used by the adapter.

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 instructions on the screen.

4. Set up COM Ports

   This option leads you to the COM port configuration menu, as described in 3.5.2, “ASM ISA Adapter COM Ports” on page 89.

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 4.2.3.6, “O/S Timeout” on page 111 for details.

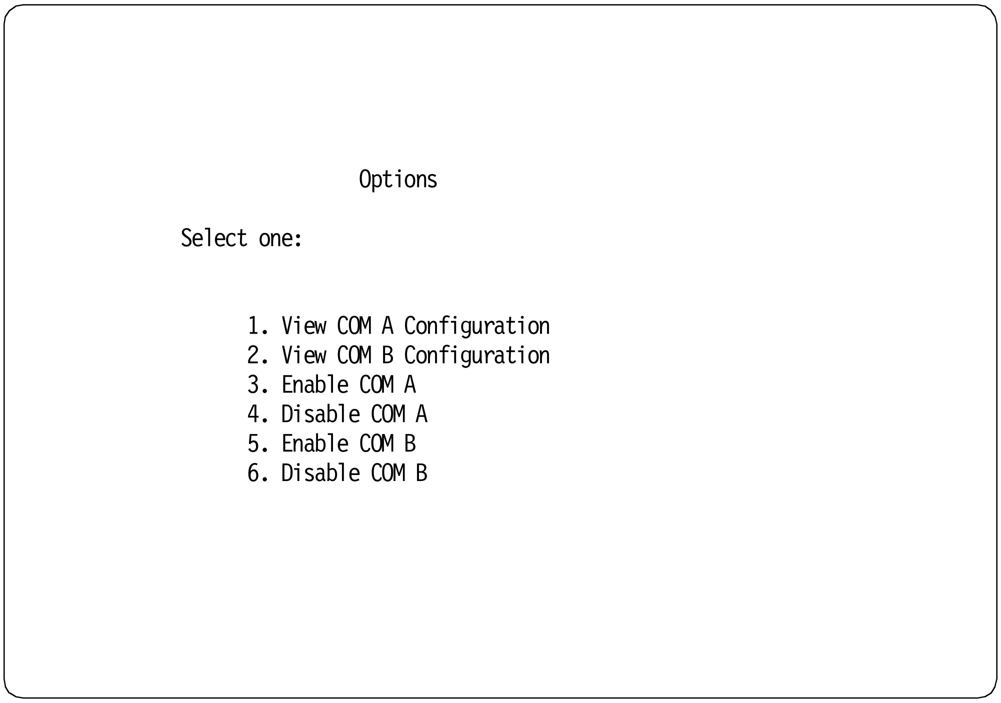
6. Exit

   Save the configuration and exit the utility.

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

3.5.2 ASM ISA Adapter COM Ports

Selecting Option 4, **Set up COM Ports**, from the main menu results in Figure 69 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
```

Figure 69. COM Port Configuration Utility

The options from this menu are:

- **View Configuration (options 1, 2)**

  Display resources currently used for 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

Even though the ability to share COM ports between the adapter and the operating system is possible, this function is no longer supported. A flyer included with the adapter says the following:

> The COM ports on the Advanced Systems Management Adapter cannot be configured for use by the system. Please disregard the information regarding serial port sharing found in the “Service Processor and COM Port Configuration” section of the Advanced Systems Management Adapter Installation Instructions Publication.

For the sake of completeness, however, we describe what enabling a COM port achieves.

For more information, see RETAIN tip H164699.

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 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 loads 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 starts, no active serial connection (dial-in or dial-out) exists. 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 used 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 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 be able to dial in to the Advanced Systems Management Adapter only. The Advanced Systems Management Adapter can dial out when one of the 14 selectable dial-out alerts occurs or when an event log entry is made by Netfinity Manager (requires **Application** be checked in Service Processor Automatic Dialout Settings per Figure 87 on page 118).

  If you want alerts to be forwarded by Netfinity Manager via a serial connection, you need a second modem or a null modem connection. For how to set up alerts see 2.4, "Alerts" on page 25.

  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 saved in SM.INI on the utility diskette. This file provides setup information used during the device driver installation process.

3.5.3 Adapter LEDs

The Advanced Systems Management Adapter has two 7-segment LEDs on board as shown in Figure 70. These display different numbers depending on the status of the server. At boot time, the LEDs display the POST Check Points. After operating system startup, the LEDs display different numbers depending on operating system and server type.

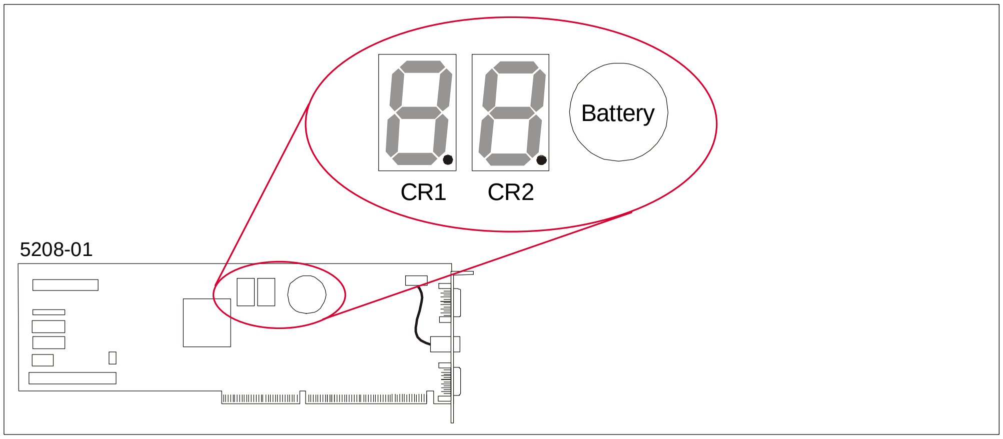


Figure 70. ASM ISA Adapter LEDs

In the power-off status, the LEDs have two dashes in the middle. The status of the dots in each of the characters is as follows:

- CR1: Off=Normal; On=Error has occurred
- CR2: Off=No microcode loaded; On=Normal

Under normal conditions, CR1 is off and CR2 is blinking, indicating that 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.

3.5.4 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`

3.6 Advanced System Management Remote Access

As well as accessing the ASM processors and adapters via Netfinity Manager, you can access them remotely through connections other than the standard client-access LAN ports. The supported connection options vary depending on the device as listed in Table 17:

Table 17. Remote Access Options

Connection Method	ASM PCI adapter	ASM processor	ASM ISA adapter
Netfinity Manager	Yes	Yes	Yes
Terminal emulator	Yes	Yes	Yes
Web browser	Yes	Via ASM PCI adapter[1]	No
Telnet session	Yes	Via ASM PCI adapter[1]	No
Note: 1 Web browser and Telnet access is via an RS-485 ASM interconnect bus connection from a ASM PCI adapter on the same bus.			

This section describes these methods other than Netfinity Manager. The use of Netfinity Manager in conjunction with the ASM devices is discussed in detail in Chapter 4, “Integrating Netfinity Manager with Netfinity Servers” on page 101. Most functions are available using any of the four methods.

When using a Telnet client or Web browser to access the ASM device, you must first configure the network settings of the adapter as described in 3.3.4, “Configuring with DOS-Based Utility” on page 76.

Each of the methods has the same functions, with the exception of the remote video function which is not supported over a Web browser. You can choose the method you find most convenient.

Table 18 lists the options available from the main menu after you have logged on to the ASM processor or ASM PCI adapter. For a complete listing of the menus, see Figure 73 on page 97.

Table 18. Remote Access Menu Descriptions

Menu Selection	Data Available for Viewing
Monitors	System board temperature, microprocessor temperatures, voltage readings, voltage regulator module readings, fan status.
Error Logs	Contents of system error log.
Service Processor Configuration	ASM processor and ASM PCI adapter modem configuration, dial-out entries, dial-out alerts, dial-in logins, system status, thresholds, system statistics, vital product data (VPD) information, and system state.
System Services	Status of watchdog timers and event alerts sent to the host system.
System Power	Current system power status, power-off configuration, and power-off delay values. **Note:** You can use selections available from the System Power menu to power the system on or off.
Boot	You can use selections available from the Boot menu to shut down and restart your system or to restart the Netfinity Advanced System Management processor.
Remote SP Access	Lets you connect to another ASM PCI adapter or ASM processor via the RS-485 ASM interconnect bus.
Remote Terminal	Current remote terminal status.

Menu Selection	Data Available for Viewing
Start Remote Video	Use Start Remote Video to enable your terminal program to remotely monitor and manage the server during POST. Not supported for Web browsers.

3.6.1 Web Browser Access

Note: This function is available only on the ASM PCI adapter (or an ASM processor via an ASM PCI adapter when the adapter and the processor are connected together via an RS-485 ASM interconnect bus.

Once you've configured your ASM PCI adapter and you've configured your adapter as described in Chapter 3.3.4, “Configuring with DOS-Based Utility” on page 76, you can connect to your ASM PCI adapter through a Web browser. Most browsers should work since frames are not used to display the information, but the supported ones are:

- Microsoft Internet Explorer 4.01 with SP1 or later
- Netscape Communicator 4.04 or later

To access the adapter, point your browser to the adapter's TCP/IP address. For example, if you've configured your ASM PCI adapter with address 9.24.105.31:

```
http://9.24.105.31
```

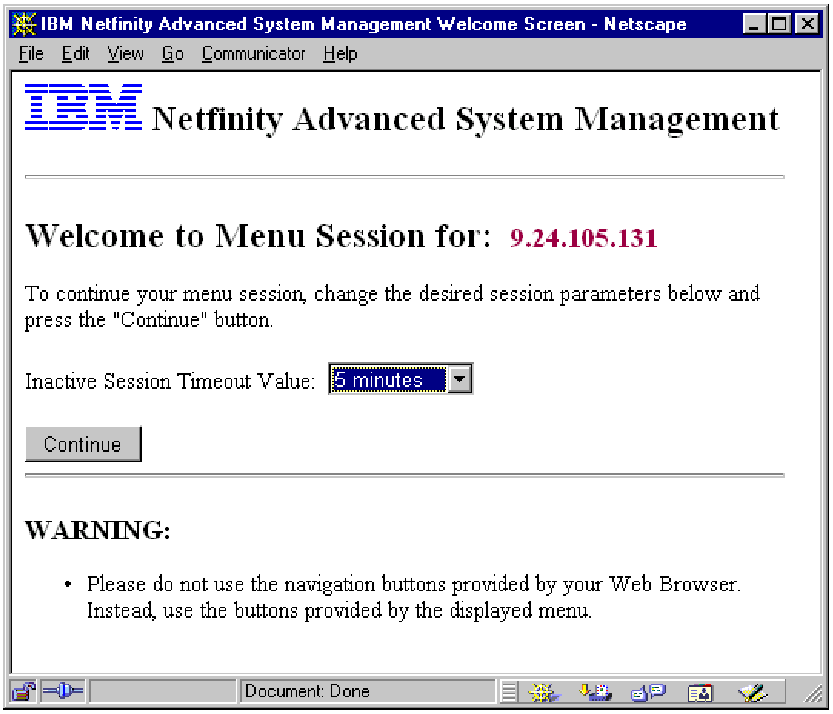
When prompted, fill in the user ID and password. The defaults are:

Userid: USERID
Password: PASSW0RD (zero, not the letter O)

These defaults are case-sensitive. You can create additional user ID/password combinations and remove the default through Netfinity Manager.

Note: If you update the adapter's firmware, the default user ID/password combination is reset back to the default of USERID/PASSW0RD.

After login, you see Figure 71. It displays where you are connected and for security purposes, allows you to set the duration your connection can be idle before disconnecting.


IBM Netfinity Advanced System Management Welcome Screen - Netscape
File Edit View Go Communicator Help

IBM Netfinity Advanced System Management

Welcome to Menu Session for: 9.24.105.131

To continue your menu session, change the desired session parameters below and press the "Continue" button.

Inactive Session Timeout Value: 5 minutes

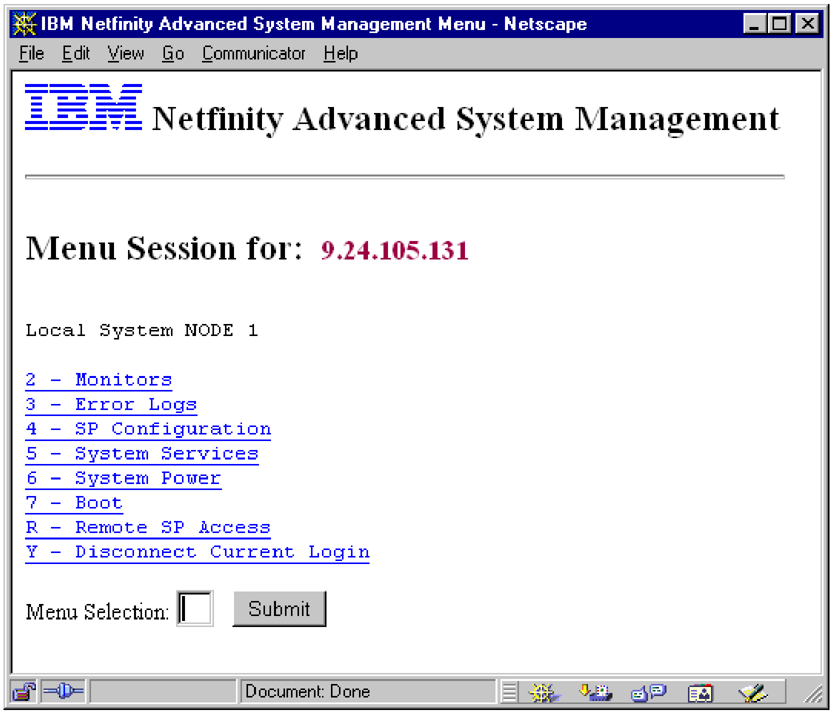
Continue

WARNING:

- Please do not use the navigation buttons provided by your Web Browser. Instead, use the buttons provided by the displayed menu.

Figure 71. ASM PCI Adapter Web Browser Interface Welcome Screen

Click **Continue** to proceed. Figure 72 appears:


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help

IBM Netfinity Advanced System Management

Menu Session for: 9.24.105.131

```
Local System NODE 1

2 - Monitors
3 - Error Logs
4 - SP Configuration
5 - System Services
6 - System Power
7 - Boot
R - Remote SP Access
Y - Disconnect Current Login
```

Menu Selection: Submit

Figure 72. ASM PCI Adapter Web Browser Interface Main Menu

For a complete listing of the menus, see Figure 73 on page 97.

You can navigate these menus as follows:

- To select an entry, click on the link or type the letter in the Menu Selection field and press Submit.
- To return to the previous menu, click the **Previous Menu** button. Do not use the browser's Back button.
- To return to the main menu, click the **Main Menu** button. Do not use the browser's Back button.
- If you have connected to another ASM PCI adapter or ASM processor via the ASM interconnect bus using **R - Remote SP Access**, then the button Main Menu returns you to the main menu of that remote device. To return to the ASM device you connected from, click **Y - Disconnect Current Login**.
- To exit the session, rather than simply closing the browser, you should return to the main menu or the ASM PCI adapter where you initially connected, then click **Y - Disconnect Current Login**.

Some of the menus are read only, so operations such as setting the TCP/IP address of the adapter or the setting of user IDs must be done using Netfinity Manager. Others, however, are active menus, such as those to control power and boot control, where the ASM device executes a command or changes the conditions of the server.

For more information, see *Advanced System Management PCI Adapter Software User's Guide.*

2 - Monitors

- 1 - Temperatures
  - 1 - Planar Temperatures
  - 2 - CPU Temperatures
  - 4 - DASD Temperatures
  - 5 - Ambient Temperatures
- 2 - Voltages
  - 1 - +5V
  - 2 - +3V
  - 3 - +12V
  - 4 - -12V
- 3 - Fans
  - 1 - Fan 1
  - 2 - Fan 2
  - 3 - Fan 3
  - 4 - Fan 4
- 5 - Service Processor Status
  - 1 - Max SLIM Package Size
  - 2 - System Specific
    - 1 - SP BIST (Boot Initial System Test) Results
  - 3 - Reset SP Configuration

3 - Error Logs

- 4 - System Error Log
- 5 - SP Error Log

4 - SP Configuration

- [see Figure 74 on page 98]

5 - System Services

- 1 - Watchdog
  - 1 - Boot
  - 2 - OS
  - 3 - Loader
- 2 - Events
  - 1 - Temperature Threshold
  - 2 - Voltage Threshold
  - 3 - Redundant Power Supply
  - 4 - Power Down
  - 6 - Remote Login

[5.2.2 Continued]

  - 7 - System Tamper
  - 8 - Error Log Full
  - 9 - Fan Fail Event
  - A - Power Supply Fail Event
  - B - DASD Event
  - C - Error Log 75% Full Event
  - D - PFA
- 3 - Post Application Alert
- 6 - POST Enable I2C
- 7 - User Enable I2C
- 8 - Command Table

6 - System Power

- 1 - Current Power Status
- 2 - Power Configuration
  - 1 - Power Off Delay
  - 2 - Power On Time
- 3 - Power Off
  - 1 - Power Off w/OS Shutdown
  - 2 - Power Off Immediately
- 4 - Power On
  - 2 - Power On Release CPU’s Res

7 - Boot

- 1 - Reboot w/OS Shutdown
- 2 - Reboot Immediately
- 4 - Restart SP

B - Remote Terminal Status

- 1 - Remote Terminal Status
- 2 - Remote Keyboard
- 3 - Remote Video
- 4 - Remote Video Control

R - Remote SP Access

- Other ASM devices available on the RS-485 Network

Y - Disconnect Current Login

Z - Start Remote Video

Figure 73. ASCII-Based Telnet, Terminal and Web Browser Menu Tree (Part 1 of 2)

```
4 - SP Configuration
    1 - Modem
        1 - Modem Software Configuration
            1 - Dialin Activated
            2 - SP Owns Serial Port When Booted
            3 - Dialout Table Retry Delay
            4 - Dialout Table Retry Limit
            5 - Dialout Number Retry Delay
            6 - Dialout Tamper Delay
        2 - Port Information
            1 - Port 1
            2 - Port 2
        3 - Dialout Entries
            1 - Dialout Entry 1
                1 - Entry Status
                2 - Phone Number / LAN Address
                3 - Text Description
                4 - Connection Type
                5 - Dialout Login
                6 - Dialout Password
                7 - Text Pager PIN
            2..C - Dialout Entry 2..C
                [same as Dialout Entry 1]
        4 - Dialin Logins
            1 - Dialin Entry 1
                1 - Login ID
                2 - Password
                3 - Last Login
                4 - Flags
                5 - Dialback Number
            2..C - Dialin Entry 2..C
                [same as Dialin Entry 1]
        5 - Dialout Status
            1 - Dialout Status
            2 - Dialout Status
        6 - Current Login Permissions
            1 - Port 1 Permissions
            2 - Port 2 Permissions
        7 - Disconnect Current Login
            1 - Disconnect Port 1
            2 - Disconnect Port
    2 - Dialout Alerts
        1 - Enable Critical Alerts
        2 - Enable Non-critical Alerts
        3 - Enable System Level Alerts
    3 - System Status
        1 - Fan Speed
            1 - Fan 1
            2 - Fan 2
            3 - Fan 3
            4 - Fan 4
        2 - Thresholds
            1 - Temperatures
                1 - Center Temp
                2 - Advanced System Management Temp

[4.3.2.1 continued]
                5 - CPU Temp
                6 - DASD Temperature
                7 - Ambient Temperature
                8 - Fan Panel Ambient
            2 - Voltages
                1 - +5 Volt
                2 - +3 Volt
                3 - +12 Volt
                4 - -12 Volt
        3 - System Statistics
            1 - Power On Seconds
            2 - Number of Reboots
        5 - VPD Information
            6 - SP Firmware VPD
                1 - SP Application Firmware
                2 - SP Boot/Flash Firmware
            7 - Hardware Revision Level
            A - Device Driver
        6 - System State
    4 - SP Clock
        1 - Get/Set SP Clock
    5 - SP Identification
        1 - Text ID
        2 - Numeric ID
    7 - Local Interface Mode
    8 - SP error LED
    9 - Network Configuration
        1 - Network Interfaces
            1 - Network Interface 1
                1 - Line Type
                2 - Enabled
                3 - Host Name
                4 - Host IP Address
                5 - Data Rate
                6 - Duplex
                7 - Hardware (MAC) Address
                9 - Gateway IP Address
                B - PPP Modem COM Port
                C - PPP Remote IP Address
                D - MTU (Maximum Transmission Unit)
                E - Host Subnet Mask
                F - Routing Bytes Disable
            2 - Network Interface 2
                [same as Network Interface 1]
        3 - TCP/IP Properties
            1 - SNMP Configuration
                1 - SNMP System Contact
                2 - SNMP System Location
                3 - SNMP Traps Disable
                4 - SNMP Community Configuration
                5 - SNMP Enable
```

Figure 74. ASCII-Based Telnet, Terminal and Web Browser Menu Tree (Part 2 of 2)

3.6.2 Telnet Access

The Telnet client access offers similar functions to that of Web browser access and serial access.

The default user ID and password are:

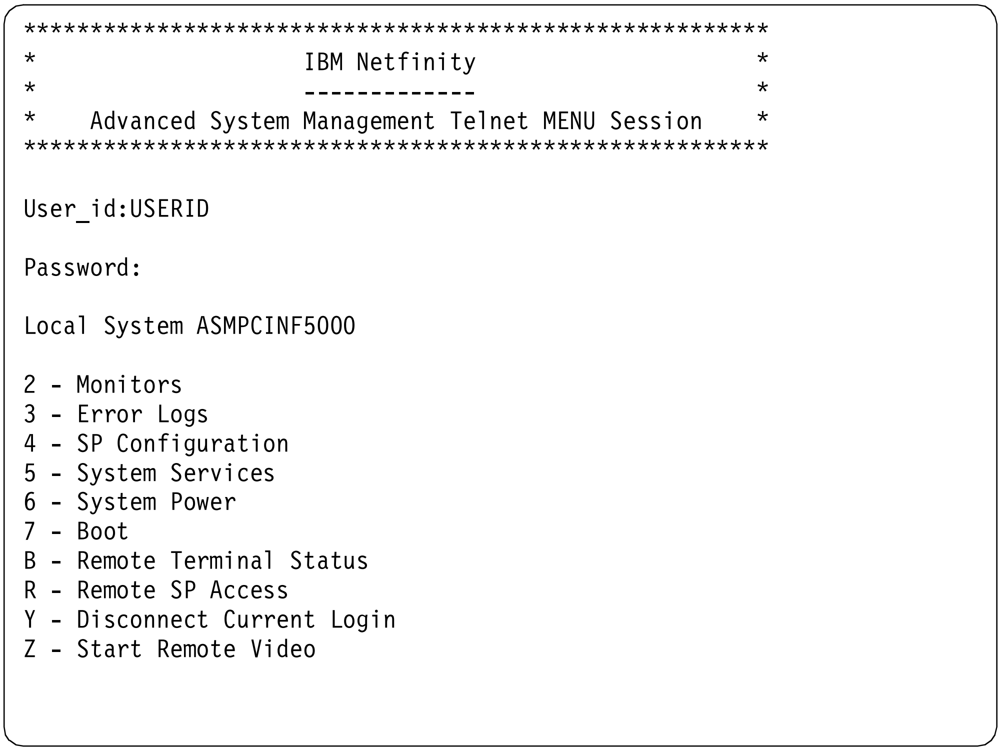
Userid: USERID
Password: PASSW0RD (zero, not the letter O)

These defaults are case-sensitive. You can create additional user ID/password combinations and remove the default through Netfinity Manager. If you update the adapter’s firmware, the default user ID/password combination is reset back to the default of USERID/PASSW0RD.

The interface is also similar as shown in Figure 75:

- To make a menu selection, press the appropriate key.
- To go back up a menu, press the Esc key.
- To exit, press Y, then 0 to exit.

See Figure 73 on page 97 and Figure 74 on page 98 for the complete list of menu choices.



```
********************************************************
*                    IBM Netfinity                     *
*                    -------------                     *
*    Advanced System Management Telnet MENU Session    *
********************************************************

User_id:USERID

Password:

Local System ASMPCINF5000

2 - Monitors
3 - Error Logs
4 - SP Configuration
5 - System Services
6 - System Power
7 - Boot
B - Remote Terminal Status
R - Remote SP Access
Y - Disconnect Current Login
Z - Start Remote Video
```

Figure 75. Telnet Client Remote Access

3.6.3 Terminal Emulator Access

Terminal emulator or serial access can be achieved either through modems or through a null modem connection. This function is available on all three ASM devices. You would normally use an ASCII terminal program such as HyperTerminal to interface with the ASM device. Modem settings required are:

- Baud: 57.6 kbps
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: Hardware

Once you connect, you will be asked for a user ID and password. The defaults are:

Userid: USERID
Password: PASSW0RD (zero, not the letter O)

These defaults are case-sensitive. You can create additional user ID/password combinations and remove the default through Netfinity Manager. If you update the adapter’s firmware, the default user ID/password combination is reset back to the default of USERID/PASSW0RD.

The menu choices are similar to those of the Web browser and Telnet accesses.

See the User’s Handbook for your adapter or server for more information.

Chapter 4. Integrating Netfinity Manager with Netfinity Servers

Now that we have discussed the functions of Netfinity Manager and the Advanced System Management devices, it is appropriate to describe how the hardware and software integrate. This chapter describes how to configure and enable the functions of the three ASM devices using Netfinity Manager and how to enable dial-out alerts.

The use of the ASM devices without Netfinity Manager is described in 3.6, “Advanced System Management Remote Access” on page 92.

Note: This chapter is based on Netfinity Manager V5.20.4. Earlier versions may not have all the functions described here, and may not support the latest hardware such as the ASM interconnect bus.

If you have followed the steps as described in 3.3.4, “Configuring with DOS-Based Utility” on page 76, your ASM device should now be configured to use a TCP/IP, serial or RS-485 connection. In order to configure other features of the ASM processor and ASM PCI adapter such as dial-in, dial-out and SNMP messaging, you need to use Netfinity Manager:

Table 19 shows the available options to connect to your ASM devices using Netfinity Manager.

Table 19. Connecting to ASM Devices Using Netfinity Manager

Connection Options	ASM PCI adapter	ASM processor	ASM ISA adapter
Locally via ASM service[1]	Supported	Supported	Supported
Via RSM service[1]	Supported	Supported	Supported
Serial via DCM[2]	Supported	Supported	Supported
TCP/IP via DCM	Supported	Supported[3]	No
RS-485 via DCM	Supported	Supported	No

Notes:

1 Using the Advanced Systems Management (ASM) service either locally on the server or remotely using the Remote System Manager (RSM) service. Netfinity Manager must be installed with the Advanced System Management Support option on both the administrator’s workstation and on the server.

2 DCM is Dynamic Connection Manager. Serial connections are via modems or a null modem cable.

3 Access an ASM processor via DCM using TCP/IP only when an ASM PCI adapter is also installed and connected to the ASM processor via an ASM interconnect bus.

Note: Table 19 lists only connection options involving Netfinity Manager. For details on connecting to ASM devices without Netfinity Manager, see 3.6, “Advanced System Management Remote Access” on page 92.

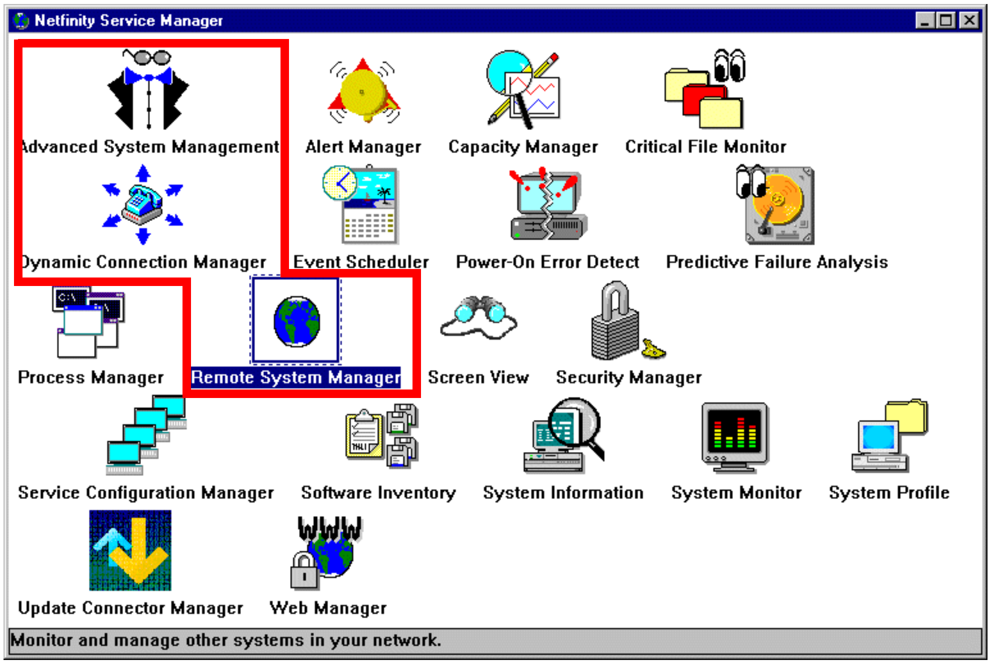


Figure 76. Netfinity Manager Main Window

There are two ways you can connect to the Advanced System Management devices through Netfinity Manager:

1. Using the Remote System Manager icon to connect to a remote server also running Netfinity Manager. Connections to the adapter are via the ASM device drivers interface into Netfinity Manager (see 3.3.1, “Device Drivers” on page 74). This is the normal method of connecting to remote Netfinity Manager systems. See 2.3.14, “Remote System Manager” on page 17 for details.
2. Using the Dynamic Connection Manager icon. This method allows direct connection to the ASM device via a modem, null modem, TCP/IP or via the RS-485 ASM interconnect bus. This is discussed in more detail in 4.1, “Dynamic Connection Manager” on page 103.

Once you establish a connection to the ASM device, you use the Advanced System Management icon to perform actions. See 4.2, “Advanced System Management” on page 106 for details.

Netfinity 5000/5500 with ASM PCI Adapter

If you have a Netfinity 5500 or 5000 system with an ASM processor and you have additionally installed an ASM PCI adapter, it is important to realize how the management functions are divided between the two:

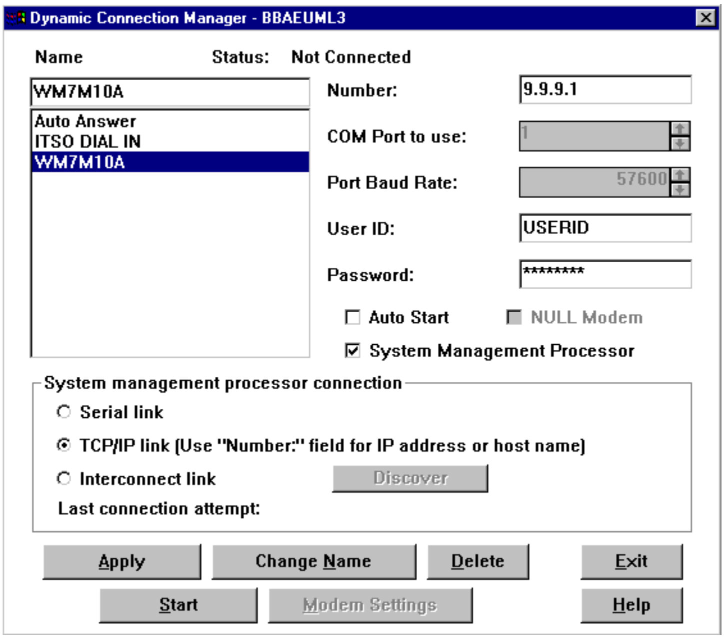
- The ASM PCI adapter acts as a network gateway only
- The ASM processor handles all management data

Consequently, you must configure the ASM processor to enable or disable the functions described in this chapter.

4.1 Dynamic Connection Manager

Dynamic Connection Manager is the Netfinity Manager service where you configure transient connections from Netfinity Manager:

- Modem to another Netfinity Manager system
- Null modem to another Netfinity Manager system
- Serial connection to an ASM device
- TCP/IP connection to an ASM device
- RS-485 connection to an ASM device



Dynamic Connection Manager - BBAEUML3

Name: WM7M10A
Status: Not Connected

Auto Answer
ITSO DIAL IN
WM7M10A

Number: 9.9.9.1
COM Port to use: 1
Port Baud Rate: 57600
User ID: USERID
Password: ********

□ Auto Start
□ NULL Modem
☑ System Management Processor

System management processor connection
○ Serial link
● TCP/IP link (Use "Number:" field for IP address or host name)
○ Interconnect link
Last connection attempt:

Figure 77. Dynamic Connection Manager

Dynamic Connection Manager is a replacement for the Serial Connection Control function of earlier versions of Netfinity Manager. However, if you don't select **Advanced System Management Support** during installation, you'll get Serial Connection Control instead, which lets you connect to modems and null modems only.

With the modem and null modem options, once you establish a connection to another Netfinity Manager system, you have access to the full range of Netfinity Manager services. However, with the ASM device options, once you establish the connection, you will have access only to the Advanced System Management service on the remote system.

Unlike the use of the Advanced System Management service in Netfinity Manager, there is no need to install the ASM device driver on the target system.

The System management processor connection options let you do the following:

- Serial link: Allows you to connect from Netfinity Manager via modem or null modem to the serial port of an ASM device. All devices are supported including the ASM ISA adapter.

This option is available in Dynamic Connection Manager as shown in Figure 77 on page 103 in Netfinity Manager V5.20.3 onward. In older versions, this option is available in the Serial Connection Control.

- TCP/IP link: Allows you to connect from Netfinity Manager via your LAN to the Ethernet (or token-ring port if you have installed that option) of an ASM PCI adapter.

  Only the ASM PCI adapter supports this connection. If you have a Netfinity 5000/5500 with an ASM PCI adapter installed, it is supported as well. This option is available in Netfinity Manager V5.20.3 onward.

- Interconnect link: Allows you to connect from Netfinity Manager via the Netfinity Advanced System Management Interconnect Bus of an ASM PCI adapter or ASM processor. The ASM ISA adapter is not supported. This option is available in Netfinity Manager V5.20.4 onward. For information on how to set up and access your ASM interconnect bus see 3.4, “ASM Interconnect Network” on page 80.

Note: Advanced System Management Support must be installed on the local workstation. An ASM device does not have to be installed locally.

4.1.1 Serial Link

To dial into a remote server’s ASM device using a modem or null modem connection, do the following:

1. On the server, set up a user ID and password per 4.2.3, “Configuration Settings” on page 108.
2. On your local workstation, configure a dial-out entry in Dynamic Connection Manager (Figure 77 on page 103):
   – Enter a name for the dial-out entry.
   – Enter the phone number or check **NULL Modem**.
   – Specify the COM port where your modem is connected.
   – Specify the baud rate.
   – Enter the user ID and password you set up in step 1.
3. Click the **System Management Processor** check box.
4. Click **Serial link**.
5. Click **Apply** to save the entry.
6. Click **Start** to dial.

If the connection is successful, you should then be able to start the **Advanced System Management** service in Netfinity Manager to access the remote server’s ASM device.

4.1.2 TCP/IP Link

To connect to a remote server’s ASM PCI adapter through its Ethernet or token-ring port, complete the following steps:

1. If you have not done so already, configure the adapter’s system identification and network settings locally using either Netfinity Manager as described in 4.2.5, “Network Settings” on page 116 or the DOS configuration utility as described in 3.3.4, “Configuring with DOS-Based Utility” on page 76.

2. On the server, set up a user ID and password per 4.2.3, “Configuration Settings” on page 108.
3. On your local workstation, configure an entry in Dynamic Connection Manager (Figure 77 on page 103):

   – Enter a name for the entry.
   – Enter the TCP/IP address in the Number field.
   – Enter the user ID and password you set up in step 2.
4. Click the **System Management Processor** check box.
5. Click **TCP/IP link**.
6. Click **Apply** to save the entry.
7. Click **Start** to dial.

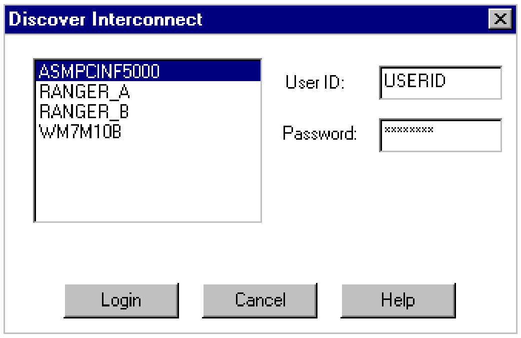
If the connection is successful, you should then be able to start the **Advanced System Management** service in Netfinity Manager to access the remote server’s ASM device.

4.1.3 Interconnect Link

To connect to a remote server’s ASM PCI adapter through its RS-485 ASM interconnect bus port, do the following:

1. On the server, set up a user ID and password per 4.2.3, “Configuration Settings” on page 108.
2. On your local workstation, configure an entry in Dynamic Connection Manager (Figure 77 on page 103):

   – Enter a name for the entry.
3. Click the **System Management Processor** check box.
4. Click **Interconnect link**.
5. Click the **Discover** button. Figure 78 appears:


Discover Interconnect

ASMPCINF5000
RANGER_A
RANGER_B
WM7M10B

User ID: USERID

Password: ********

Figure 78. Discover Window

6. Select the remote server from the list.
7. Enter the user ID and password you set up in step 1.
8. Click **Login** to connect to the server. You will then return to the Dynamic Connection Manager window (Figure 77 on page 103).
9. Click **Apply** to save the entry.

If the connection is successful, you should then be able to start the **Advanced System Management** service in Netfinity Manager to access the remote server's ASM device.

Note: If you get your user ID or password wrong, the connection won't be established, but you won't get any error messages.

4.2 Advanced System Management

Advanced System Management

This icon gives you access to the ASM device in your server. The function is installed when you select **Advanced System Management Support** during the installation of Netfinity Manager.

Note: To use the Advanced System Management icon, you must first install the appropriate ASM device driver as described in 3.3.1, "Device Drivers" on page 74.

Double-clicking **Advanced System Management** produced Figure 79:

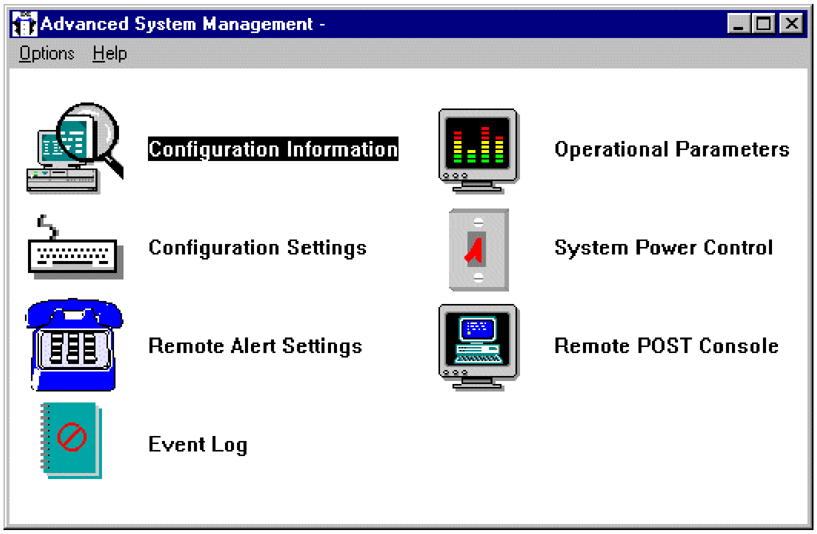


Figure 79. ASM Device Window

4.2.1 Remote BIOS Flash

Through the Advanced System Management service in Netfinity Manager, you can update the system BIOS and the firmware of the ASM device. From the Advanced System Management service, click **Options -> Update Microcode...** and select either **System Management Processor** or **BIOS**.

Updating of the system BIOS is supported only when using "out-of-band" connections to the server such as RS-485, serial and TCP/IP connections directly to the adapter. Updating the system BIOS is not supported when using Remote System Manager. However, you can use Remote System Manager to connect to another server and then use the RS-485 ASM interconnect bus to connect to the server you want to update.

Table 20 shows what connection can be used to update your server BIOS and ASM device remotely:

Table 20. ASM and System BIOS Update Options

Connection Method	ASM PCI Adapter	ASM Processor	ASM ISA Adapter
Serial	ASM and System	ASM and System	ASM only
RS-485	ASM and System	ASM and System	No
Serial and RS-485[1]	ASM and System	ASM and System	No
TCP/IP	ASM and System	No	No
TCP/IP and RS-485[1]	ASM and System	ASM and System[2]	No
Remote System Manager	No	ASM only	ASM only
Remote System Manager and RS-485[1]	ASM and System	ASM and System	No

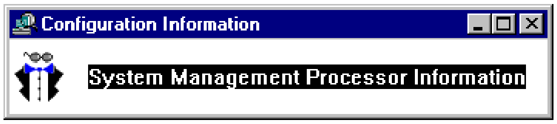
Notes:
1 These dual connections involve connecting to another server using the first method then using RS-485 to connect to the server you wish to update.
2 Supported when the ASM processor is connected to an ASM PCI adapter via RS-485.

4.2.2 Configuration Information

Configuration information gives you vital product data (VPD) information about the following components:

- ASM device microcode and driver levels
- System (BIOS level, model, serial number, etc.)
- Power supplies and power backplane
- Internal hot-swap backplane
- System board
- Processor board
- Memory DIMM size, speed, serial number (Netfinity 5500 and Netfinity 7000 M10)
- I/O Card VPD Netfinity 7000 M10 only

Double-clicking **Configuration Information** displays Figure 80 or Figure 81 depending on what ASM device you have:



Configuration Information

System Management Processor Information

Figure 80. Configuration Information for the Advanced Systems Management Adapter

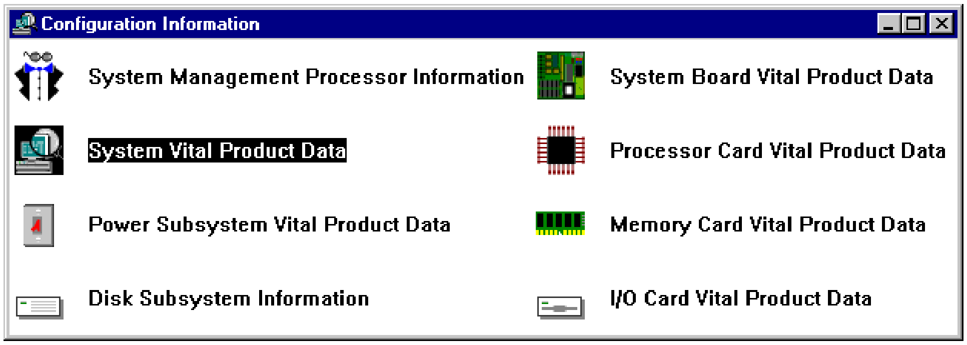
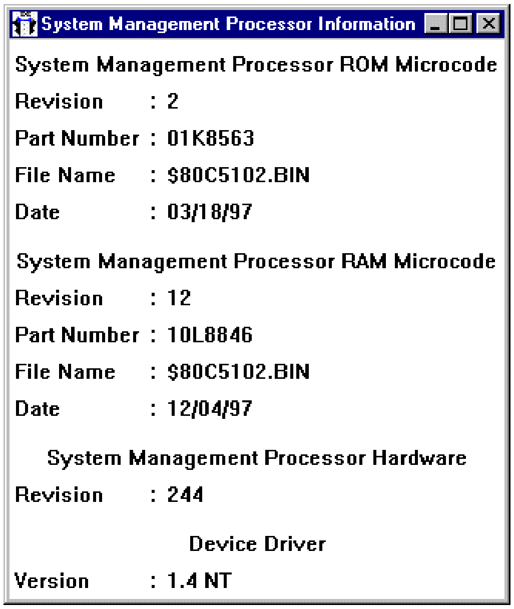

Configuration Information
System Management Processor Information
System Board Vital Product Data
System Vital Product Data
Processor Card Vital Product Data
Power Subsystem Vital Product Data
Memory Card Vital Product Data
Disk Subsystem Information
I/O Card Vital Product Data

Figure 81. Configuration Information for Advanced System Management PCI Adapter

Double-clicking **System Management Processor Information** shows the firmware levels of the ASM device as shown in Figure 82:



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
```

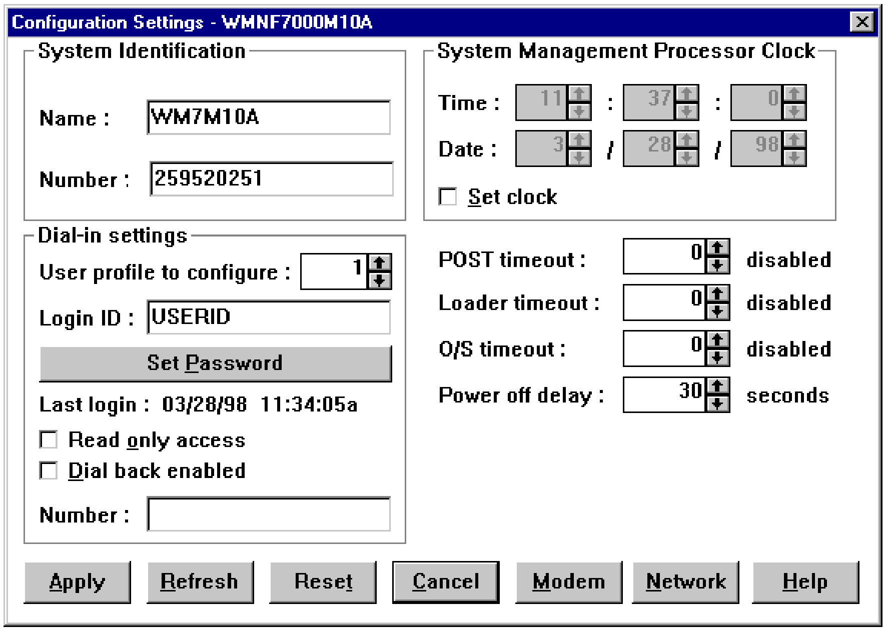
Figure 82. ASM Processor Information

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

- 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 DIMM’s size, speed, and serial number

4.2.3 Configuration Settings

The Configuration Settings window (Figure 83) 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 and network settings here.


Configuration Settings - WMNF7000M10A

System Identification

Name : WM7M10A

Number : 259520251

System Management Processor Clock

Time : 11 : 37 : 0

Date : 3 / 28 / 98

□ Set clock

Dial-in settings

User profile to configure : 1

Login ID : USERID

Last login : 03/28/98 11:34:05a

□ Read only access

□ Dial back enabled

Number :

POST timeout : 0 disabled

Loader timeout : 0 disabled

O/S timeout : 0 disabled

Power off delay : 30 seconds

Figure 83. ASM Configuration Settings

Each of the items in this window is described below:

4.2.3.1 System Identification

These two fields let you enter a name and phone number that will identify the ASM device. The phone number is for informational purposes only.

4.2.3.2 System Management Processor Clock

The ASM device has its own independent clock. This clock is used to record the time and date for every operation of the ASM device, 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 clock** check box. You can then change the time and date using the spin controls, then press **Apply** to save the changes.

4.2.3.3 Dial-In Settings

The dial-in group of properties in Figure 83 lets you enable or disable dial-in support, enable users to dial in to and access the ASM device. These properties are:

- User Profile to Configure

  Use the spin buttons to select the user profile you want to configure. With the ASM processor and ASM PCI adapter, you can configure up to 12 user profiles. When using the ASM ISA adapter, you can configure up to six separate 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 in to this machine. A login ID must be specified to enable remote access. The default user ID is USERID for the ASM PCI adapter and ASM processor. (The ASM ISA adapter does not have a default user ID).

- 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 ASM device. After providing a login ID, click the **Set Password** button to open the Set Password window. The default password for USERID is PASSW0RD with a zero instead of an O.

  User IDs

  With the ASM PCI adapter, the user ID and password, once created, can also be use to log in via TCP/IP link or Interconnect link.

  On the ASM processor, the user ID and password can also be used to log in via Interconnect link.

- 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 ASM device 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 ASM device 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 the **Modem** button in Figure 83 on page 109 to access the Modem Settings window. These settings enable you to specify modem settings and dialing settings. See 4.2.4, “Port and Dialing Settings” on page 112 for details.

Creating a New User

To create a new login ID for a remote user:

1. At the User profile to configure field, 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 ASM device, click the **Set Password** button and enter a password for them to use.
4. Click **Apply** to remove the user ID.

Note: We recommend you set a password to prevent unauthorized access to your system. If you do not configure a password, any remote user that knows the configured login ID can use the Advanced System Management service to access your system's ASM device. If you configure a password, remote users will have to supply both the correct login ID and the correct password to access the ASM device. 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 **Apply** to remove the user ID.

4.2.3.4 POST Timeout

The POST timeout field shows the number of seconds that the ASM device will wait for the server's POST to complete.

Note: This function is not supported by the ASM ISA adapter except when installed in a Server 325 or Server 330 system.

If the POST takes longer than the time specified, the ASM device will generate a POST timeout event and forward a POST timeout alert to all enabled dial-out entries. See 4.2.6, “Remote Alert Settings” on page 117 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 automatically reboot on the second successive POST timeout.

4.2.3.5 Loader Timeout

The Loader timeout field is used to configure the time the ASM device will allow the server to load the operating system before it initiates a system restart. The operating system is considered loaded once the ASM driver is started.

Note: This is *not* supported by the ASM ISA adapter except when installed in a Server 325 or Server 330.

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 ASM driver.

If the time between POST and the end of operating system startup exceeds the configured time, the ASM device will generate a loader timeout event and forward a loader timeout alert to all *enabled* dial-out entries with the Loader timeout field selected in their Automatic Dial-out Settings configuration (see 4.2.6, “Remote Alert Settings” on page 117).

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

4.2.3.6 O/S Timeout

The OS timeout field is used to configure the time the ASM device will wait before it initiates a system restart, in case the operating system stops responding to the ASM device. This is also known as the OS watchdog timer.

If the response time exceeds the configured value, the ASM device will generate an OS timeout event and forward an OS timeout alert to all enabled dial-out entries that have OS timeout selected in their automatic dial-out settings configuration (see 4.2.6, “Remote Alert Settings” on page 117). The system will then be rebooted.

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

4.2.3.7 Power Off Delay

When a shutdown is requested via the ASM device, the operating system is either shut down (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 shut down.

The Power off delay field is used to configure the time the ASM device will wait for the operating system to shut down before powering off the system, when such problems occur. If the ASM device 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 4.2.6, “Remote Alert Settings” on page 117).

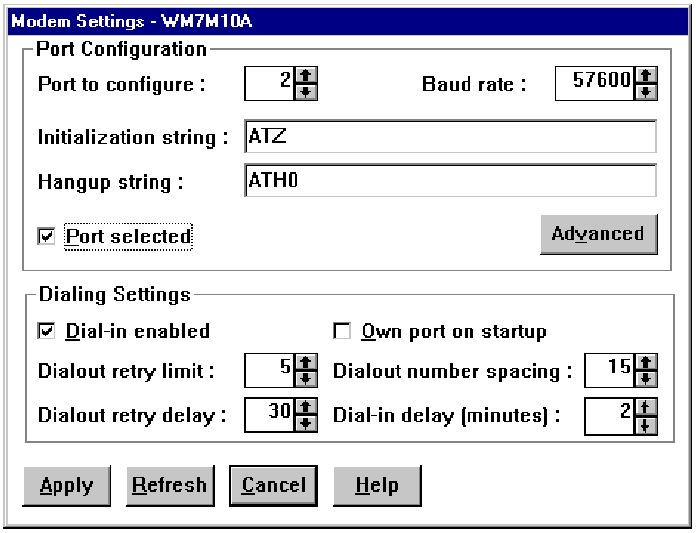
To find out what is a suitable value to put here, we recommend you time how long it takes to shut down your server when no problems occur, then set the power-off delay to a value slightly above this time.

Click Apply to Save

If you change any option or setting, you must click the **Apply** button to store these changes in the ASM device.

4.2.4 Port and Dialing Settings

Clicking the **Modem** button in the window shown in Figure 83 on page 109 brings up the Modem Settings window shown in Figure 84. There are two groups of properties in this window: Port Settings and Dialing Settings.


Modem Settings - WM7M10A

Port Configuration

Port to configure : 2

Baud rate : 57600

Initialization string : ATZ

Hangup string : ATH0

☑ Port selected

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 84. ASM Device Modem Settings

4.2.4.1 Port Settings

Use the Modem Settings group to specify and configure the modem that will be used to forward the alert when an ASM device dial-out event occurs.

- Port to Configure

  This option lets you select the ASM device port connected to the modem. With the Advanced Systems Management Adapter, there will be only one option, “1” as the ASM ISA adapter only uses a modem on COM B. The ASM processor and ASM PCI adapter let you configure any of the shared or ASM dedicated ports.

  For details on the ports associated with the ASM processor and ASM PCI adapter, see 3.3.5, “COM Ports” on page 79. For more information on the ASM ISA adapter, see 3.5.2, “ASM ISA Adapter COM Ports” on page 89.

- Baud Rate

  Use the spin buttons to specify the speed you wish to set the modem. 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 to enter modem commands that perform the following functions:

  – Command echoing OFF
  – Online character echoing OFF
  – Result codes ENABLED
  – Verbal result codes ENABLED
  – All codes and Connect messages with BUSY and DT detection
  – Protocol identifiers added - LAPM/MNP/NONE V42bis/MNP5
  – Normal CD operations
  – DTR ON-OFF hangup, disable AA and return to command mode
  – CTS hardware flow control
  – RTS control of received data to computer
  – Queued and nondestructive break, no escape state

- Caller ID String

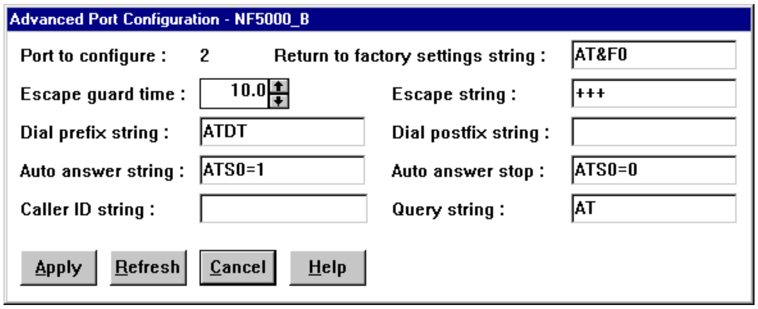
  This field is currently not implemented and should be left blank. This field is not available with the Advanced Systems Management Adapter.

- Port Selected (only ASM PCI adapter and ASM ISA adapter)

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

4.2.4.2 Advanced Port Settings

Clicking the **Advanced** button in Figure 84 produces Figure 85:



Advanced Port Configuration - NF5000_B

Port to configure :	2	Return to factory settings string :	AT&F0
Escape guard time :	10.0	Escape string :	+++
Dial prefix string :	ATDT	Dial postfix string :	
Auto answer string :	ATS0=1	Auto answer stop :	ATS0=0
Caller ID string :		Query string :	AT

Figure 85. Advanced Port Configuration

On supported systems, this window enables you to specify additional modem settings. You should not need to change these settings unless your alert forwarding functions are not working properly.

The Advanced Port Configuration window contains the following items:

- Port to Configure

  This is the port configuration entry currently selected in the Modem Settings window.

- Return to Factory Settings String

  Type in this field the string that should be used to make the modem return to its factory settings when it is initialized. The default is AT&F0.

- Escape Guard Time

  Use this spin button to specify the length of time before and after the escape string is to be issued to the modem. The default is 1 second.

- Escape String

  Type in this field the string that should be used to return the modem to command mode when it is currently connected to another modem. The default is +++.

- Dial Prefix String

  Type in this field the string that should be issued prior to the number to be dialed. The default is ATDT.

- Dial Postfix String

  Type in this field the string that should be issued after the number is dialed to tell the modem to start dialing.

- Auto Answer String

  Type in this field the string that should be used to tell the modem to answer the phone when it rings. The default is to answer after two rings or ATS0=1.

- Auto Answer Stop String

  Type in this field the string that should be used to tell the modem to stop answering the phone when it rings. The default is ATS0=0.

- Caller ID String

  Type in this field the string that should be used to get caller ID information from the modem.

- Query String

  Type in this field the string that should be used to find out if the modem is attached. It should be an AT command that has OK as an answer and returns in less that 200 ms. The default is AT.

4.2.4.3 Dialing Settings

Use the Dialing Settings group to specify settings that will be used to forward the alert when an ASM device dial-out event occurs.

- Dial-In Enabled

  Mark this check box to enable remote users to dial in to and access the ASM device. If this box is unchecked, remote users will be unable to dial in to the ASM device.

- Own Port on Startup

  Advanced System Management PCI Adapter and Advanced System Management Processor

  If that box is checked, your ASM PCI adapter will take over an operating system COM port. The serial device connected to the ASM PCI adapter will not be available for OS use. All dial-in and dial-out options are fully functional.

  If that box is not checked the OS can take over the serial device connected to your ASM PCI adapter. The COM port acts as a normal OS device until a critical alert occurs. If a critical alert is triggered, the ASM PCI adapter will regain the COM port and send out the alert. The OS will not regain the COM after the alert is sent.

  Advanced Systems Management Adapter

  With the ASM ISA adapter, you need to mark this check box if you disabled COM B. Configuration Utility (see 3.5.2, “ASM ISA Adapter COM Ports” on page 89). 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, unmark this check box.

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

- Dial-Out Retry Limit

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

- Dial-Out Delay

  Select a delay in seconds before the ASM device retries to forward the alert again.

- Dial-Out Number Spacing

  If you have configured more than one dial-out entry to forward alerts, the ASM device will attempt to contact each of these entries sequentially. Use the spin buttons to specify the number of seconds that the ASM device 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 ASM device, before any valid dial-in access will be permitted.

  Note: If six failed attempts are made to dial in to the adapter, the adapter will generate a “Tamper” event, as described in 4.2.6, “Remote Alert Settings” on page 117.

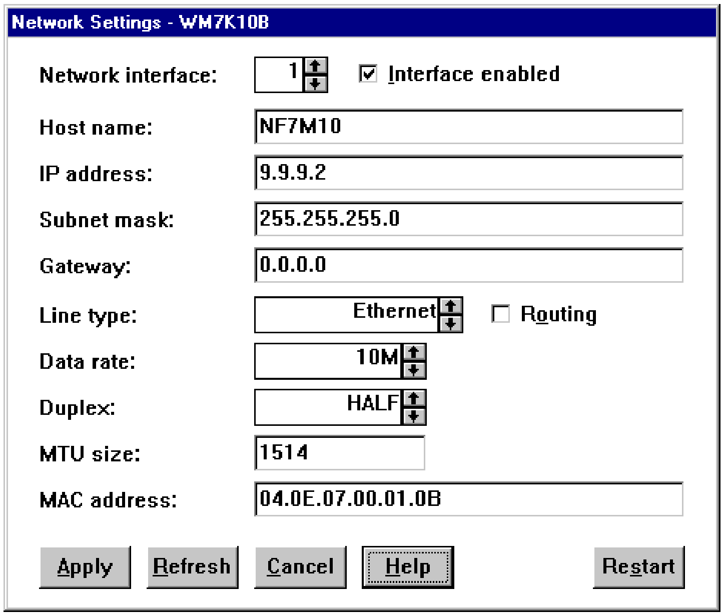
Click on Apply to Save

If you change any option or setting, you must click the **Apply** button to store these changes in the ASM device.

4.2.5 Network Settings

Clicking the **Network** button in Figure 83 on page 109 produces Figure 86.

This window is available only if you have an ASM PCI adapter. It lets you specify your TCP/IP setting. The configuration fields are the same as in the DOS-based configuration utility.



Network Settings - WM7K10B

Network interface: 1 ☑ Interface enabled

Host name: NF7M10

IP address: 9.9.9.2

Subnet mask: 255.255.255.0

Gateway: 0.0.0.0

Line type: Ethernet □ Routing

Data rate: 10M

Duplex: HALF

MTU size: 1514

MAC address: 04.0E.07.00.01.0B

Figure 86. TCP/IP Network Settings for ASM PCI Adapter

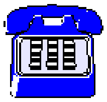
- Network interface. Use the spin buttons to select a network interface to configure. When you have selected the network interface you want to use, mark the **Interface enabled** check box. Interface 1 refers to Ethernet, Interface 2 refers to token-ring.
- Host name. Type the TCP/IP host name that will be used by the Advanced System Management PCI Adapter.
- IP address. Type the IP address that will be used by the Advanced System Management PCI Adapter.
- Subnet mask. Type the subnet mask that will be used by the Advanced System Management PCI Adapter.

- Gateway address. Type the TCP/IP address of the gateway that will be used by the Advanced System Management PCI Adapter.
- Line type. Use the spin buttons to select the line type that will be used by the Advanced System Management PCI Adapter. Available selections are Ethernet, PPP, and token-ring. Mark the Routing check box if needed.
- Data rate. Use the spin buttons to select the data rate that will be used by the Advanced System Management PCI Adapter. Available selections are AUTO, 4M, 16M, 10M, and 100M.
- Duplex method. Use the spin buttons to select the duplex method that will be used by the Advanced System Management PCI Adapter. Available selections are AUTO, FULL and HALF.
- MTU size. Type the maximum transmission unit (MTU) value that will be used by the Advanced System Management PCI Adapter.
- MAC address. Type the media access control (MAC) address of the network adapter being used by the Advanced System Management PCI Adapter. The default value 00.00.00.00.00.00 will indicate the adapter is to use the burnt-in MAC address.

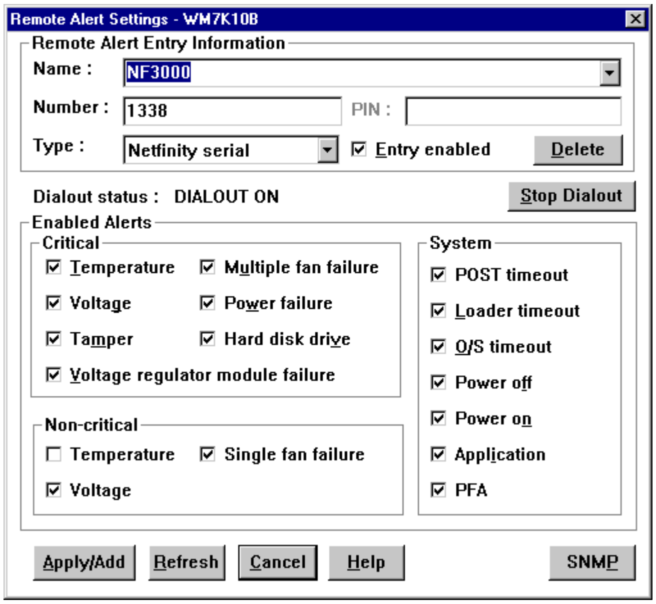
> **MAC Address**
>
> If you apply or change the MAC address space make sure no other adapter uses that address.

After making any changes to these settings, first click **Apply** to save the changes and then click **Restart** to restart the ASM PCI adapter so that the changes will take effect. Changes to Network Settings on the adapter will not take effect until the adapter has been restarted.

4.2.6 Remote Alert Settings



Double-clicking the **Remote Alert Settings** icon yields Figure 87:


Remote Alert Settings - WM7K10B

Remote Alert Entry Information

Name : NF3000

Number : 1338 PIN :

Type : Netfinity serial ☑ Entry enabled

Dialout status : DIALOUT ON

Enabled Alerts

Critical

☑ Temperature ☑ Multiple fan failure
☑ Voltage ☑ Power failure
☑ Tamper ☑ Hard disk drive
☑ Voltage regulator module failure

Non-critical

□ Temperature ☑ Single fan failure
☑ Voltage

System

☑ POST timeout
☑ Loader timeout
☑ O/S timeout
☑ Power off
☑ Power on
☑ Application
☑ PFA

Figure 87. ASM Device Remote Alert Settings

This is where you configure when and how the ASM device generates an alert and sends it to a remote machine. You can configure the adapter to send alerts when particular critical and non-critical alerts occur and these alerts can be sent to different types of devices. Table 21 shows which devices support the different remote alert methods:

Table 21. Remote Alert Capability

Alert Method	ASM PCI Adapter	ASM Processor	ASM ISA Adapter
Numeric Pager	Supported	Supported	Supported
Alpha-numeric Pager	Supported	Supported	Supported
Serial link to NFM	Supported	Supported	Supported
TCP/IP link to NFM	Supported	Supported[1]	No
SNMP Trap	Supported[2]	No	No

Notes:
1 Only available on the ASM processor when connected to an ASM PCI adapter via RS-485
2 When an ASM PCI adapter is installed in a system with an ASM processor, SNMP traps are not supported. This is because the ASM PCI adapter acts only as a network interface.

If you have an RS-485 network between ASM devices, it will automatically be searched for modem and network resources as described in 3.4.5, “Sending Alerts Through Shared Resources” on page 84.

You can configure up to six separate entries. If you have more than one entry enabled in your name list, the ASM device will sequentially try to connect to each one of them.

Note: A full list of alerts generated by the Advanced System Management PCI Adapter and Advanced System Management Processor can be found in Appendix A, “Advanced System Management Alerts” on page 265.

Dial-Out Fails

You may have a situation where the adapter is configured to dial out to a pager, but the pager does not receive the alert. The solution is to add one or more commas at the end of the telephone number. Each comma will cause a two-second delay from the time that the ASM device completes dialing to the time that the numeric or alphanumeric alert is transmitted.

Reference: RETAIN Tip H163746

The fields in Figure 87 on page 118 are described in the following sections:

4.2.6.1 Remote Alert Entry Information

- Name

  Enter a name that will identify the recipient of that alert. You can also select previously added names and modify them.

- Number

  Enter here the phone number or TCP/IP address that will be used when an event occurs.

- Type

  This is where you select what method will be used to forward the alert:

  1. A numeric pager
  2. An alphanumeric pager
  3. A remote Netfinity Manager system
  4. Another ASM PCI adapter configured for TCP/IP
  5. An SNMP trap to send to an SNMP-enabled management system

- PIN

  If you select **Alphanumeric** 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 entry. If you do not check the box, the entry will not be used to transmit alerts.

- Delete button

  Use the Delete button to erase an entry.

4.2.6.2 Dialout Status

This field displays the present status of the ASM device. The status will be either `DIALOUT OFF` or `DIALOUT ON`. When it is on, the ASM device is currently performing a dial-out function. You can use the **Stop Dialout** button to interrupt a dial-out process. The dial-out status will also change when a TCP/IP or SNMP trap alert is sent.

Note: Examine the Dialout status field after you configure your dial-out entries to see whether the dial-out attempt is successful. The dial-out status displays an attempt to dial out; `DIALOUT ON` will appear even when the ASM device is not connected to a modem.

4.2.6.3 Critical Alerts

These alerts are generated if a system enters a critical status such as a 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 temperature sensors report that the temperature has exceeded the threshold, the ASM device will issue an alert and attempt to shut down the operating system and power off the server.
- Voltage: If the power supplies are outside of their operational ranges, an alert will be issued and an attempt to shut down the operating system and power off the server will be made.
- Tamper: If checked, the ASM device will send an alert when six consecutive login attempts are made using an invalid password.
- Multiple fan failure: If checked, the ASM device will send an alert if two or more of the system's fans fail. The ASM device will attempt to shut down the operating system and power off the server.
- Power failure: An alert will occur if a power supply fails. There are some limitations to the ASM processor and ASM ISA adapter. Both of them rely on a consecutive power supply through the system board. The ASM PCI adapter relies also on the system board’s power supply as long as the optional power supply is not use. With the optional power supply the ASM PCI adapter becomes an independent device even when all system power supplies are broken down.

  The external power supply option for the Advanced Systems Management Adapter is used on servers where it is required and supported (see Table 15 on page 87).

  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 your system has a VRM, the ASM device will dial out if the VRM fails.

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

4.2.6.4 Non-Critical Alerts

The following non-critical alerts are configurable:

- Temperature: If checked, the ASM device 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 ASM device will dial out if any monitored voltage exceeds its 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.

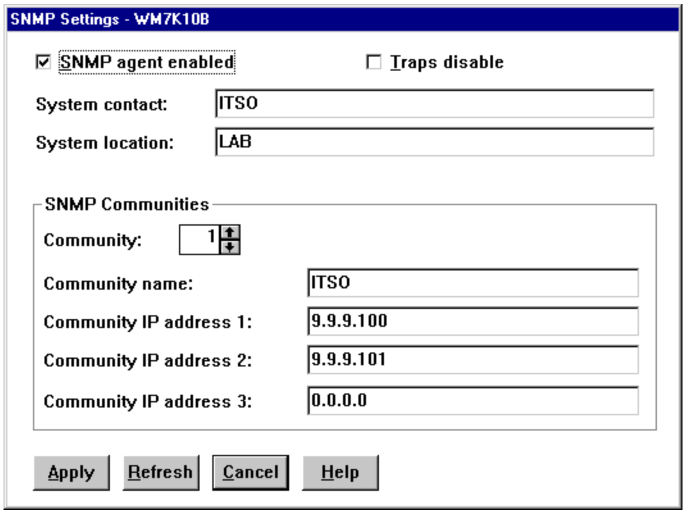
4.2.6.5 System Alerts

The System group enables dial-out events to cover operational faults such as operating system loader (that is, operating system boot) timeout or power on/off events. For how to configure the timeout WatchDog timers, see 4.2.4, “Port and Dialing Settings” on page 112.

- POST timeout: The POST timeout (as configured in 4.2.3.4, “POST Timeout” on page 111) was exceeded.
- Loader timeout: The Loader timeout (as configured in 4.2.3.5, “Loader Timeout” on page 111) was exceeded.
- O/S timeout: The operating system boot timeout (as configured in 4.2.3.6, “O/S Timeout” on page 111) was exceeded.
- Power off: The ASM device will dial out if the server was powered off using the on/off button on the server. Power must still be available to the ASM device 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 15 on page 87) must still have power.
- Power on: The ASM device will dial out when the server is powered on.
- Application: This option, when checked, will cause the ASM device 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 in to the ASM device and examine the event log to see the alert. See 2.4, “Alerts” on page 25 for details about setting up alerts in Netfinity Manager.
- PFA: The ASM device will dial out if it receives a PFA notification from the server. This is available only on systems that have specially architected PFA hardware, such as the Netfinity 5500. It is not available with the Advanced Systems Management Adapter.

4.2.6.6 SNMP

Clicking the SNMP button in Figure 87 on page 118 lets you configure alerts to be sent out using the Simple Network Management Protocol on systems with the ASM PCI adapter installed. If the system has an ASM processor also, then the two ASM devices must be connected together using the dual pigtail cable (see Figure 50 on page 67).



☑ SNMP agent enabled

□ Traps disable

System contact: ITSO

System location: LAB

SNMP Communities

Community: 1

Community name: ITSO

Community IP address 1: 9.9.9.100

Community IP address 2: 9.9.9.101

Community IP address 3: 0.0.0.0

Figure 88. SNMP Configuration Window for the ASM PCI Adapter

The fields in Figure 88 are:

- SNMP agent enabled — check this box if you want the operating system's SNMP agent to forward the alert. SNMP agent enabled works only as long as the operating system is running. Once the operating system shuts down, the ASM PCI adapter will send out the SNMP alerts.
- Traps disable — check this box to prevent SNMP traps from being sent.
- System contact — the name of the SNMP contact person.
- System location — the location of the server.
- Community — use the spin button to select a new community or to create a new entry.
- Community name — enter the community name for this entry.
- Community IP address — you can enter three IP addresses for systems that are SNMP enabled.

After you finish click **Apply** to store the new settings or changes.

4.2.7 Event Log

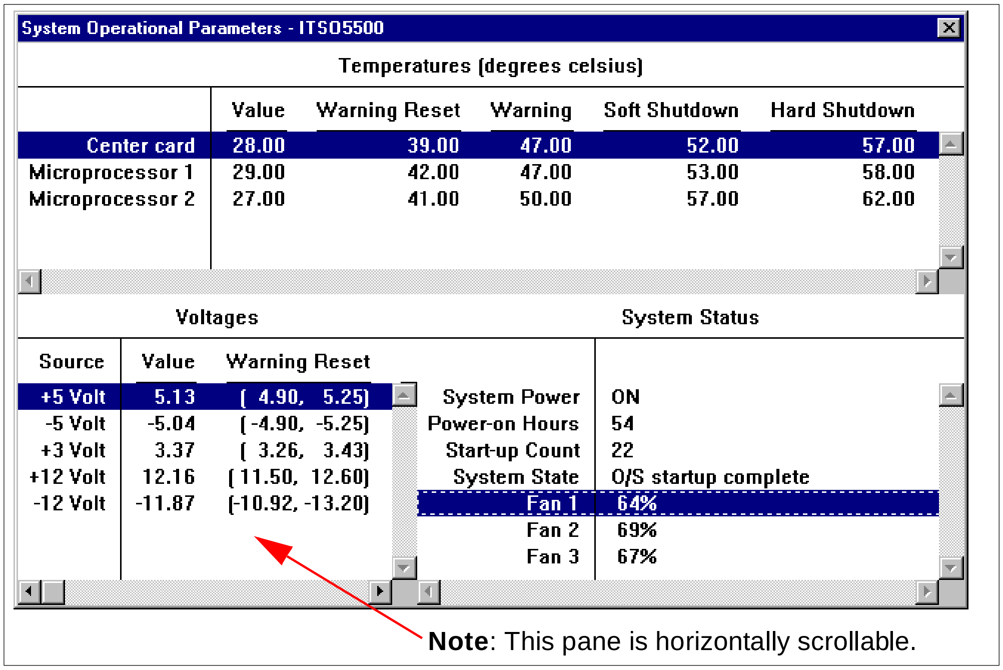
The Event Log window enables you to view the contents of the Service Processor Event Log. Information about all remote access attempts and dial-out events that have occurred are recorded in the Service Processor Event Log.

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

4.2.8 Operational Parameters

The Operational Parameters window shows the current values or status of many system components monitored by the ASM device. The values that are available are dependent upon the hardware configuration of the system. Figure 89 shows the window for the Netfinity 5500.

Note: The voltages pane in Figure 89 is scrollable to the right.



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%

Note: This pane is horizontally scrollable.

Figure 89. ASM Device Operational Parameters on Netfinity 5500

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

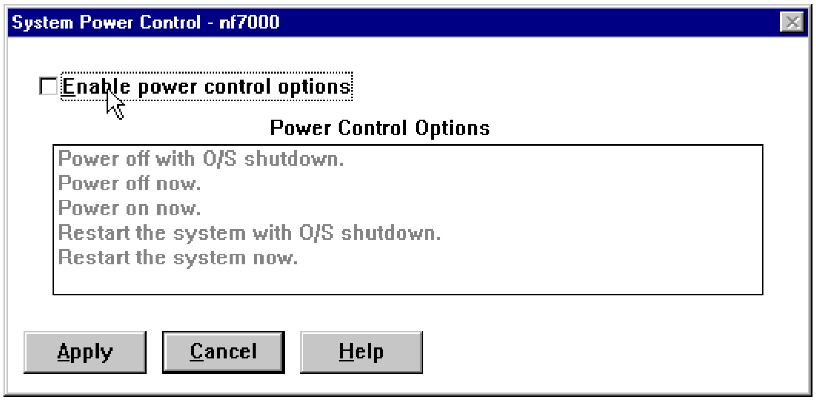
- Current temperatures and threshold levels for the far-end of the adapter card, the center of the adapter card (or near the processor), the microprocessor area and near the microprocessors themselves.
- The status of system fans and blowers, including % speed of maximum.
- Power supply voltages (for +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 Reset: The warning threshold was reached, but the temperature or voltage decreased back to a “normal” operating range.
- Warning: The first temperature/voltage threshold. This corresponds to the non-critical temperature event as defined in 4.2.6.4, “Non-Critical Alerts” on page 120.
- Soft Shutdown: The second threshold where the operating system will be shut down. This corresponds to the critical temperature event as defined in 4.2.6.3, “Critical Alerts” on page 120.
- Hard Shutdown: The server is immediately powered down.

4.2.9 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.

Figure 90. ASM Device System Power Control

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

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

4.2.10 Remote POST Console

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

The Remote POST Console function is supported only on systems with the ASM PCI adapter or ASM processor and with selected systems with the ASM ISA adapter installed. Currently, supported systems are:

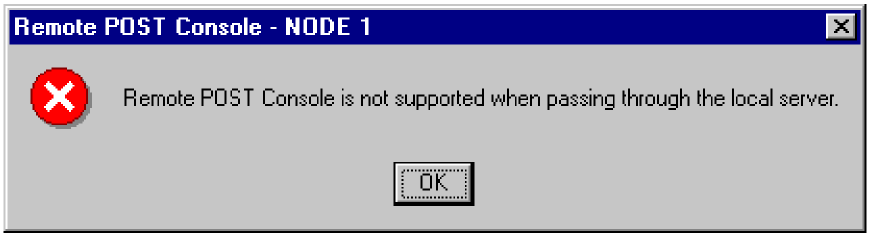
- Netfinity 5000
- Netfinity 5500 family
- Netfinity 7000
- Netfinity 7000 M10
- Server 325/330 with an ASM ISA adapter

Table 22 lists the supported connection methods for Remote POST Console:

Table 22. Remote POST Console Supported Connections

Connection Method	ASM PCI Adapter	ASM Processor	ASM ISA Adapter
Terminal emulator	Supported	Supported	Supported
Dial-up via DCM	Supported	Supported	Supported
Telnet	Supported	Supported[1]	No
TCP/IP via DCM	Supported	Supported[1]	No
RS-485[2]	Supported	Supported[1]	No
Notes: 1 Supported when the ASM processor is connected to an ASM PCI adapter via RS-485. 2 The use of RS-485 is supported only when used in conjunction with serial or TCP/IP connections.			

Note: In Table 22, RS-485 is supported for the ASM PCI adapter and ASM processor. RS-485 is supported only when used in conjunction with TCP/IP or serial connections. The use of RS-485 via Dynamic Connection Manager (DCM) directly from one server to another server is not supported. If you attempt this you will get the following error message:


Remote POST Console - NODE 1

Remote POST Console is not supported when passing through the local server.

Figure 91. Remote POST Console Error

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

1. Connect to the ASM device on the remote system via one of the following:
2. After you are connected, close or minimize the Dynamic Connection Manager and open **Advanced System Management**.
3. Open **Remote POST Console** and leave it open while returning to the ASM device main window.
4. Restart the remote system using the **System Power Control** function.

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 ASM device 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.

Chapter 5. Management Functions in Netfinity Servers

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

- IBM Netfinity 7000 M10
- IBM Netfinity 7000
- IBM Netfinity 5500 M20
- IBM Netfinity 5500 M10
- IBM Netfinity 5500
- IBM Netfinity 5000
- IBM Netfinity 3000

5.1 Netfinity 7000 M10

The IBM Netfinity 7000 M10 server is an advanced, high-throughput, four-way SMP network server using the 400 MHz and faster Intel Pentium II Xeon processors. With new 100 MHz F-16 bus architecture, matched by up to 1 MB of L2 cache and four-way interleaved ECC EDO memory expandable to 8 GB, the Netfinity 7000 M10 server delivers excellent scalability for adding memory and processors.

The Netfinity 7000 M10 server provides exceptional fault-tolerant and high-availability functions integrated within the server as standard features. These standard features include Hot-Plug PCI and redundant hot-plug drives. Additional hard drives, memory and power supplies are optional. IBM Predictive Failure Analysis (PFA) for fans, power supplies, disk drives, memory and processors help your business avoid down time

Advanced manageability and serviceability features can help you control the Netfinity 7000 M10 server and diagnose problems quickly from remote locations, even if your system is down without power. An integrated Advanced System Management PCI Adapter combined with Netfinity Manager software, support remote power-on self-test (POST), in addition to setup and diagnostics via a LAN, a modem or the Web.

5.1.1 Control and Indicators

The controls and indicators on the front of the server are shown in Figure 92 on page 128:

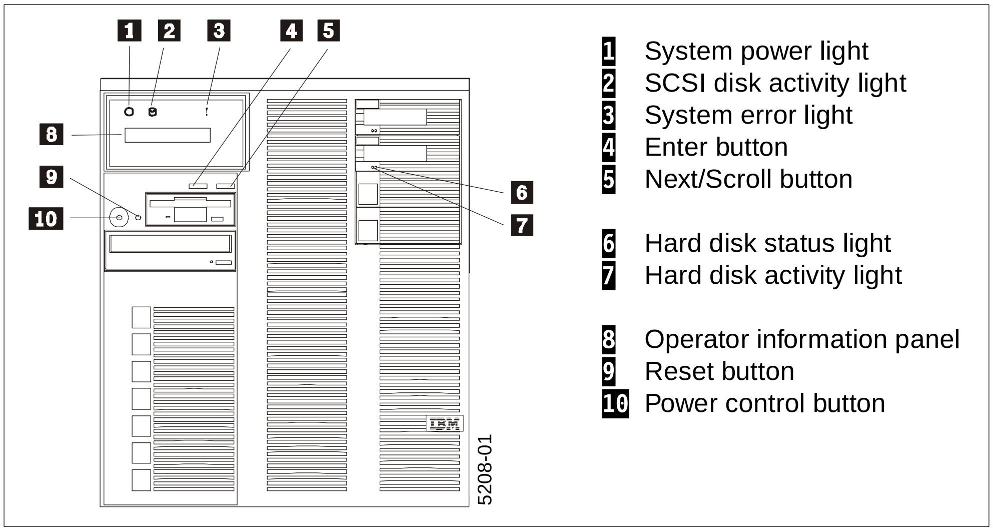


Figure 92. Netfinity 7000 M10 Front View

The system error light (3 in Figure 92) is an amber light and is lit when a system error occurs. When this is lit, the details of the error are displayed on the information panel.

5.1.1.1 Information Panel

The operator information panel (8) on the front of the server provides the following information:

- Checkpoint information during POST
- Boot-up error messages
- Server information

System monitor information appears on this display. The Advanced System Management PCI Adapter monitors system functions and generates these messages as shown in Table 23:

Table 23. System Monitoring Messages

Code	Message	Description
00	Post Fail	Errors were detected that prevented the system from successfully completing POST.
01	Post Warn	Errors detected in POST, but the system can still complete the POST process.
08	App Fail	An application has failed.
09	App Warning	An application has issued a warning message.
10	Boot Fail	The network operating system failed to load.
18	OS Hang	The watchdog timer on the ASM PCI adapter detected that the operating system has stopped responding.
20	Log Full	The ASM PCI adapter’s system error log is full.
80	Over Temp	A monitored temperature is above the normal range.
85	Over Volt	A monitored power source exceeds the threshold value.
86	Under Volt	A monitored power source is below the threshold value.

Code	Message	Description
9x	Power *x*	Power supply failure, where *x* is the power supply identifier.
98	Power Fail	A failure occurred in the power supply system.
A0	Fan *x* Fail	A fan has failed, where *x* is the fan identifier.
B0	Intrusion	The intrusion-detection switches have been set.
B8	Display Fail	The information panel has failed.
C0	SMI Error	A critical error has occurred.
C1	Memory Fail	A double-bit ECC system memory error has occurred.

The server also has a set of press buttons that let you select an action (Next button, 5 in Figure 92 on page 128) and to perform the action (Enter button, 4 in Figure 92) on a system monitoring message. You can select:

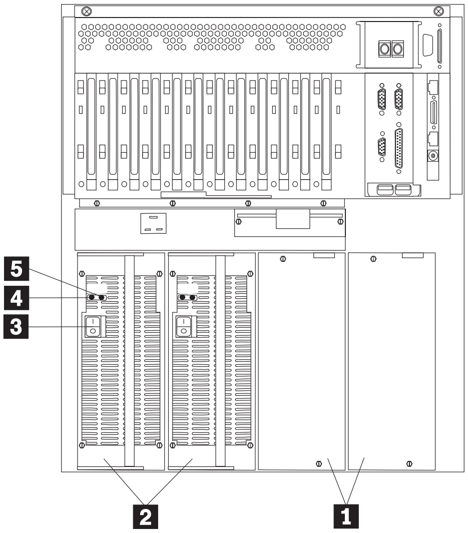
- **Keep** to retain the message on the information panel and leave the system error light (3 in Figure 92) flashing normally.
- **Remind** to retain the message on the information panel and enable the system error light to flash slowly.
- **Clear** to clear the message from the information panel and stop the system error light from flashing.

5.1.1.2 Power Supplies

The Netfinity 7000 M10 ships standard with one or two 400-watt hot-swap power supplies, depending on the model. Up to four power supplies can be installed (using the optional IBM Netfinity 400W Hot-Swap Redundant Power Supply, part 01K7951) can be added to allow the Netfinity 7000 M10 to operate without interruption. The replacement of the failing power unit (easily removed and reinstalled) will be possible without powering down the server.

The system power light (1 in Figure 92 on page 128) indicates the status of system power:

- On: System power is present in the server.
- Flash: The server is in standby mode (the system power supply is turned off and AC current is present).
- Off: Either power supply failure or an AC power failure.



1 Spaces for third and fourth power supplies
2 Hot-swap power supplies (1 on the left, 2 on the right)
3 Power switch for the power supply
4 AC power light (green)
5 DC power light (green)

Figure 93. Netfinity 7000 M10 — Rear View

As shown in Figure 93, there is a DC power and an AC power LED on each power supply indicating its status of the power supply. For normal operation, both of these should be on.

Table 28 lists the status of the power supplies depicted by these LEDs:

Table 24. Power Supply Indicators

AC Power	DC Power	Description and Action
On	On	The power supply is on and operating correctly.
On	Off	There is a DC power problem. Possible causes are: • If the DC power LEDs on all power supplies are off, then it is likely the power control button on the front of the server is not turned on. • If at least one DC power LED is on, then either the power switch on the power supply is in the off position, or the power supply has failed.
Off	Off	There is an AC power problem. Possible causes are: • There is no AC power to the power supply (that is, the power supply is not plugged in to the wall outlet or the outlet is not functioning). • The power supply has failed.

5.1.1.3 Disk Drive Indicators

The SCSI hard disk activity light (2 in Figure 92 on page 128) shows the disk activity of the on-board SCSI controller. In addition, each disk drive has two LEDs:

1. Green activity light (7 in Figure 92 on page 128): When it is lit, the drive is in use.
2. Amber status light:
   - – Off: The drive is OK.
   - – Continuously on: Drive has failed.

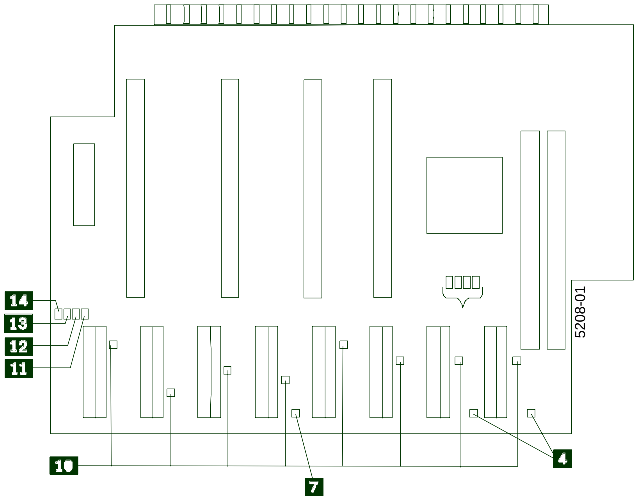
– Slow blink (one flash per second): The drive is being rebuilt.
– Fast blink (three flashes per second): The controller is identifying the drive.

To aid in the detection of heat-related problems in the drive subsystem, the Netfinity 7000 M10 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. (It’s correct.)
2. If the temperature continues to increase and reaches the second threshold, the 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.

5.1.1.4 Indicators on the Planar Boards

The Netfinity 7000 M10 has LEDs on the processor board, I/O board and memory board; the indicators are lit during POST to ensure the indicators operate. After POST completes, the indicators show the status of components.



LEDs on the Processor Board:

4 ERR 0 and ERR 1
7 CPU termination
10 VRM
11 Bus activity for CPU 4
12 Bus activity for CPU 3
13 Bus activity for CPU 2
14 Bus activity for CPU 1

Figure 94. 7000 M10 Processor Board Indicators

The LEDs perform the functions described in Table 25:

Table 25. Status Indicators on Processor Board

Indicator	Description
Microprocessor Bus Activity LED	If activity on the microprocessor bus is present, the indicator for the slot is lit.
Microprocessor VRM Status LED	If a microprocessor voltage regulator module (VRM) is present and has failed, the indicator for the slot is lit.
Microprocessor Termination LED	If proper termination of the microprocessor slots is present, the indicator is lit.

Indicator	Description
ERR 0 and ERR 1 LED	Reserved.

Note: Other components on the processor board are described in “Processor Board Component Locations” in Chapter 7 of *Netfinity 7000 M10 Hardware Information*.

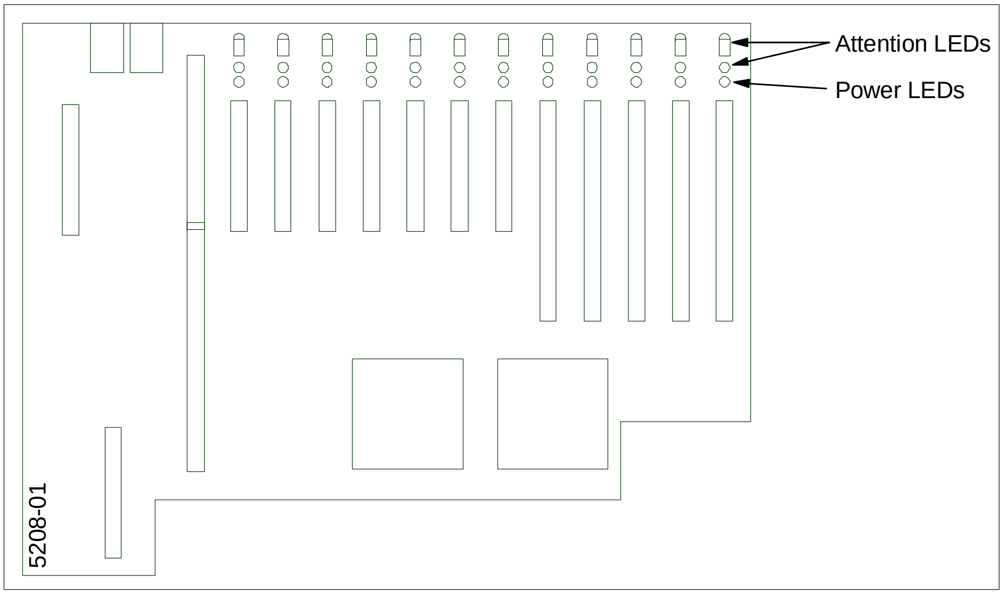


Figure 95. 7000 M10 I/O Board Indicators

As shown in Figure 95, each PCI slot has three lights, two attention LEDs and one power LED. The power LED indicates the PCI slot is active and has power. Do not add or remove an adapter from the PCI slot when its power LED is lit.

Each PCI slot has two attention LEDs showing identical status: one that is visible from the rear of the server and one that is visible from inside the server. The attention LEDs are controlled by the operating system and are meant to warn you about the status of that particular slot.

Note: Other components on the I/O board are described in “I/O Board Component Locations” in Chapter 7 of *Netfinity 7000 M10 Hardware Information*.

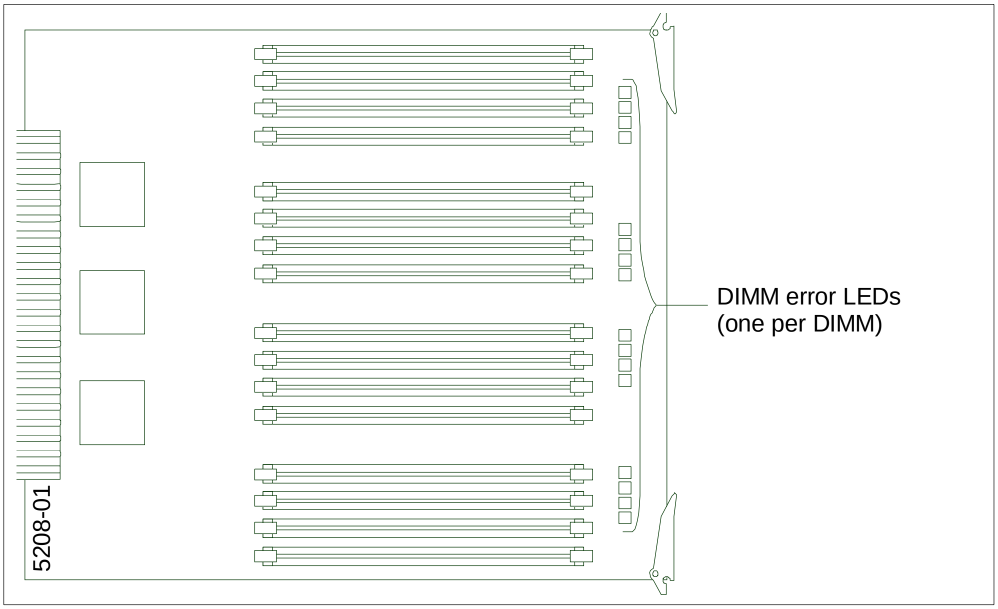


Figure 96. 7000 M10 Memory Board Indicators

If any DIMM has failed, the corresponding LED will light signaling the failed component.

Note: Other components on the memory board are described in “Memory Board Component Locations” in Chapter 7 of *Netfinity 7000 M10 Hardware Information*.

5.1.2 Advanced System Management PCI Adapter

The Netfinity 7000 M10 is shipped with the Advanced System Management PCI Adapter. With this adapter, in conjunction with Netfinity Manager, you can locally and remotely configure and monitor many features of your server. You can configure system-management events (such as POST, OS loader, and operating system timeout values and critical temperature, voltage, and tamper alerts). If any of these events occurs, the Advanced System Management PCI Adapter can forward an alert to other resources:

- Another Netfinity Manager or other service-processor interface, through an Ethernet or token-ring network or serial connection
- A standard numeric pager
- An alphanumeric pager

You can dial out and directly access and control a remote Advanced System Management PCI Adapter. In addition, you can remotely monitor, record, and replay all textual data generated during POST on a remote server with the adapter. While monitoring a remote system during POST, you can enter keyboard commands that will be relayed to the remote system.

Note: The Advanced System Management PCI Adapter is sometimes referred to generically as the service processor.

Table 26. Advanced System Management PCI Adapter LEDs

Indicator	Description
Power On LED	If power to the Advanced System Management PCI Adapter is present, the indictor is lit.
Processor Error LED	If the processor on the Advanced System Management PCI Adapter has failed, the indicator is lit.
Ethernet Activity LED	If the Ethernet controller on the Advanced System Management PCI Adapter is transmitting data, the indicator is lit.
Ethernet Link LED	If an active link to the Ethernet controller on the Advanced System Management PCI Adapter is present, the indicator is lit.

5.1.3 COM Ports

The Netfinity 7000 M10 has four COM ports. Their use is shown in Table 30.

Table 27. COM Ports on the Netfinity 7000 M10

Physical ports (as labeled)	A	B	Modem	COM/AUX
Ports available to ASM	N/A	N/A	Port 1 Shared	Port 2 dedicated
Dedicated ports available to OS	COM 1	COM 2	COM 3 shared[1]	N/A
1 The ASM device driver must be running for the operating system to see COM3. N/A means Not Available.				

5.2 IBM Netfinity 7000

The IBM Netfinity 7000 is a highly reliable enterprise server offering four-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.

5.2.1 Status Indicators

The Netfinity 7000 server information panel is on the front of the server as shown in Figure 97. It provides information about the status of the machine.

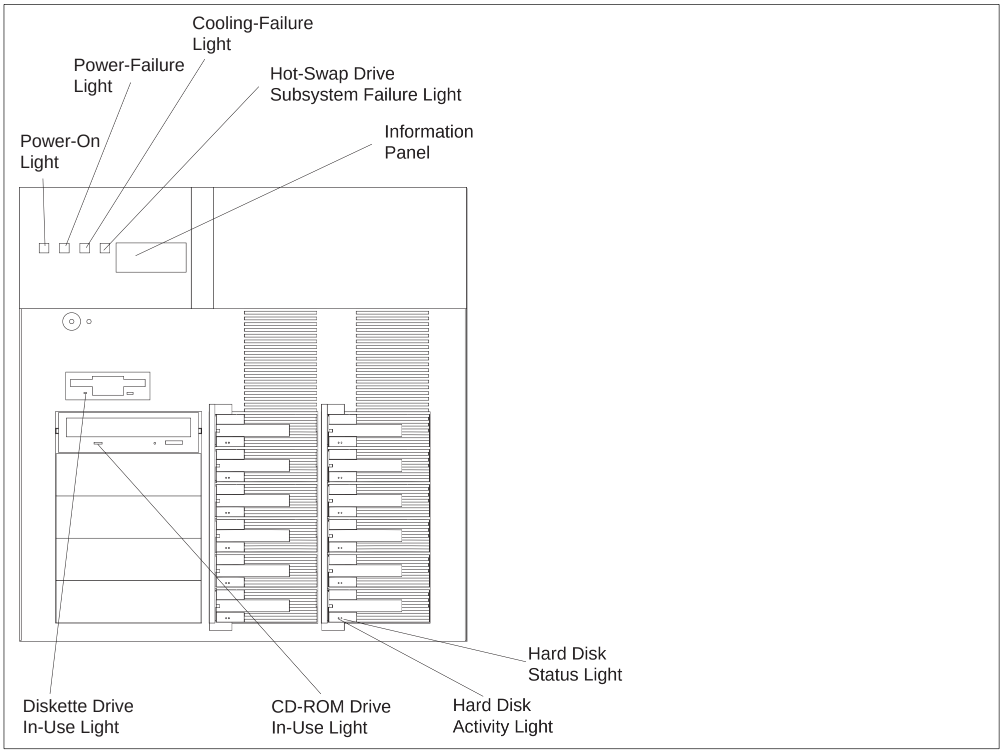


Figure 97. Netfinity 7000 Front View

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.

5.2.1.1 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 (part number 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 reinstalled) 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 97 and Figure 98.

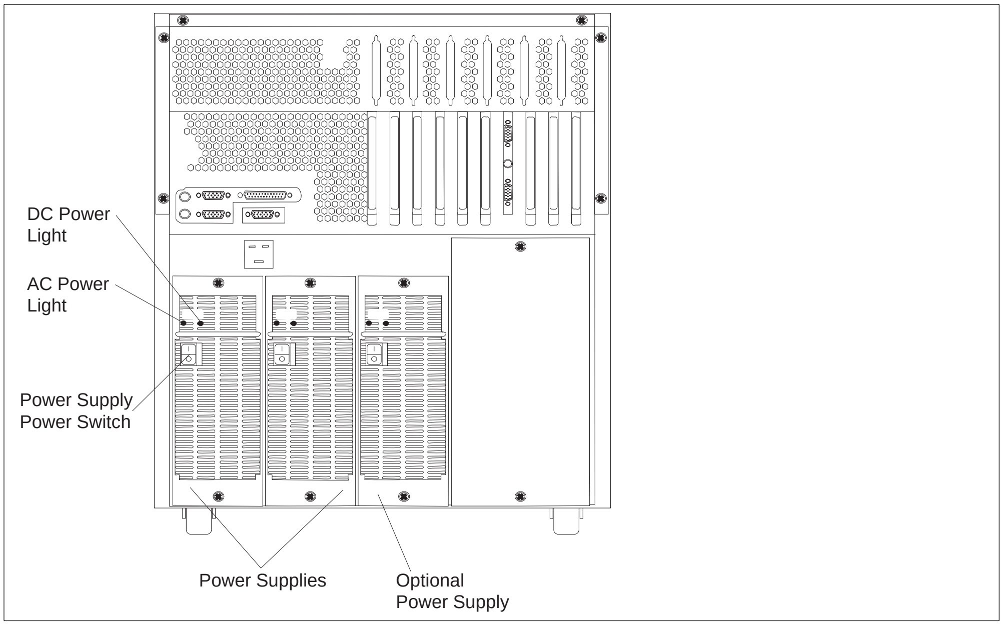


Figure 98. Netfinity 7000 Rear View

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

Table 28. 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 are 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.
on	blinking	on	1+ on	The power supply with the DC Power Good light off has either 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.				

5.2.1.2 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 97 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, the 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 shut down 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.

5.2.1.3 Hot-Swap Drive Indicators

To show the status of the hot-swap drive subsystem, the Netfinity 7000 has an 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 97:

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

5.2.2 Advanced Systems Management Adapter

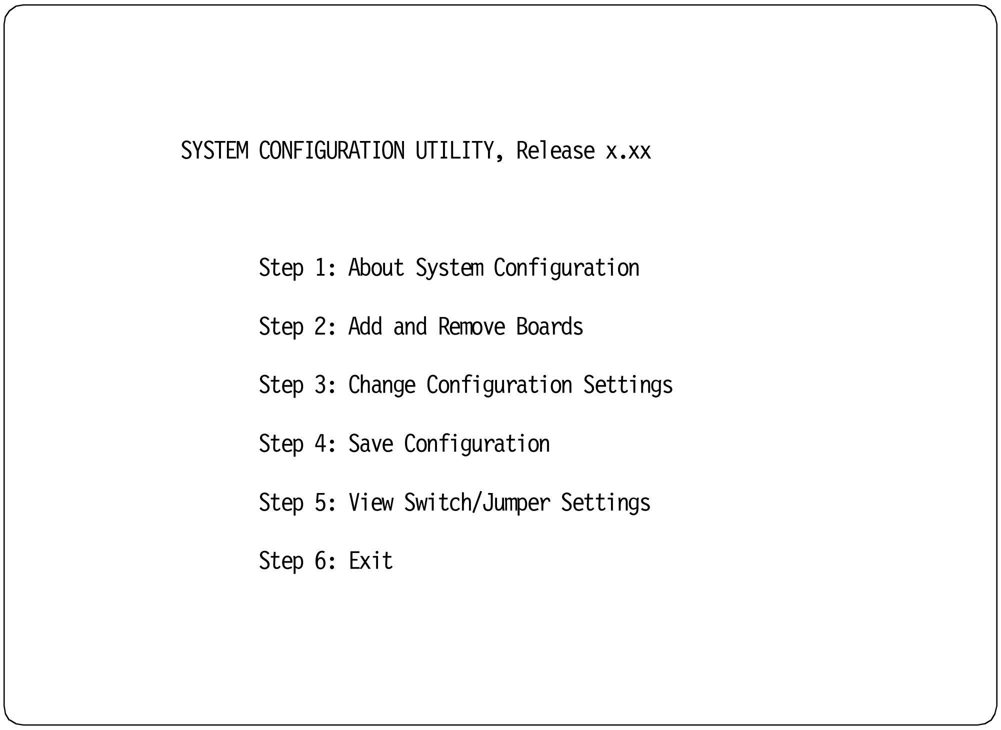
The Netfinity 7000 is shipped with an Advanced Systems Management Adapter installed. This ISA adapter, in conjunction with Netfinity Manager, allows you to manage the functions of the server remotely through a modem. It also provides system monitoring, event recording, and dial-out alert capability.

The ASM ISA adapter comes completely installed and configured. You should change only the default parameters if conflicts arise with other adapters you install.

The following resources are assigned by default:

- IRQ 5
- I/O Address 200

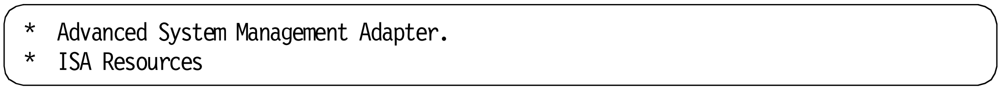
You can check the setting by running the System Configuration Utility (SCU). To start the SCU insert the Netfinity 7000 CD-ROM (or diskette if you download a later version) and reboot the server. You will see a menu with several choices:



```
           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
```

Figure 99. 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. Highlight **Advanced Systems Management Adapter** and press Enter. The following window appears:



```
*  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 System Management Hardware” on page 63.

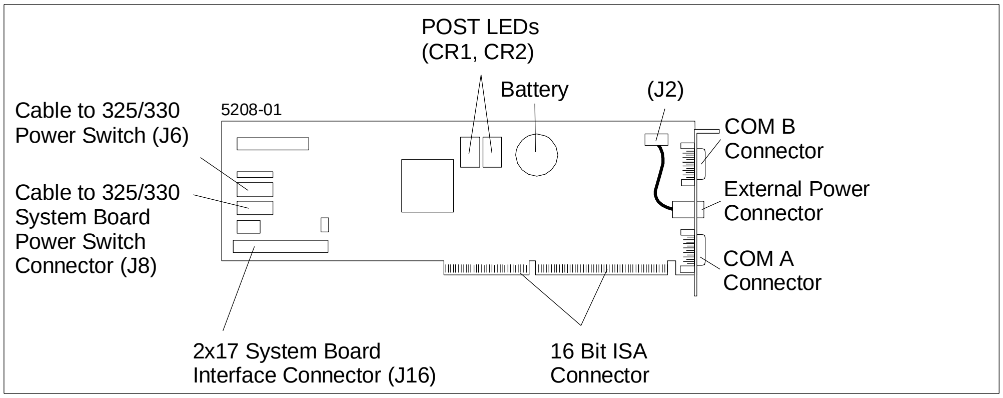


Figure 100. Advanced Systems Management Adapter

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.

5.3 IBM Netfinity 5500 Server Family

The Netfinity 5500 server family comprises IBM's mid-range servers that provides significant levels of performance, fault-tolerance and integrated management capability. There are three members of the 5500 family:

- Netfinity 5500
- Netfinity 5500 M10
- Netfinity 5500 M20

Each is available in a tower or rack chassis form factors.

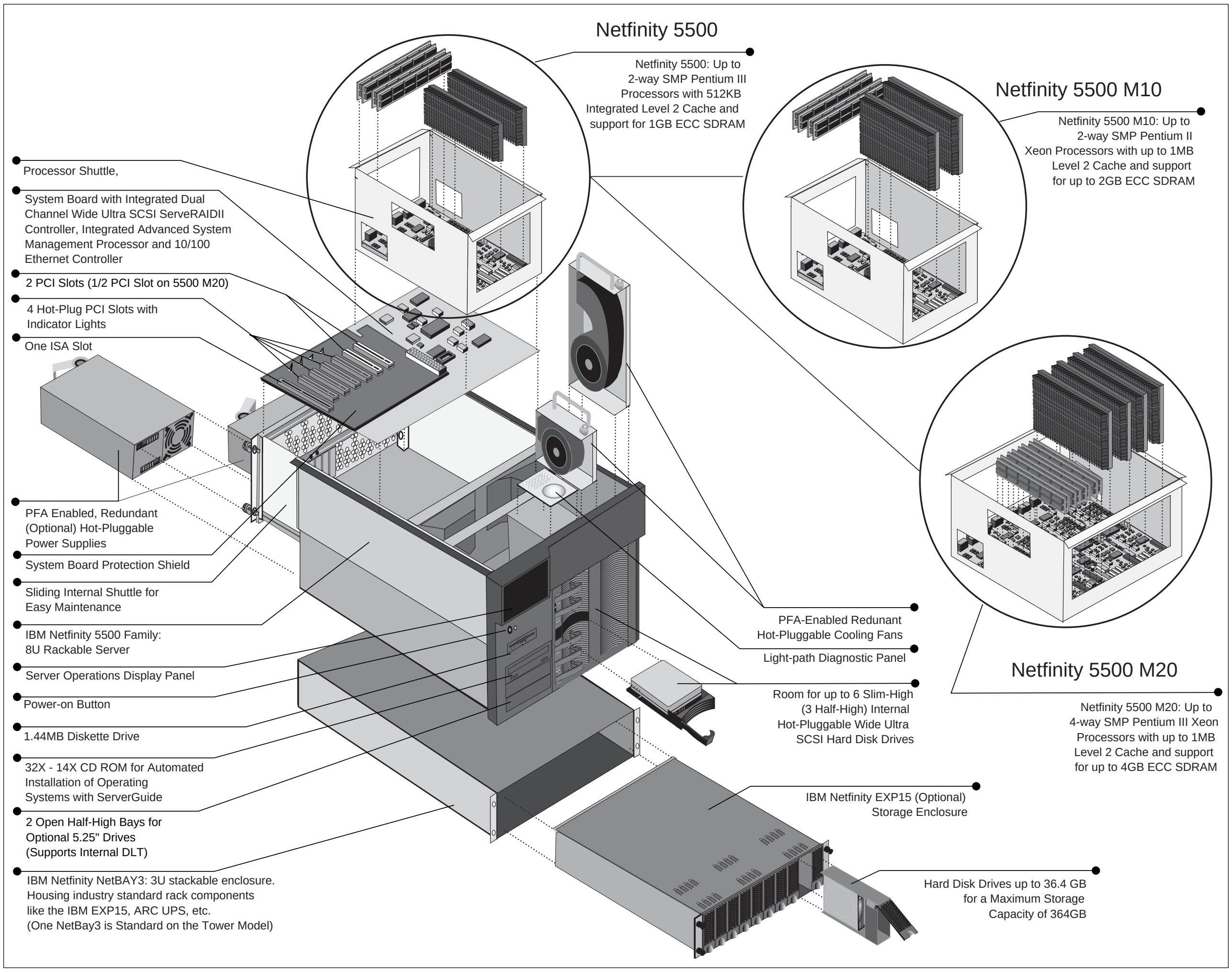

Netfinity 5500
Netfinity 5500: Up to 2-way SMP Pentium III Processors with 512KB Integrated Level 2 Cache and support for 1GB ECC SDRAM
Netfinity 5500 M10
Netfinity 5500 M10: Up to 2-way SMP Pentium II Xeon Processors with up to 1MB Level 2 Cache and support for up to 2GB ECC SDRAM
Processor Shuttle,
System Board with Integrated Dual Channel Wide Ultra SCSI ServeRAIDII Controller, Integrated Advanced System Management Processor and 10/100 Ethernet Controller
2 PCI Slots (1/2 PCI Slot on 5500 M20)
4 Hot-Plug PCI Slots with Indicator Lights
One ISA Slot
PFA Enabled, Redundant (Optional) Hot-Pluggable Power Supplies
System Board Protection Shield
Sliding Internal Shuttle for Easy Maintenance
IBM Netfinity 5500 Family: 8U Rackable Server
Server Operations Display Panel
Power-on Button
1.44MB Diskette Drive
32X - 14X CD ROM for Automated Installation of Operating Systems with ServerGuide
2 Open Half-High Bays for Optional 5.25" Drives (Supports Internal DLT)
IBM Netfinity NetBAY3: 3U stackable enclosure. Housing industry standard rack components like the IBM EXP15, ARC UPS, etc. (One NetBay3 is Standard on the Tower Model)
PFA-Enabled Redunant Hot-Pluggable Cooling Fans
Light-path Diagnostic Panel
Room for up to 6 Slim-High (3 Half-High) Internal Hot-Pluggable Wide Ultra SCSI Hard Disk Drives
Netfinity 5500 M20
Netfinity 5500 M20: Up to 4-way SMP Pentium III Xeon Processors with up to 1MB Level 2 Cache and support for up to 4GB ECC SDRAM
IBM Netfinity EXP15 (Optional) Storage Enclosure
Hard Disk Drives up to 36.4 GB for a Maximum Storage Capacity of 364GB

Figure 101. The IBM Netfinity 5500 M20

At the time of writing, the following models were available (Table 29):

Table 29. Supported CPUs in Netfinity 5500 Family

Pentium II Processors	5500	5500 M10	5500 M20
350 MHz 512 KB L2	yes		
400 MHz 512 KB L2	yes		
450 MHz 512 KB L2	yes		
500 512 KB L2	yes		
400 MHz Xeon 512KB/ 1 MB L2		yes	yes
450 MHz Xeon 512KB/ 1 MB L2		yes	yes
500 MHz Xeon 512KB/ 1 MB L2		yes	yes

All systems support 100 MHz accessible SDRAM memory; 128 MB ECC DIMMs are standard, with the following DIMMs supported:

- Netfinity 5500: up to 1 GB using 128 MB and 256 MB DIMMs
- Netfinity 5500 M10: up to 2 GB using 128 MB, 256 MB or 512 MB DIMMs
- Netfinity 5500 M20: up to 4 GB using 128 MB, 256 MB or 512 MB DIMMs

Each system in the Netfinity 5500 family has an integrated two-channel Ultra SCSI ServeRAID II RAID controller with six internal hot-swap bays. The tower models also include the NetBAY3 which lets you install options such as the Netfinity EXP15 internally, to provide an additional 10 hot-swap storage bays.

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

- Single CPU failure recovery with two or more (Netfinity 5500 M20) 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 5.3.1.3, “Locating Failures” on page 145;
- 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 Netfinity Advanced Remote Management processor. This integrated subsystem is based on a PowerPC RISC processor and communicates to all other subsystems through five separate I^2C busses. The Advanced Remote Management is described in 3.2, “Advanced System Management Processor” on page 73.

5.3.1 Indicators

The front of the server has a variety of indicators and controls as shown in Figure 102:

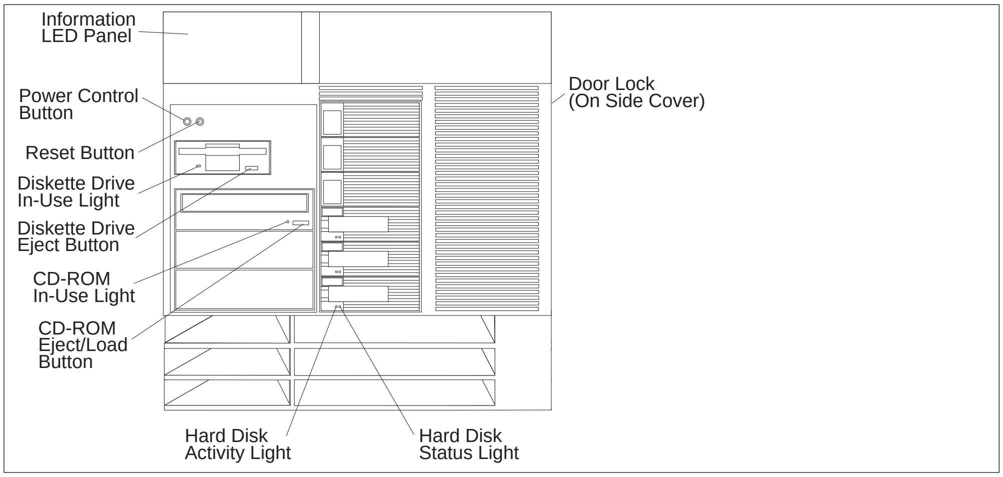


Figure 102. Netfinity 5500 Front Panel

5.3.1.1 Information LED Panel

The Information LED panel at the top-left corner of the front panel provides information about the current status of the server and is also the first place to look when hardware failures occur. The various components of the panel are shown in Figure 103:

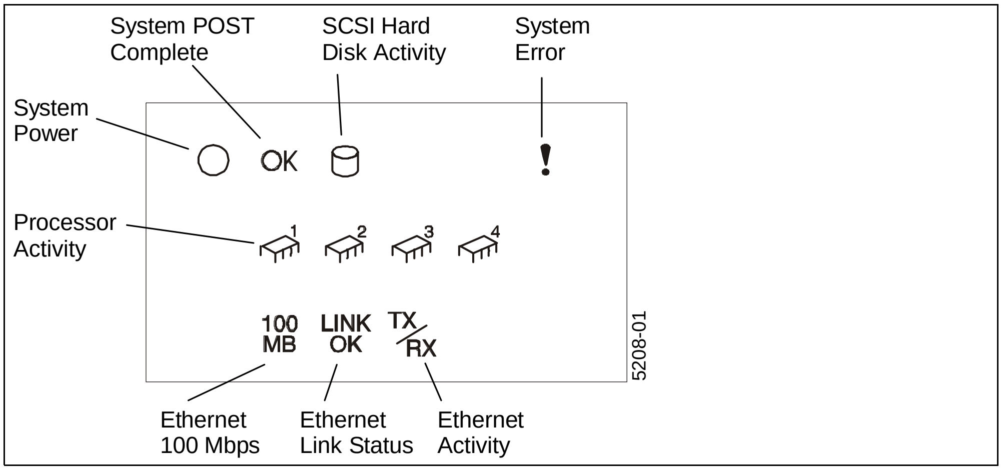


Figure 103. Netfinity 5500 Information LED Panel

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 occurred in the power supply, wall socket, 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 occurred. Remove the top cover of the server and examine the diagnostics LED panel to determine the cause of the error. See 5.3.1.3, “Locating Failures” on page 145.

5.3.1.2 Planar Boards

The Netfinity 5500 family has a system board, a processor board and with the M20, a memory board. Each of these have indicators on them showing the status of various components in the server.

Figure 104 shows LEDs on the Netfinity 5500 system board:

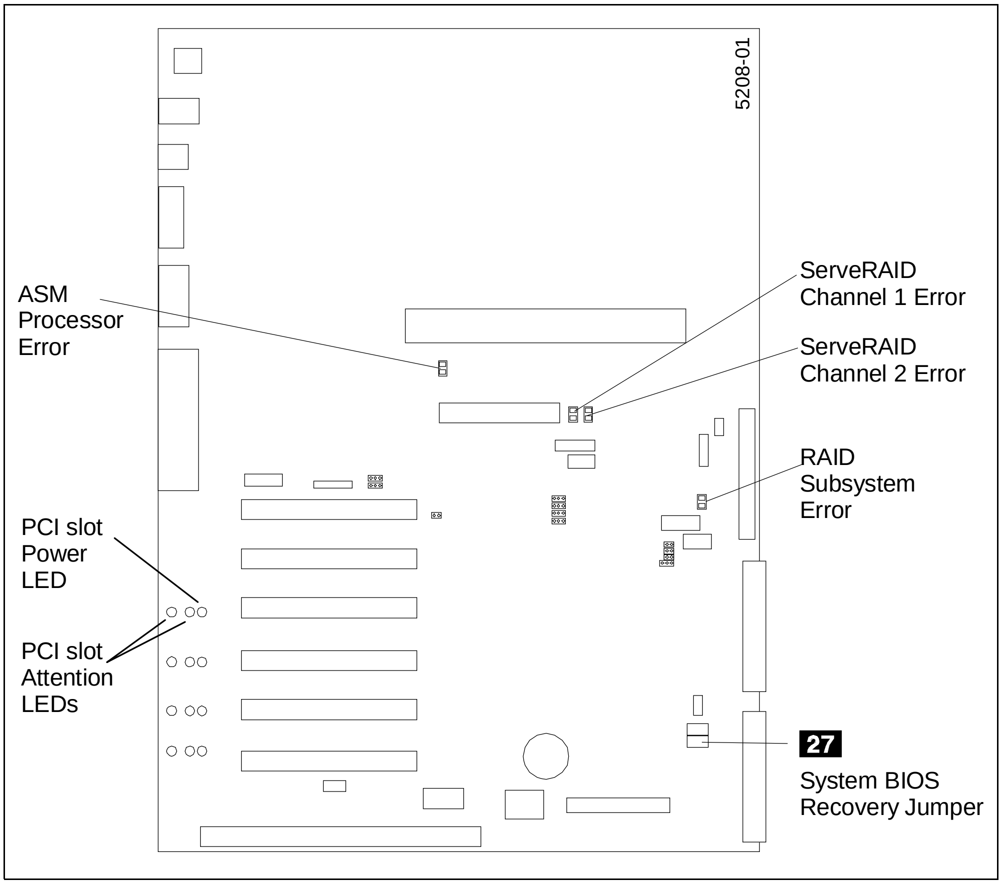


Figure 104. Netfinity 5500 System Board

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 7.8, “Example 8: Remote Update of Netfinity 5500 BIOS” on page 239.

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

The processor board for the Netfinity 5500 and Netfinity 5500 M10 is shown in Figure 105 on page 144. The processor board for the Netfinity 5500 M20 is shown in Figure 106 on page 144.

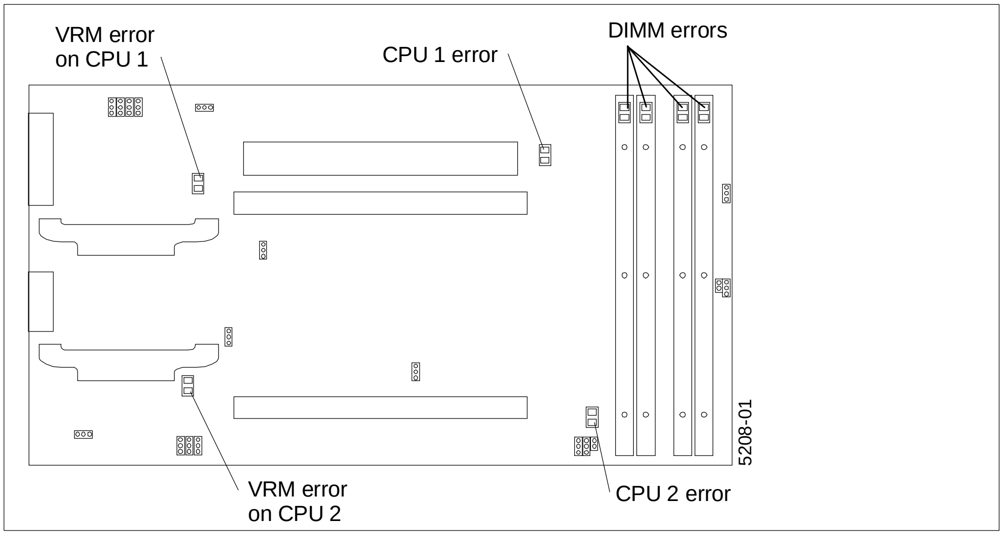


Figure 105. Netfinity 5500/5500 M10 Processor Board

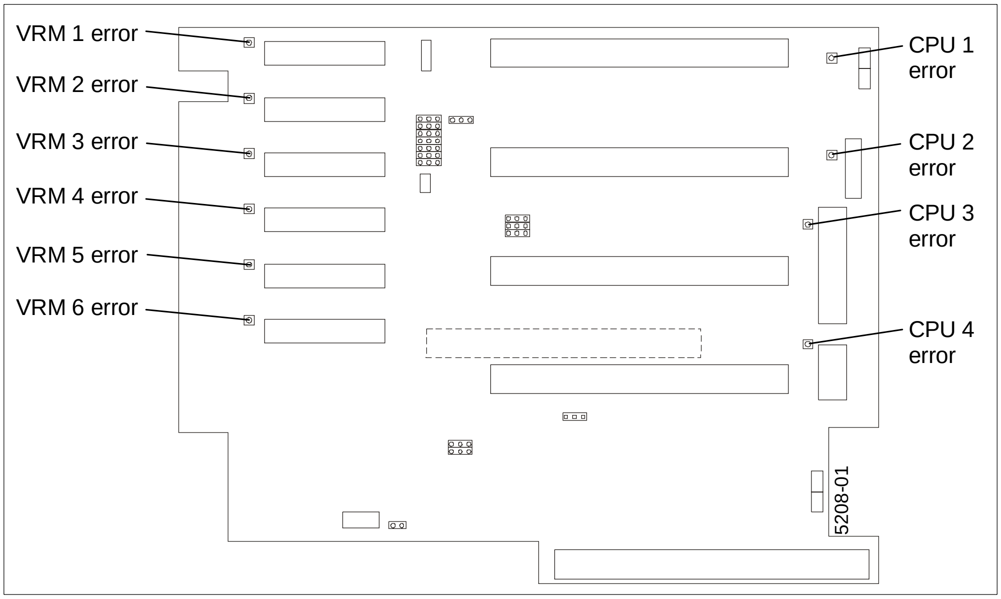


Figure 106. Netfinity 5500 M20 Processor Board

The memory modules are installed on the processor board in the Netfinity 5500 and Netfinity 5500 M10. On the Netfinity 5500 M20, the memory is installed on a separate board as shown in Figure 107 on page 145.

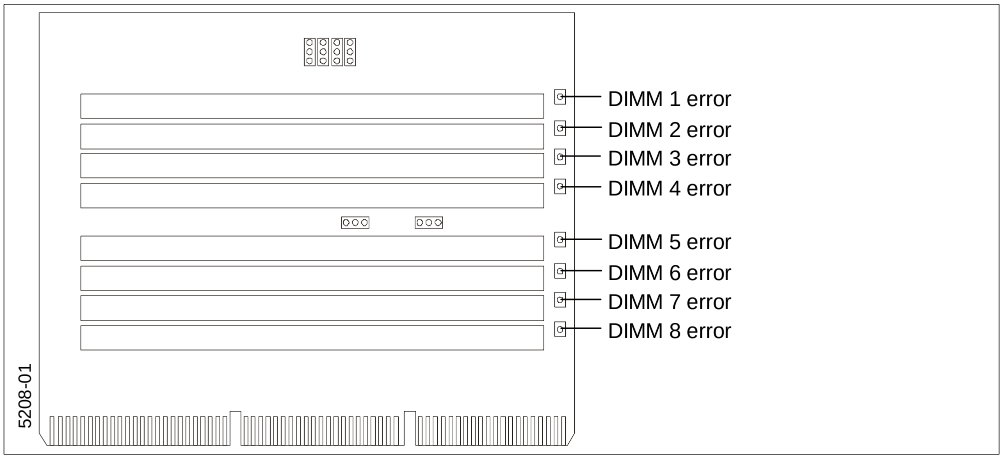


Figure 107. Netfinity 5500 M20 Memory Board

5.3.1.3 Locating Failures

The Netfinity 5500 family of servers 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 108:

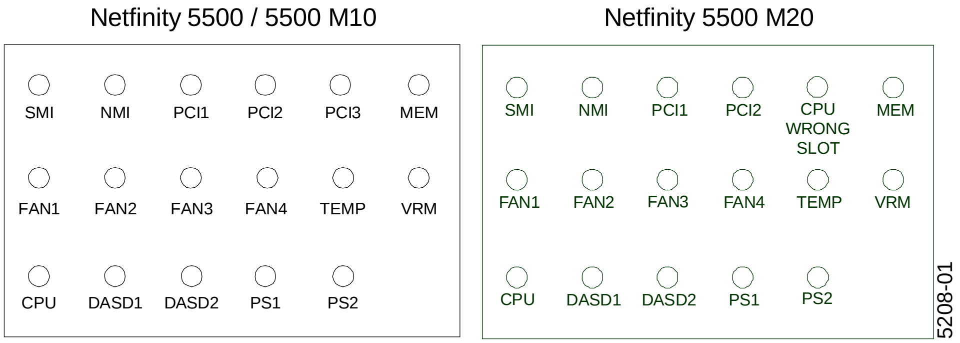


Figure 108. Netfinity 5500 Diagnostics LED Panels

The LEDs on this panel are:

SMI System Management failure
NMI Non-maskable Interrupt failure
PCI1 Failure on the primary PCI bus (bus 0, slots 5-6)
PCI2 Failure on the secondary PCI bus (bus 1, slots 1-4)
CPU WRONG SLOT The combination of microprocessors and terminators installed in the server is not valid
MEM Memory failure; check LEDs near each DIMM on the processor board
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
FAN4 Fan 4 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
CPU A CPU has failed; check the LEDs near each CPU on the processor board
DASD1 A hot-swap hard disk drive has failed on SCSI RAID channel 1
DASD2 A hot-swap hard disk drive has failed on SCSI RAID channel 2
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*.

5.3.2 COM Ports

The Netfinity 5500 family has three COM ports. Their use is shown in Table 30.

Table 30. COM Ports on Netfinity 5500 Family

Physical ports (as labeled)	A	B	C (Management)
Ports available to ASM processor	Port 1 shared	Not available	Port 2 dedicated
Ports available to OS	COM 1 shared	COM 2	Not available

For information on available COM ports when an ASM PCI adapter is installed in the Netfinity 5500, see 3.3.5, “COM Ports” on page 79.

5.4 IBM Netfinity 5000

The IBM Netfinity 5000 closes the gap between the Netfinity 5500 family and the Netfinity 3500. The Netfinity 5000 is designed for small business or workgroup/department solutions.

It comes standard with 64 MB expandable to 1GB 100 MHz ECC SDRAM using four DIMMs. The system supports up to two Pentium III 500 MHz processors.

The new design and mechanics make this server easy to maintain and service. New features include screwless integrated fans, a shuttle for planar and a screwless mechanism for easy removal of the front cover. For detailed information see *Netfinity 5000 Server Hardware Information and Procedures* which ships with your server.

The Netfinity 5000, like the 5500 family, is equipped with an Advanced System Management Processor providing status, control and error information as well as management functions such as remote configuration and remote access.

Key to the server’s fault tolerance and recovery is an integrated Netfinity Advanced System Management processor, which allows diagnostic, reset, POST, and auto recovery functions from remote locations and the monitoring of temperature, voltage, and fan speed.

Other high-availability and serviceability features include:

- Five hot-swap disk drive bays supporting SAF-TE functions.
- A dual-channel Adaptec 7895 controller with support for the ServeRAID Ultra2 SCSI adapters.

- ECC DIMMs combined with an integrated ECC memory controller correcting soft and hard single-bit memory errors.
- Memory hardware scrubbing correcting soft memory errors automatically without software intervention.
- ECC L2 cache processors.
- Predictive failure analysis (PFA) on HDD options, memory, processors, VRMs, and fans.
- A 350-watt power supply with auto restart and built-in redundancy. An optional Netfinity 175 W Redundant Power Supply delivering uninterrupted service for configurations requiring full 350-watt redundancy.
- Information LED panel giving visual indications of system well-being.
- Light Path Diagnostics providing an LED map to a failing component reducing down time and service costs.
- Easy access to system board, adapter cards, processor, and memory.
- CPU failure recovery in SMP configurations allowing:
  - Failed processor to be forced offline
  - Server automatically rebooted
  - Alerts to be generated
  - Operation to be continued with the working processor

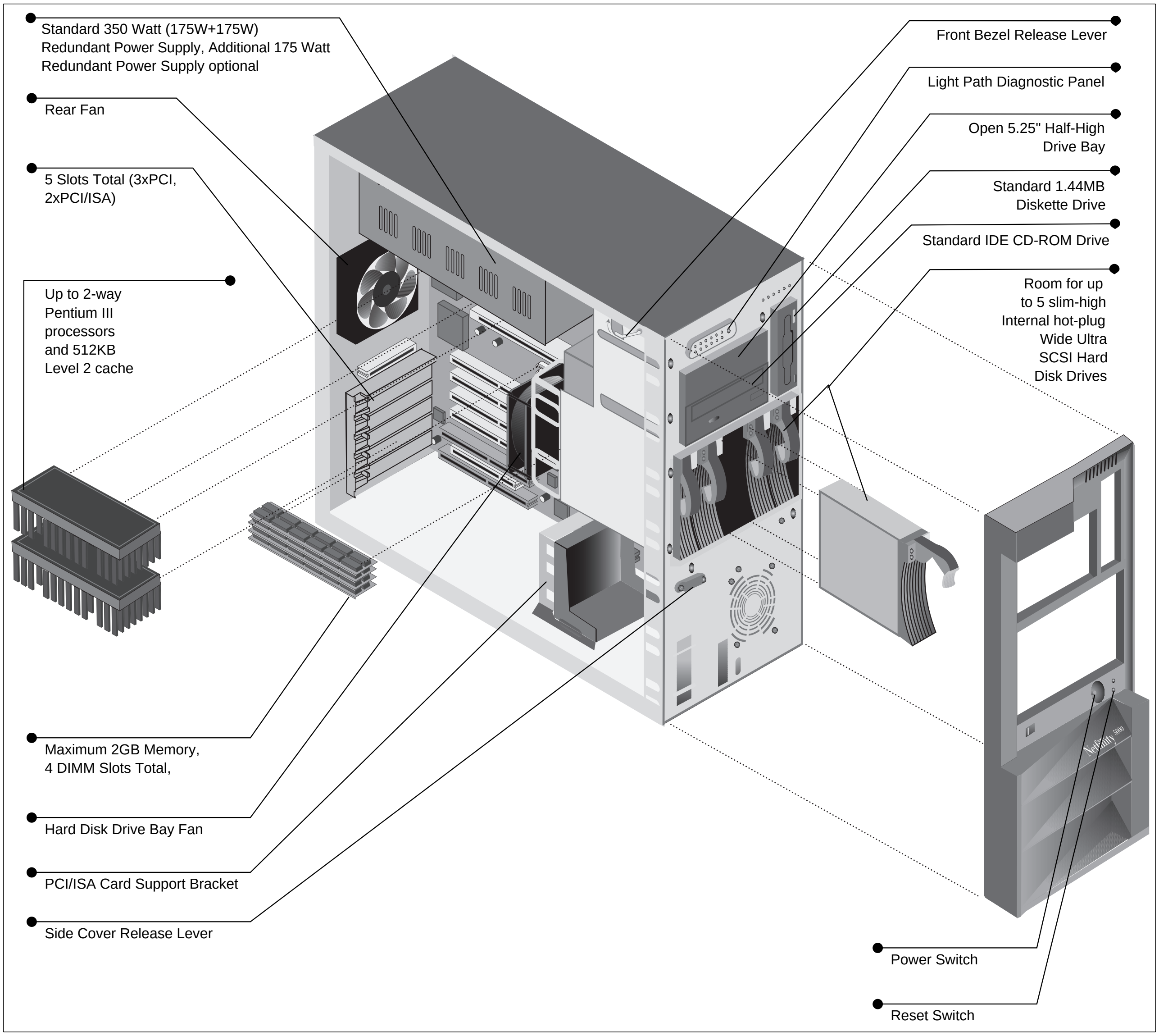
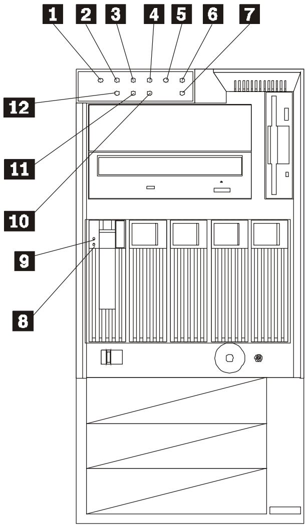

Standard 350 Watt (175W+175W) Redundant Power Supply, Additional 175 Watt Redundant Power Supply optional
Rear Fan
5 Slots Total (3xPCI, 2xPCI/ISA)
Up to 2-way Pentium III processors and 512KB Level 2 cache
Maximum 2GB Memory, 4 DIMM Slots Total,
Hard Disk Drive Bay Fan
PCI/ISA Card Support Bracket
Side Cover Release Lever
Front Bezel Release Lever
Light Path Diagnostic Panel
Open 5.25" Half-High Drive Bay
Standard 1.44MB Diskette Drive
Standard IDE CD-ROM Drive
Room for up to 5 slim-high Internal hot-plug Wide Ultra SCSI Hard Disk Drives
Power Switch
Reset Switch
Netfinity 5000

Figure 109. Netfinity 5000

The Netfinity 5000 is available as a tower or a rack model, and conversion kits are available to convert from one form to the other.

5.4.1 Indicators

The front of the Netfinity 5000 has various indicators and LEDs as shown in Figure 110:



Netfinity 5000 Status Indicators

1	Power-on
2	POST Complete
3	SCSI Disk Drive In Use
4	CPU 1 Activity
5	CPU 2 Activity
6	System Error
7	Reserved
8	Disk Drive Status
9	Disk Drive Activity
10	Ethernet Activity
11	Ethernet Link Status
12	Ethernet 100 Mbps Speed

Figure 110. Status Indicators

For more information about the LEDs see *Netfinity 5000 Server Hardware Information and Procedures*.

5.4.1.1 System Board LEDs

Figure 111 shows the location of some of the LEDs for components controlled by the ASM processor.

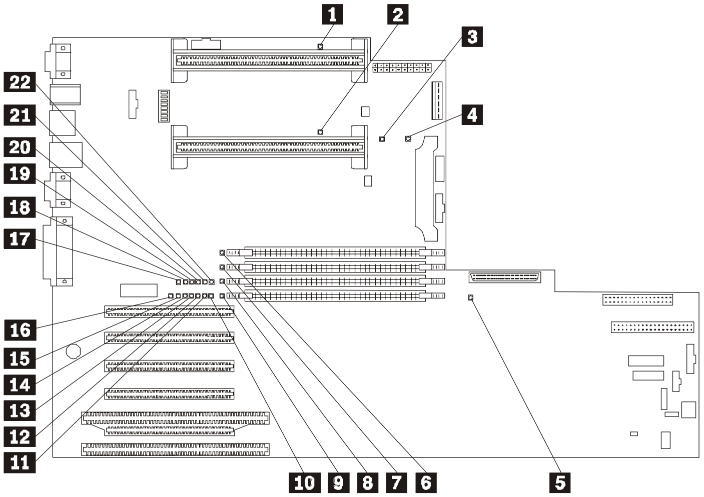


Figure 111. Netfinity 5000 System Board LEDs

1. Microprocessor 1 error LED
2. Microprocessor 2 error LED
3. Integrated voltage regulator error LED
4. Voltage regulator module (VRM) error LED
5. Service Processor error LED
6. DIMM 1 error LED
7. DIMM 2 error LED
8. DIMM 3 error LED
9. DIMM 4 error LED

10. System management interrupt (SMI) LED
11. Non-maskable interrupt (NMI) error LED
12. PCI bus 1 error LED
13. PCI bus 0 error LED
14. Reserved
15. DASD error LED
16. Temperature error LED
17. Fan 1 (DASD) error LED
18. Fan 2 (rear) error LED
19. Reserved
20. Reserved
21. Power supply 1 error LED
22. Power supply 2 error LED

If the System Error LED (or any other LED for that matter) is lit, proceed with steps as described in Chapter 6 “Solving Programs”, *Netfinity 5000 Server Hardware Information and Procedures*.

5.4.2 COM Ports

The Netfinity 5000 has three COM ports. Their use is shown in Table 30.

Table 31. COM Ports on Netfinity 5000

Physical ports (as labeled)	**A**	**B**	**C (Management)**
Ports available to ASM processor	Port 1 shared	Not available	Port 2 dedicated
Ports available to OS	COM 1 shared	COM 2	Not available

For information on available COM ports when an ASM PCI adapter is installed in the Netfinity 5000, see 3.3.5, “COM Ports” on page 79.

5.5 IBM Netfinity 3000

The IBM Netfinity 3000 models are designed for small to medium sized businesses that require a server for their e-business needs. They are at home as a file and print server or as an entry level application server.

Current models are powered by single 500 MHz Pentium III processors. The systems offer 512 KB of integrated Level 2 ECC cache; 64 MB of high-speed, 100 MHz SDRAM 72-bit ECC system memory is standard and is upgradable to 768 MB.

Figure 112 shows an exploded view of the Netfinity 3000:

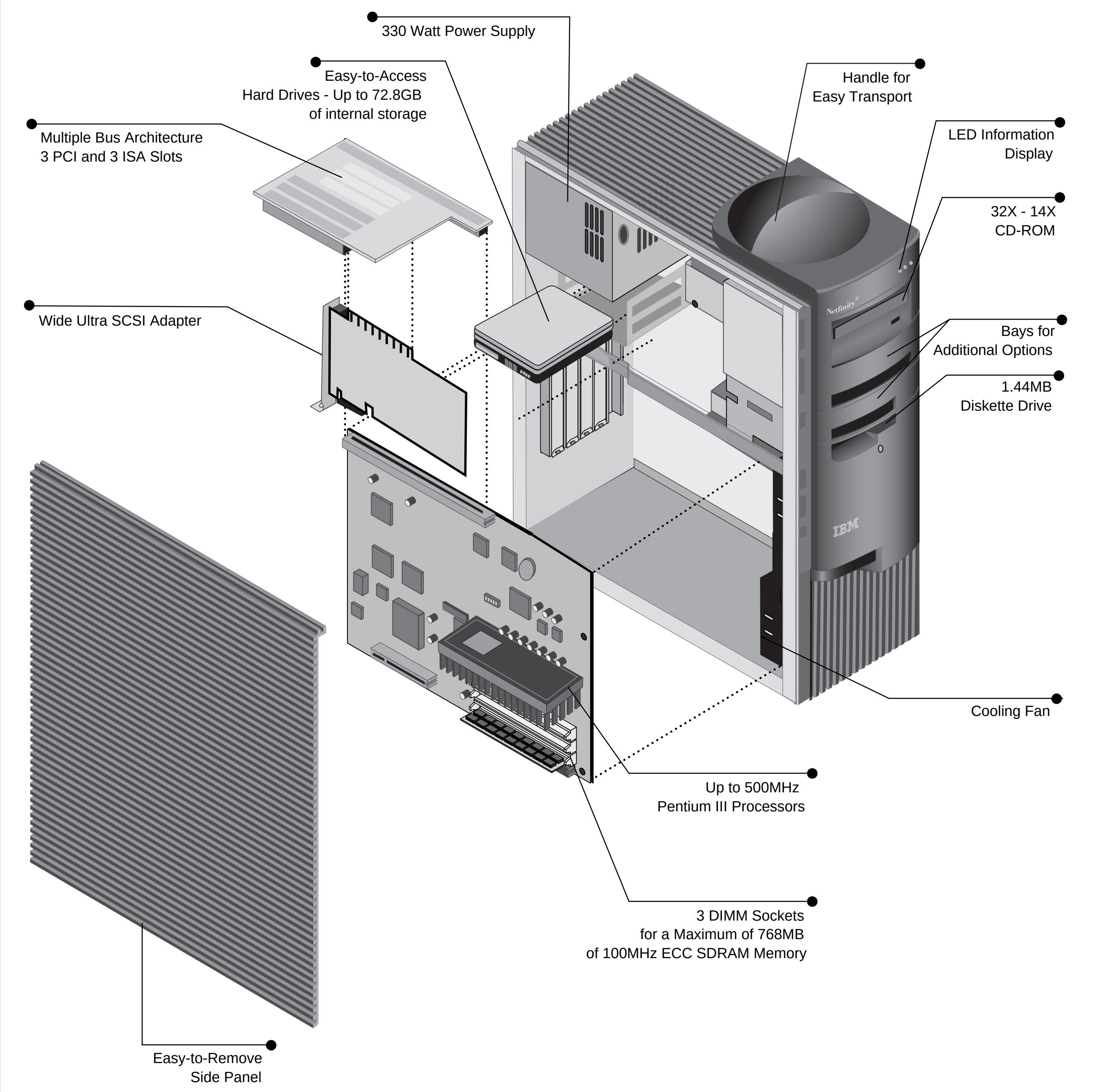

330 Watt Power Supply
Easy-to-Access Hard Drives - Up to 72.8GB of internal storage
Multiple Bus Architecture 3 PCI and 3 ISA Slots
Handle for Easy Transport
LED Information Display
32X - 14X CD-ROM
Wide Ultra SCSI Adapter
Bays for Additional Options
1.44MB Diskette Drive
Netfinity
IBM
Cooling Fan
Up to 500MHz Pentium III Processors
3 DIMM Sockets for a Maximum of 768MB of 100MHz ECC SDRAM Memory
Easy-to-Remove Side Panel

Figure 112. The Netfinity 3000 Exploded View

5.5.1 System Management

As well as the standard Netfinity Manager functions, the Netfinity 3000 has a National Semiconductor LM78 management processor and I^{2}C bus on the planar that provide a number of hardware monitors that can be integrated into Netfinity Manager.

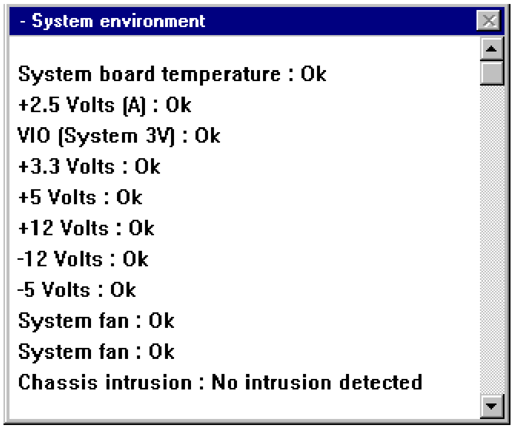
Note: These additional management functions are available only for OS/2 and Windows NT. No support is provided for NetWare .

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 shown in Figure 113:



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 113. Netfinity 3000/3500 Hardware Monitors

A history of all changes to these monitors is also available by right-clicking 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 32. Alerts can be set up in System Monitor by right-clicking 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 25 for more information on how to set up actions in Alert Manager.

Table 32. 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
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)

5.5.1.1 Management Driver Installation

Prior to installing Netfinity Manager, you need to install the necessary management drivers.

Note: The drivers are available only for OS/2 and Windows NT. No support is provided for NetWare.

The diskette image for the Netfinity 3000 is available on ServerGuide 4.0.4 or later. It should also be available from:

`http://www.pc.ibm.com/us/support`

Select **Server** from Select a brand.
Select **Netfinity 3000** from Select your family.
Click **Downloadable files**.
Click **Windows NT** or your operating system.
Look for the Client Care diskette and download it.

To build the diskette image from ServerGuide, follow these steps (if you already have Diskette Factory installed, skip to Step 6 on page 153):

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 the **Install** button.
6. Run Diskette Factory **Start -> Programs -> ServerGuide Utilities -> Diskette Factory**.
7. Select **Other Servers** and click the “>” button.
8. Select **IBM Netfinity 3000 System Diskettes** and click on “>” to continue.
9. Deselect all options, by clicking the **Select/Deselect All** button.
10. Select **Windows NT Device Drivers** or **OS/2 Device Drivers** and click ">".
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.

5.5.2 Advanced Systems Management Adapter

The Advanced Systems Management Adapter is also available as an option in the Netfinity 3000. The adapter, in conjunction with Netfinity Manager, allows you to better manage the availability of your server.

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

See 3.5, “The IBM Advanced Systems Management Adapter” on page 86 for information about functions.

5.5.2.1 Adapter Installation

As there is no I^2C connector on the system board, the installation of the Advanced Systems Management Adapter is straightforward:

1. Install the adapter in the slot using the usual electrostatic precautions.
2. Reserve an IRQ and a port address for the adapter in the 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 per Table 33:

Table 33. 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.

   We recommend that you use the default settings, port 200-207 and IRQ 5.

2. 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 2.30 of this diskette and we set up port 200-207 and IRQ 5 for the card.
3. Set up the COM ports on the adapter.

   For further information on the configuration of COM ports see 3.5.2, “ASM ISA Adapter COM Ports” on page 89.

Chapter 6. Netfinity Capacity Manager

Netfinity Capacity Manager is an efficient system management tool integrated into the Netfinity Manager software to help you to measure the potential bottlenecks of various subsystems. You can use this tool to forecast performance degradation of a server and its subsystems. You may plan for an appropriate action to overcome the bottleneck well in advance, so as to prevent overall performance degradation.

Key resource utilizations over time are collected from network systems and merged into a single report that can be viewed graphically or exported into a spreadsheet for further analysis. These reports show at a glance potential capacity bottlenecks within the selected systems. Your analysis and ability to predict bottlenecks is critical when planning for future upgrades. Capacity Manager gives you the ability to plan the allocation of hardware upgrades for the systems that really need them before a capacity bottleneck occurs.

Capacity Manager is available as part of Netfinity Manager V5.1 onward.

New to Netfinity Manager V5.2 is a performance analysis feature of Capacity Manager. This is discussed in 6.7, “Performance Analysis” on page 181.

Key Concept

The key concept to understand about Capacity Manager is that the data is *always* being gathered. Unlike Performance Monitor, you do not have to start the logging of data. With Capacity Manager, you simply specify what data you want retrieved from the servers and workstations in your network and it is gathered up and displayed graphically for you. Up to one month’s worth of data is automatically saved by every system running Netfinity Manager 5.1 or later.

6.1 Installation

Like other Netfinity Manager components, Capacity Manager is made up of two components, a user interface and a base. The base component is automatically installed whenever both the manager and client services of Netfinity Manager are installed. The base component is included with Netfinity Manager Version 5.1 or later and is installed on the following configurations:

- Active Client: Version 5.1 or later
- Passive Client: Version 5.2 or later
- Manager: Version 5.1 or later

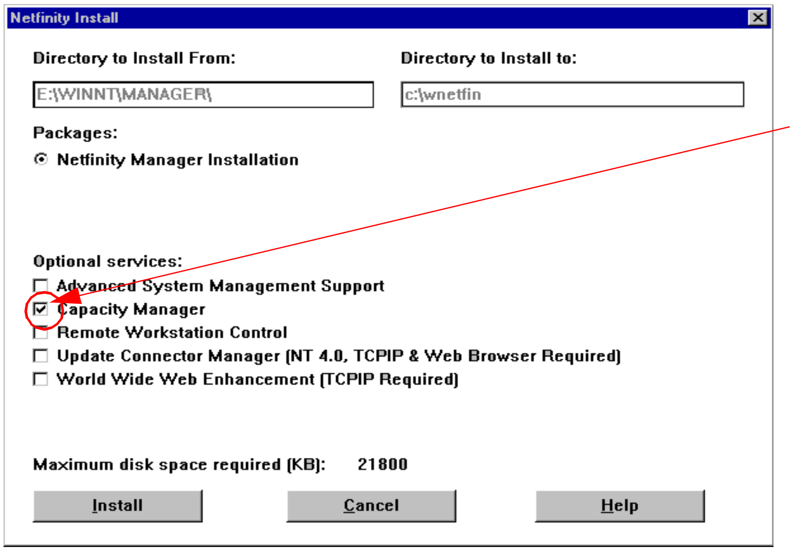
The Capacity Manager base runs on all Netfinity Manager-supported platforms:

- Windows NT 3.5/4.0
- OS/2 Warp
- NetWare
- Windows 95/98

Note: The Capacity Manager base does not run on Windows 3.1.

The base uses very few system resources and should not be disabled.

The Capacity Manager user interface is available only as part of the manager code on the Windows NT or Windows 95/98 platforms (that is, it is not part of Client Services for Netfinity Manager). Installation of the user interface is optional when Netfinity Manager is installed. During the installation of Netfinity Manager, you are presented with Figure 114:



Netfinity Install

Directory to Install From: E:\WINNT\MANAGER\

Directory to Install to: c:\wnetfin

Packages:

● Netfinity Manager Installation

Optional services:

□ Advanced System Management Support
☑ Capacity Manager
□ Remote Workstation Control
□ Update Connector Manager (NT 4.0, TCPIP & Web Browser Required)
□ World Wide Web Enhancement (TCPIP Required)

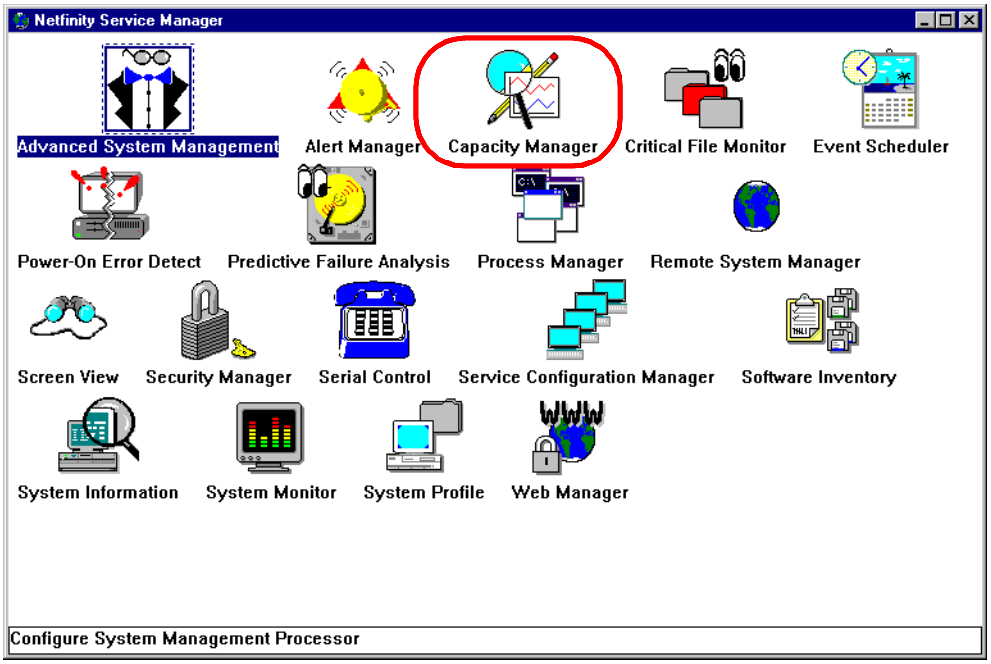
Maximum disk space required (KB): 21800

Mark this check box to install Capacity Manager

Figure 114. Netfinity Manager Installation Options

To install the Capacity Manager user interface, select **Capacity Manager** prior to clicking **Install**.

After you install Capacity Manager, a new icon appears in the Netfinity Manager window as shown in Figure 115:



Configure System Management Processor

Figure 115. Capacity Manager Icon

Note: You would normally run Capacity Manager from the Netfinity Manager main window. However, you can also start it independently, by running CAPMGT.EXE from the Netfinity Manager directory.

6.2 Capacity Manager Data Files

There are three types of data files used with Capacity Manager:

- Raw data files, with the extension .SLT
- Report Definition files, with the extension .MON
- Report files, with the extension .CMR or .TXT

When you use the Report Generator, it uses these SLT files from the various systems that you specify, and a report definition file (a .MON file) and it builds a report file (a .CMR). This is shown graphically in Figure 116:

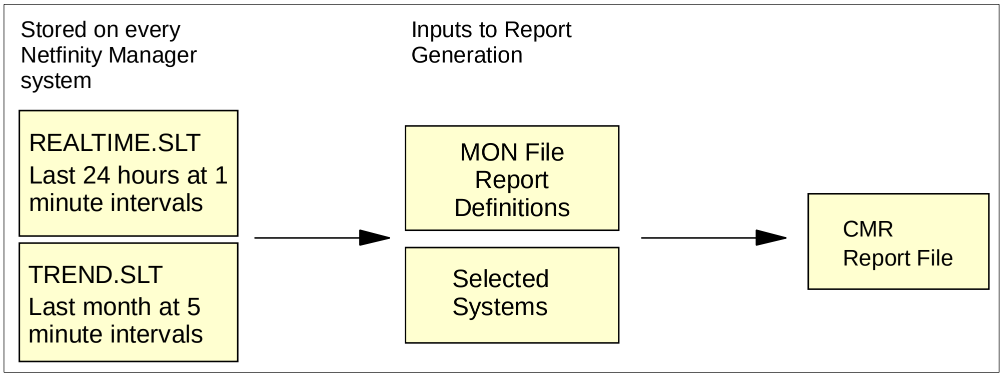

Stored on every Netfinity Manager system
Inputs to Report Generation
REALTIME.SLT
Last 24 hours at 1 minute intervals
TREND.SLT
Last month at 5 minute intervals
MON File Report Definitions
Selected Systems
CMR Report File

Figure 116. Generating Report Files

Capacity Manager also uses file CMUserSettings.properties which gets created when the user makes changes to the default settings.

6.2.1 SLT Files

Capacity Manager automatically saves one calendar month of data. The data is stored in two .SLT (or “slot”) files. These files are stored in the SLTFILES directory.

- REALTIME.SLT

  This file contains data from the last 24 hours, stored at one-minute intervals. Data that is older than 24 hours is discarded. The data is actually retrieved from the System Information service of Netfinity Manager at one-minute intervals.

- TREND.SLT

  This file contains data from the last calendar month, stored at five-minute intervals. For example, on October 15, the TREND.SLT file contains data back to September 15. Data older than one calendar month is discarded. The values stored in this SLT file are the average of the five one-minute values of the last five minutes.

On all machines with Netfinity Manager installed, the SLT files are continually being updated with the latest data.

6.2.2 MON Files

The MON files are effectively filters. Each is a description of what monitors are to be collected and when. During the course of report generation (as described in 6.5.1, “Step 1: Report Definition” on page 165), these MON files are used to gather only the data required.

Four MON files are supplied as samples: Hourly, Daily, Weekly and Monthly. You can use these as is or edit them or create new ones. See 6.5.1, “Step 1: Report Definition” on page 165 for details.

6.2.3 CMR Files

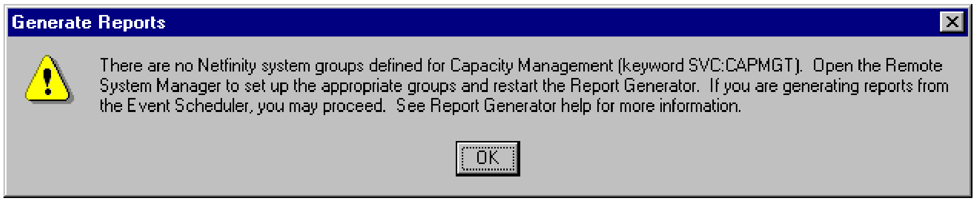
CMR files are the output of the report generation process. They contain the data specified by the selected MON file and for the systems chosen during the process. As described in 6.10, “Automatically Collecting Data Longer Than One Month” on page 192, you can merge multiple CMR files together.

6.3 Before You Begin

Before you start Capacity Manager, you should configure Netfinity Manager for the appropriate groups and for the appropriate security settings.

6.3.1 Creating Capacity Manager Groups

Before you can use Capacity Manager, you must first define special Netfinity Manager groups using the Remote System Manager. If you proceed without first defining a group, you will get the following error message (Figure 117):



There are no Netfinity system groups defined for Capacity Management (keyword SVC:CAPMGT). Open the Remote System Manager to set up the appropriate groups and restart the Report Generator. If you are generating reports from the Event Scheduler, you may proceed. See Report Generator help for more information.

Figure 117. Error Message for Generating Reports

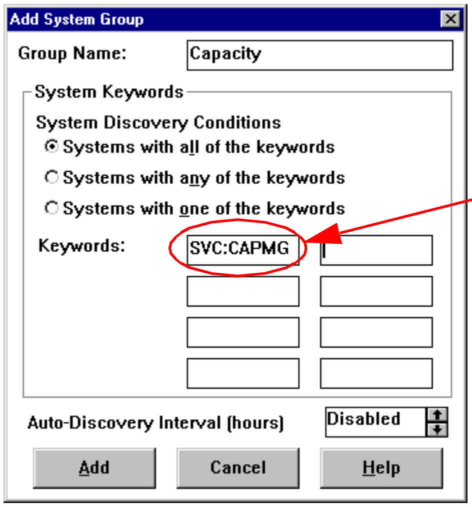
Note: We assume you are already familiar with Netfinity Manager and Remote System Manager. If you need information on these, consult the *Netfinity Manager User’s Guide*.

Capacity Manager will work only with systems in existing groups that use the system keyword SVC:CAPMGT. Follow these steps:

1. From the Netfinity Manager main window (Figure 115 on page 156), double-click **Remote System Manager.**
2. From the System Group Management window, click **Group -> Add Group**. Figure 118 on page 159 appears.
3. Type in a name for your group in the Group Name field.
4. In one of the Keywords field, type in `SVC:CAPMGT`**.** If you wish to add other keywords, or change the System Discovery Conditions, you may do so.

   Note: The SVC:CAPMGT keyword must be in all capital letters.
5. Set the Auto-Discovery Interval as required.

6. Click on **Add**.



Group Name: Capacity

System Keywords

System Discovery Conditions

● Systems with all of the keywords

○ Systems with any of the keywords

○ Systems with one of the keywords

Keywords: SVC:CAPMG

Auto-Discovery Interval (hours) Disabled

All groups used for Capacity Manager must have the keyword SVC:CAPMGT

Figure 118. Adding a New Group

After you add the new group, it will appear in the System Group Management window as shown in Figure 119:

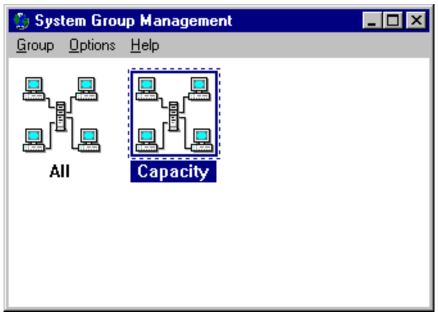


Figure 119. Newly Defined Group

To see the systems that will be included in the group, double-click the groups icon. Click **System -> Discover Systems**. The systems that match your keywords (other than the SVC:CAPMGT keyword) should appear in the window after a short time.

Note: You can also use SVC:CAPMGT to show all systems in your network that have the Capacity Manager function installed (that is, Manager and Active Clients running Version 5.1 or later and Passive Clients running Version 5.2 or later).

6.3.2 Setting Netfinity Manager Security

By default, Netfinity Manager has no security enabled. However, you would normally set security to remove all access to the Netfinity Manager services from <PUBLIC> access. For the rest of this section, we assume you have removed all access from public access.

Before you can use Capacity Manager to gather data from remote systems, you will need to configure security on both the local and the remote systems to authorize the transfer of data. The first step is to set up incoming security on each remote server, then to set up outgoing access from the system running the Capacity Manager GUI to each of the servers. You need to set this up only once.

Note: This also applies when you are gathering data locally — the Capacity Manager request is still treated as coming from a remote system.

For more information about the security functions of Netfinity Manager, see the *Netfinity Manager User's Guide*.

6.3.2.1 Setting Up Incoming Passwords

Here we want to provide access to the Capacity Manager service on each remote server. Follow these steps:

1. On each remote server run Netfinity Manager and open Security Manager. (You can also do this remotely through Remote System Manager.) Figure 120 appears:

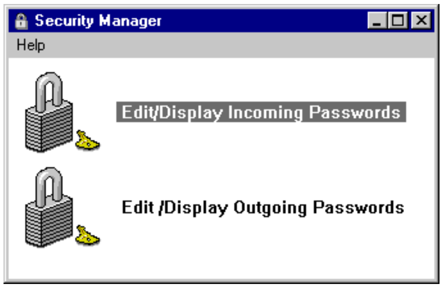
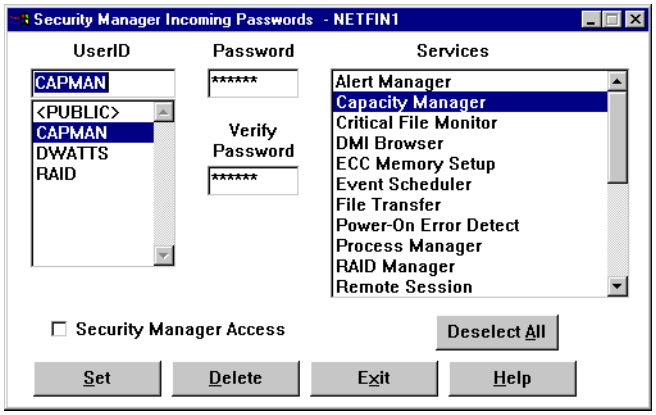

Security Manager
Help
Edit/Display Incoming Passwords
Edit /Display Outgoing Passwords

Figure 120. Netfinity Manager Security Manager

2. Double-click **Edit/Display Incoming Passwords**. Figure 121 appears:



UserID: CAPMAN

<PUBLIC>
CAPMAN
DWATTS
RAID

Password: ******

Verify Password: ******

Services:
Alert Manager
Capacity Manager
Critical File Monitor
DMI Browser
ECC Memory Setup
Event Scheduler
File Transfer
Power-On Error Detect
Process Manager
RAID Manager
Remote Session

☐ Security Manager Access

Figure 121. Incoming Passwords for a Remote Server

We recommend you set up a user ID and password combination that has access to the Capacity Manager service only, as we have done in Figure 121. This ensures that, even if the password is compromised, none of the critical services are accessible.

1. Type in the user ID CAPMAN.
2. Type in the password you want in both password fields.
3. Click the **Deselect All** button.
4. Select the **Capacity Manager** service.
5. Deselect **Security Manager Access** (this is important).
6. Click **Set.**

You need to repeat the above steps for each server from which you will be retrieving Capacity Manager data.

6.3.2.2 Setting Up Outgoing Passwords

On the system where you will be running the Capacity Manager GUI, you now need to set up outgoing passwords that match the ones you've just defined as incoming passwords.

From the Security Manager main window, double-click **Edit/Display Outgoing Passwords**. Figure 122 appears:

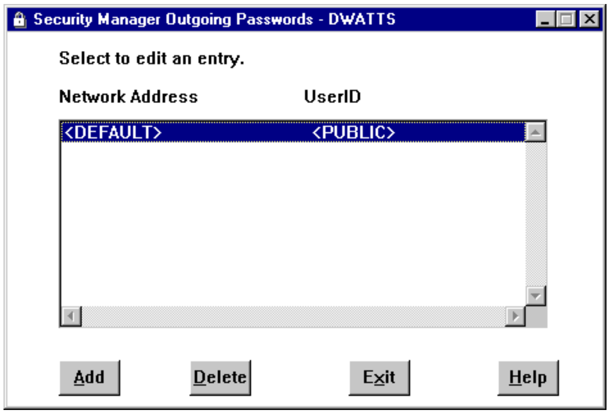


Figure 122. Outgoing Passwords on the Local System

Netfinity Manager allows you to set up the Capacity Manager access in one of three ways:

1. Change the default outgoing user ID from <PUBLIC> to CAPMAN.

   This is the easiest way to set security, as it involves only one change. In Figure 122, double-click the **<DEFAULT>** Network Address. Figure 123 appears:

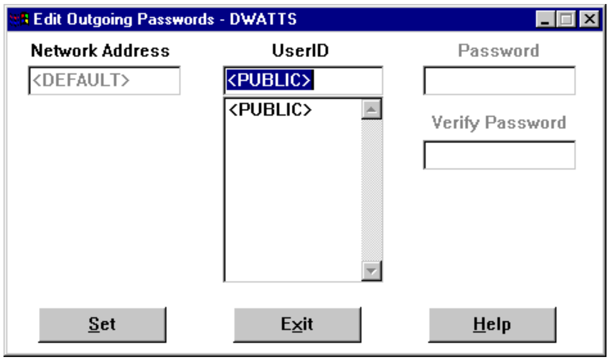


Figure 123. Editing the Default Outgoing Password

   Change `<PUBLIC>` to `CAPMAN` and type in the password you specified in 6.3.2.1, "Setting Up Incoming Passwords" on page 160 in the two password fields, then click **Set**.

   This method is easy to configure but has some implications:

   – Every system you access remotely from this workstation will use the user ID of CAPMAN instead of <PUBLIC>. If you use this workstation for other purposes or with other administrators, you may prefer to use <PUBLIC> by default.
   – It may become confusing because the Capacity Manager service does not have an icon in the Netfinity Manager window (the GUI does, but the GUI icon does not appear unless you specifically install it per 6.1, "Installation"

on page 155). If you have CAPMAN as the default and then double-click that system from within Remote System Manager, the next window will not show any icons.

2. Setting a default password for each server.

   If you do not want to set the default user ID to be CAPMAN for *every* system you access, you can just set it as the default for specific systems.

   Note: This option is available only if you have not selected **Force Remote Logons** in the Network Driver Configuration program (in the Netfinity folder). Setting this option disables the ability to save default user IDs for specific systems.

   1. Set up a group in Remote System Manager. See 6.3.1, “Creating Capacity Manager Groups” on page 158 for details.

   2. For each of the systems in the group, right-click the icon. Figure 124 appears:

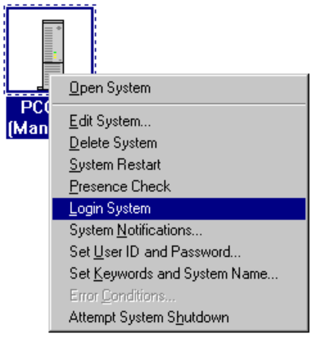


Figure 124. Logging On to a Remote System

   3. Select **Login System**. You will be prompted to enter a user ID and password. Type in `CAPMAN` and the associated password. You will then be prompted:

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

      Note: If you do not get this message, then you have set **Force Remote Logons** in the Network Driver Configuration program.

   4. Click **Yes**. An entry will then be added to your Outgoing Passwords list (Figure 122 on page 161).

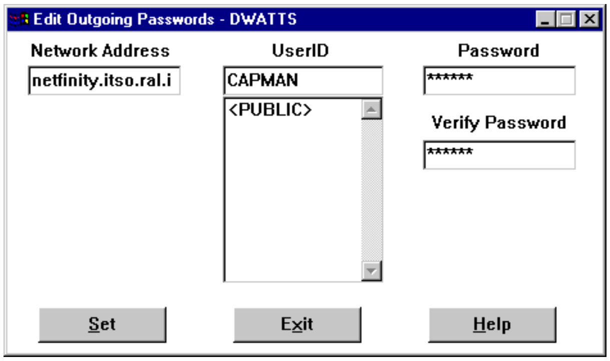
   5. Repeat for each server you want to access via Capacity Manager.

   The implications for setting a default password of CAPMAN for specific systems are similar to those listed in the first option. Of course, as you are setting only a default for some systems, the implications are lessened.

3. Setting a specific password for each server.

   Here, you do not modify the default user IDs for any systems. However, you do have to make more effort to set up the outgoing passwords.

   1. In the Outgoing Passwords list (Figure 122 on page 161), click the **Add** button. Figure 125 appears:



Edit Outgoing Passwords - DWATTS

Network Address: netfinity.itso.ral.i

UserID: CAPMAN

<PUBLIC>

Password: ******

Verify Password: ******

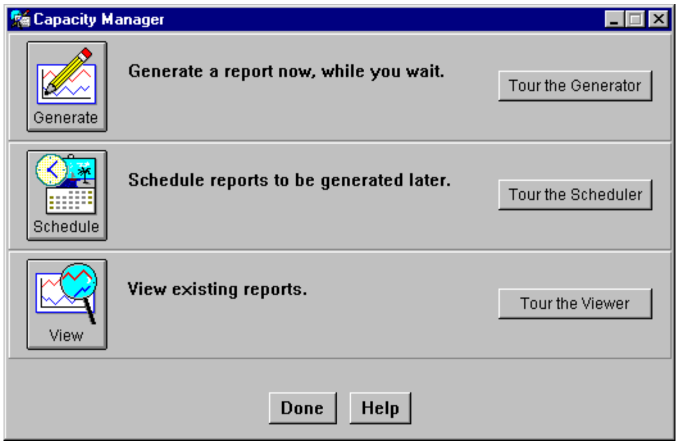
Figure 125. Adding a Specific Password for a Specific Server

2. Type in the network address (the TCP/IP, for example) of the remote server, the CAPMAN user ID and password (**Note**: Do not include “TCP::” as in other Netfinity Manager configuration windows.)
3. Click **Set.**
4. Repeat for each remote server.

You can select any of these three methods depending on your requirements and the degree to which you wish to separate the default system access from the access to the Capacity Manager service on each remote server.

6.4 Starting Capacity Manager

After you successfully install the Capacity Manager software, double-click the **Capacity Manager** icon. Figure 126 will appear. This is the main menu of Capacity Manager.



Capacity Manager

Generate a report now, while you wait.

Schedule reports to be generated later.

View existing reports.

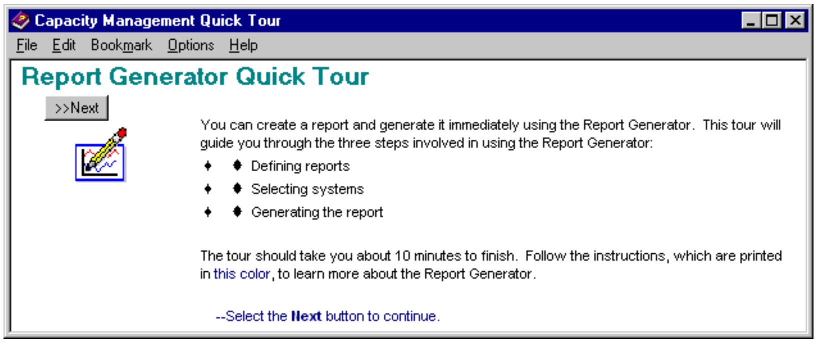
Figure 126. Capacity Manager Main Menu

You can perform three important functions from this menu:

1. Generating a report immediately (see page 164).
2. Scheduling a report to be generated later (see page 186).
3. Viewing a report that has already been generated (see page 174).

6.4.1 Running the Tour

Each of the three functions has a **Tour the...** button which will guide you through the process. Clicking the button launches the function and also displays some help screens to explain what to do. Figure 127 shows you the first help screen when you click **Tour the Generator** in Figure 126:



Report Generator Quick Tour

You can create a report and generate it immediately using the Report Generator. This tour will guide you through the three steps involved in using the Report Generator:

- Defining reports
- Selecting systems
- Generating the report

The tour should take you about 10 minutes to finish. Follow the instructions, which are printed in this color, to learn more about the Report Generator.

--Select the **Next** button to continue.

Figure 127. Report Generator Quick Tour

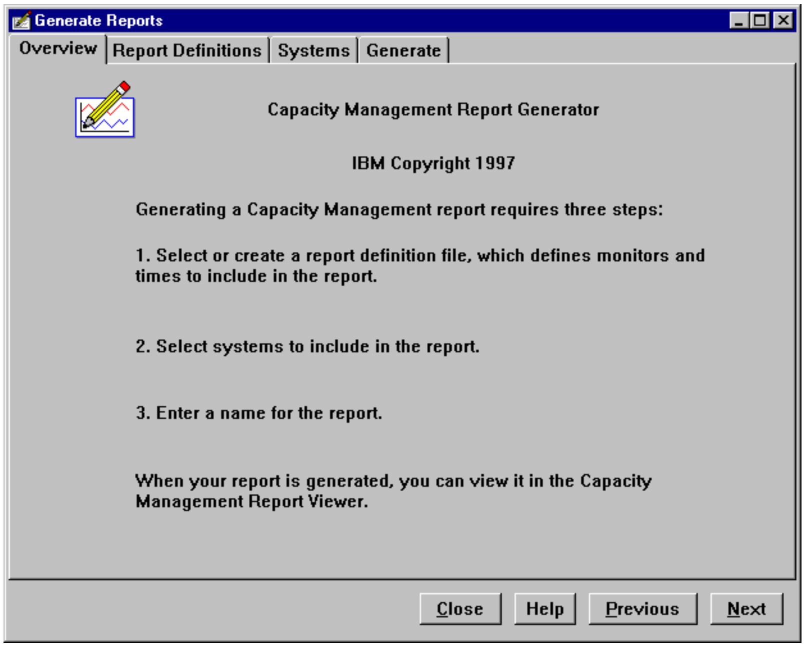
Now you are ready to generate a report.

6.5 Generating a Report Immediately

You can create a report and generate it immediately using the Report Generator. We will discuss the three steps involved in using the Report Generator:

1. Defining the report
2. Selecting the systems
3. Generating the report

Clicking the **Generate** button in Figure 126 on page 163 brings up the first window, as shown in Figure 128 on page 165. This window explains the overview of the process. The other three tabs in this window are the three steps in the generate process.



Capacity Management Report Generator

IBM Copyright 1997

Generating a Capacity Management report requires three steps:

1. Select or create a report definition file, which defines monitors and times to include in the report.

2. Select systems to include in the report.

3. Enter a name for the report.

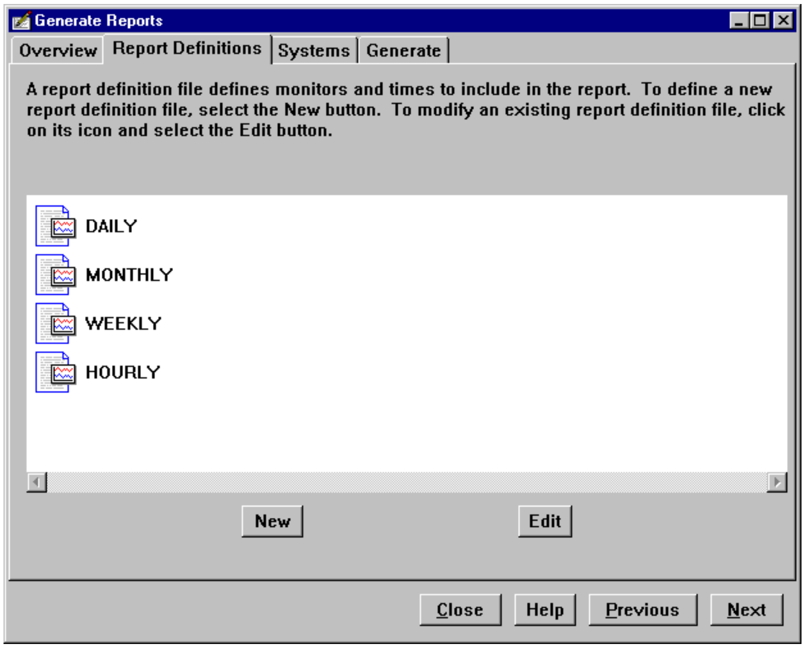
When your report is generated, you can view it in the Capacity Management Report Viewer.

Figure 128. Overview of Report Generator

To continue to the first step, report definition, click the **Report Definitions** tab or the **Next** button. Figure 129 appears.

6.5.1 Step 1: Report Definition

The first step in creating a Capacity Management Report is to work with a Report Definition file. Think of these as data filters. Here you specify what data you want gathered from systems in your network.



A report definition file defines monitors and times to include in the report. To define a new report definition file, select the New button. To modify an existing report definition file, click on its icon and select the Edit button.

DAILY
MONTHLY
WEEKLY
HOURLY

Figure 129. Report Definition

You can do one of three things at this point:

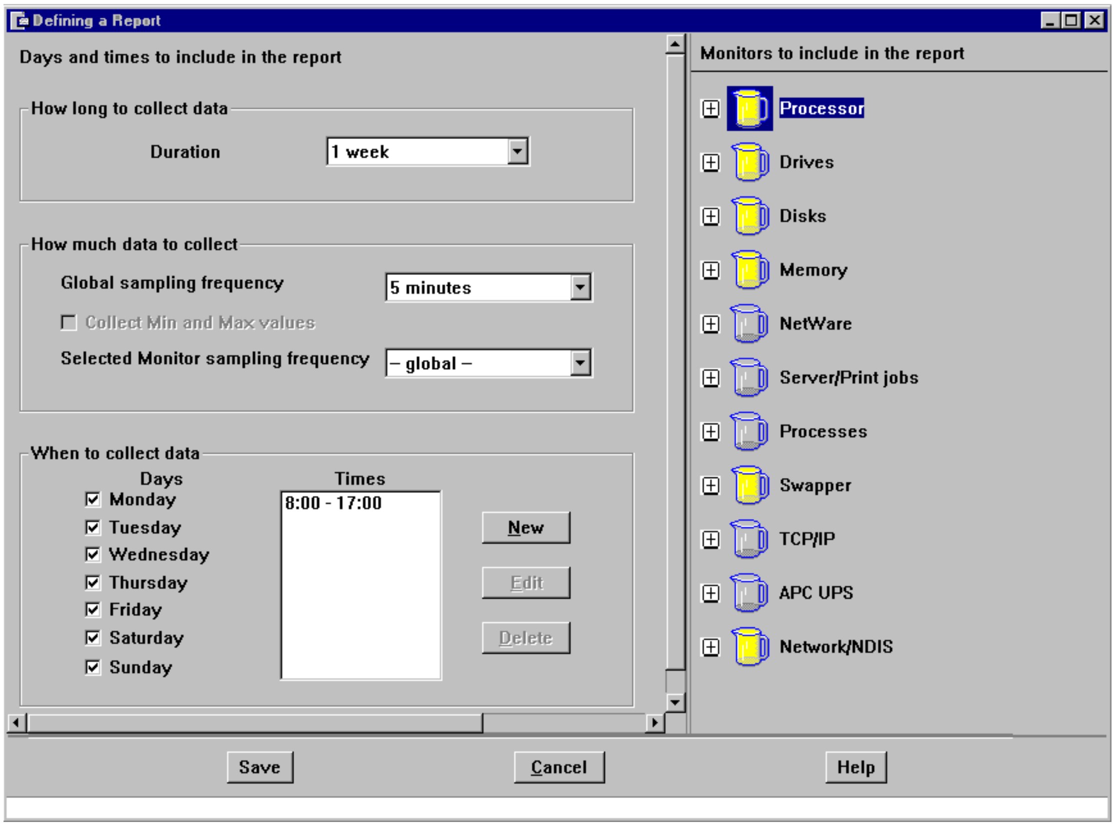
1. Create a new report by clicking **New.**

2. Selecting an existing report.
3. Editing an existing report by selecting it, then clicking **Edit.**

Tip: To delete a report, you have to delete the associated .MON file in the \WNETFIN\MONFILES directory, then restart the Report Generator.

6.5.1.1 Creating a New Report

To create a new report (or filter), click the **New** button. Figure 130 appears:



Defining a Report

Days and times to include in the report

How long to collect data

Duration: 1 week

How much data to collect

Global sampling frequency: 5 minutes

□ Collect Min and Max values

Selected Monitor sampling frequency: – global –

When to collect data

Days:
- ☑ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday
- ☑ Saturday
- ☑ Sunday

Times: 8:00 - 17:00

Figure 130. Creating a New Report Definition

The components of this window are as follows:

Duration

Duration specifies how far back you want your report to measure. Since Capacity Manager keeps one month of data (a calendar month, for example, November 10 back to October 10), you can schedule a report to measure up to one month of time. Available choices are:

- 1 hour
- 8 hours
- 1 day
- 1 week
- 1 month

Time periods of one hour look back one hour from the beginning of the current hour but also include whatever time has passed in the current hour. (For example, if you run your report at 3:18 p.m., the report will measure from 2 p.m. to 3:18 p.m.)

Time periods of eight hours look back eight hours from the beginning of the current hour but also include whatever time has passed in the current hour. Time periods of one day look back 24 hours from the beginning of the current hour. Time periods of one week or one month look back from the previous midnight.

Global Sampling Frequency

This determines how often data is collected, and therefore the granularity of your report data. You can select:

- 1 minute
- 5 minutes
- 30 minutes
- 1 hour
- 1 day

You may want to choose a larger value if you are concerned about the space taken to store this data. Not all of these choices will be available. If you choose a duration of one week or one month, the one minute sampling frequency will not be available. This is because the data for the last 24 hours is saved per minute, but after a day, data is averaged to one value per five minutes.

If, for example, you set the global sampling frequency to one minute, you will get data from all monitors every minute. For monitors such as free disk space, this can be a waste of bandwidth and space. In such instances, use a sampling frequency that is higher for that specific monitor. Do this by specifying a value in **Selected Monitor Sampling Frequency** other than **-global-**.

Note: Raw data is gathered from the System Information service of Netfinity Manager at one-minute intervals. These one-minute values are instantaneous values and are not averages over the last minute of activity. This means that any spikes in usage that do not continue over a sampling point will not be recorded.

Collecting Minimum and Maximum Values

Collecting minimum and maximum values gathers the highest and lowest value for each monitor within the sampling frequency. Doing so triples the size of report files and slows performance in the Report Viewer, but provides valuable data, especially if the sampling frequency is set to a large amount of time. Minimum and maximum values are not available when the sampling frequency is set to the smallest sampling frequency available for that time period.

Warning

If you wish to display minimum and maximum values in the Report Viewer (6.6, “Viewing a Report” on page 174), we strongly recommend you collect the min/max data at this point. If you don’t collect the min/max data but choose to display the min/max values anyway, then the graphs displayed will be approximations based on incomplete data and are likely to be inaccurate.

Selected Monitor Sampling Frequency

There are two ways to define sampling frequencies: a *global* sampling frequency, which applies to all monitors, and an *individual* sampling frequency, which can be set for a particular monitor. You might want to set the frequency of monitors that do not change dramatically during the day to a larger unit of time, such as one day, while setting other monitors that do change dramatically, such as CPU utilization, to a smaller unit of time, such as five minutes.

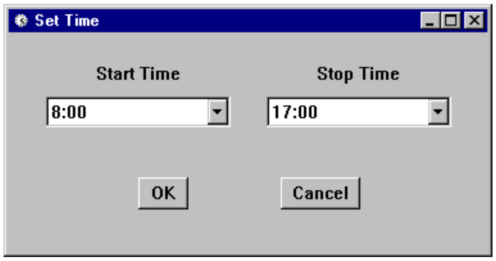
To set an individual frequency, highlight the monitor name in the right side of the window and specify the individual frequency in the Selected monitor sampling frequency drop-down list box.

The default is a global sampling frequency.

When to Collect Data

The next step is to define when data is collected. To make your report accurately reflect the use of your systems, you can select the days and times they are typically used. To define days, click the check boxes of the days you want included. To define times to measure, click the **New** button and enter start and stop times in the window shown in Figure 131 on page 168.

To measure the entire day, select 0:00 for both choices. To exclude times when systems are typically not used (for example, the lunch hour) you can define more than one time in this field. Click the **Edit** button and enter 08:00 for the start time and 12:00 for the end time. Click the **New** button and enter 13:00 for the start time and 17:00 for the end time.



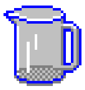
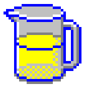
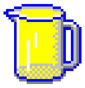
Start Time: 8:00
Stop Time: 17:00

Figure 131. Setting Start and Stop Times

Monitors to Include in the Report

The final step in working with a report definition file is to define which monitors to collect data. Monitors are listed in groups as shown in Figure 130 on page 166. You can expand the group by clicking the ⊞ icon next to it. The groups and monitors are represented as pitchers (or jugs) per Table 34:

Table 34. Meaning of the Pitcher Icons

Pitcher	Group Meaning	Monitor Meaning
	No items in the group have been selected.	The monitor has not been selected.
	Some items in the group have been selected or you selected an entire group by selecting every monitor individually.	No meaning.
	An entire group has been selected by double-clicking the group pitcher.	The monitor has been selected.

To select an entire group of monitors, double-click the group icon that will display the pitcher as full. To select individual monitors, click the plus icon next to the monitor group and double-click the monitor's pitcher icon.

Note: You will see monitors listed that may not apply to all systems in your network (for example, space remaining on Drive Z). Only monitors that apply to each individual system will be included in the report.

Table 35 is a list of all monitors available to Capacity Manager:

Table 35. Monitors in Capacity Manager

Group	Monitors
Processor	CPU Utilization Port I/O Rate Memory I/O Rate Interrupt Rate Integer Instructions Rate Floating Point Operation Rate Cache Hit Ratio Utilization CPU 1, 2, etc.
Drives	Space Remaining for Drive C:, D:, etc. Space Used for Drive C:, D:, etc.
Disks	Disk Utilization for Disk 1, 2, etc. Disk Workload for Disk 1, 2, etc. Disk Error Rate for Disk 1, 2, etc.
Memory	Memory Usage Locked Memory Error Correction
NetWare	Space Remaining for Volumes Sys, Data and others Space Used for Volumes Sys, Data and others
Server/Print Jobs	Server Sessions Server Connections Opens Shared Devices KB Sent KB Received Average Response Time Requested Buffer Shortages Big Buffer Shortages Print Jobs Queued
Processes	Process Count Thread Count
Swapper	Swap File Size Swapper Drive Remaining Space
TCP/IP	Datagrams Sent and Received IP Packets Sent and Received IP Packets Received with Error Connections Sockets in use Unicast Packets Sent and Received Broadcast Packets Sent and Received Bytes Sent and Received

Group	Monitors
APC UPS	Run Time Remaining Utility Line Voltage Battery Voltage Battery Capacity UPS Load UPS Temperature External (Ambient) Temperature External (Ambient) Humidity
Network / NDIS	NDIS Adapter Packets Received and Sent Segment % Network Utilization Packets Sent and Received Bytes Sent and Received Transmit Errors Receive Errors Host Errors Wire Errors Ring Utilization

Saving Reports

After you have specified the settings and monitors you want in the report, you need to save it. Click the **Save** button. You will then be prompted to specify the name of a .MON file. We recommend you save it in the default directory of NETFIN\MONFILES. The file name can be more than eight characters and can include spaces. It is converted to all uppercase by Capacity Manager.

6.5.1.2 Predefined Reports

As shown in Figure 129 on page 165, four reports are predefined:

1. Hourly
2. Daily
3. Weekly
4. Monthly

These reports gather a predefined subset of all available monitors. Table 36 shows the characteristics of each of these reports. The complete list of all monitors is in Table 35 on page 169.

Table 36. Characteristics of the Predefined Definition Reports

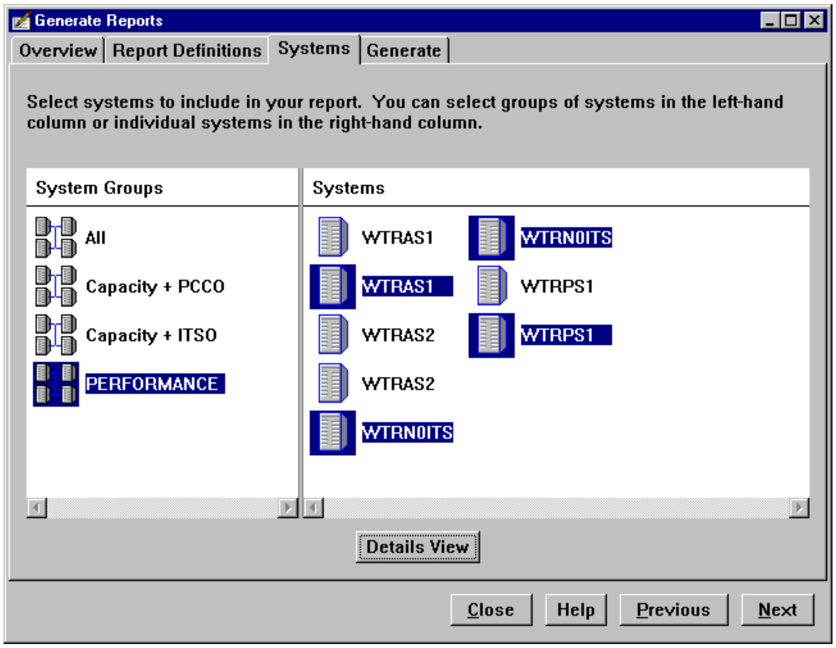
	Hourly	Daily	Weekly	Monthly
Duration	1 hour	1 day	7 days	30 days
Sampling Frequency	Every minute	Every minute	Every 5 minutes	Every hour
Hours		24 hours	0800-1700	0800-1700
Monitors	All Processors All Drives All Disks All Memory All Swappers All Network/NDIS	All Processors All Drives All Disks All Memory All Swappers All Network/NDIS	All Processors All Drives All Disks All Memory All Swappers All Network/NDIS	All Processors All Drives All Disks All Memory All Swappers All Network/NDIS

A duration of one hour starts on the hour but also includes whatever time has passed in the current hour. For example, if you schedule your report at 3:18 p.m., the report will measure from 2 p.m. to 3:18 p.m.

Durations of eight hours look back eight hours from the beginning of the current hour but also include whatever time has passed in the current hour. Durations of one day look back 24 hours from the beginning of the current hour. Durations of one week or one month look back from the previous midnight.

6.5.2 Step 2: Selecting Systems

The next step is to select the systems from which you want the data gathered. Click the **Systems** tab or the **Next** button. Figure 132 on page 171 appears:



Select systems to include in your report. You can select groups of systems in the left-hand column or individual systems in the right-hand column.

Figure 132. Selecting Multiple Systems Using the Ctrl Key

From here, you can select:

- All systems in a single group, by clicking the group icon.
- All systems in multiple groups, by selecting the first group, then using the Ctrl or Shift keys to select the other groups.
- Specific systems within one group, by selecting the group, then the first system you want, then using the Ctrl or Shift keys to select the other systems (as we have done in Figure 132).
- Specific systems within one group by clicking and dragging the left mouse button.

Note: The only groups that will be displayed here are the ones with the SVC:CAPMGT defined. If there are no groups listed in Figure 132, then you have either not defined any Netfinity Manager groups with this keyword, or you defined them while the Generate Reports window was open and you did not close and reopen it. See 6.3.1, “Creating Capacity Manager Groups” on page 158 for details on the SVC:CAPMGT keyword.

Groups and Systems in the Report Generator

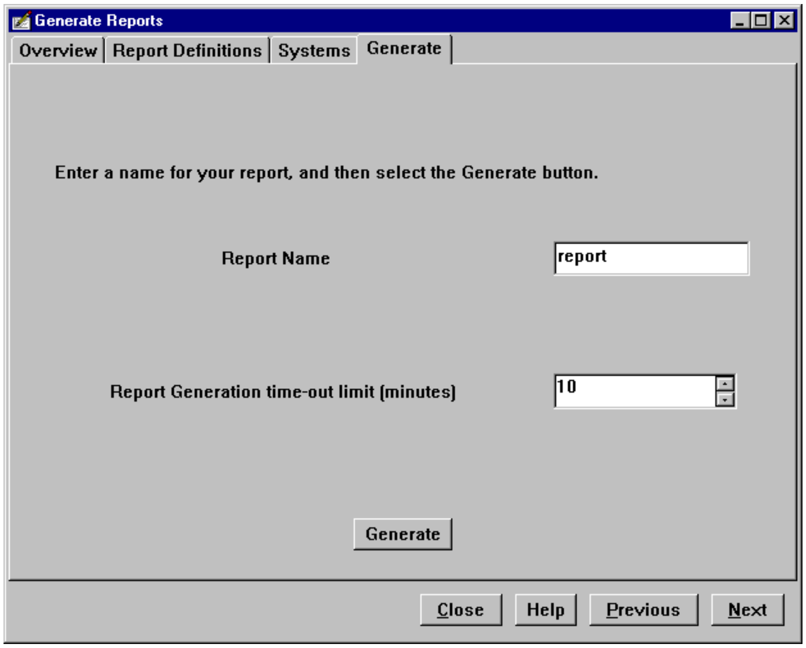
The Report Generator determines what Netfinity Manager groups and systems are available only when it starts (by clicking the **Generate** button in Figure 126 on page 163).

If you define a new group, or add systems to existing groups while the Report Generator window is open, you must close it and restart it before the changes will be picked up.

6.5.3 Step 3: Generating the Report

Now that you have defined the data you want to gather (6.5.1, “Step 1: Report Definition” on page 165) and the systems you want the data gathered from (6.5.2, “Step 2: Selecting Systems” on page 171), you can now request the process to begin.

Click the **Generate** tab, or the **Next** button. Figure 133 appears:



Enter a name for your report, and then select the Generate button.

Report Name: report

Report Generation time-out limit (minutes): 10

Figure 133. Generate Window

Type in a name for the report. If you select a name you have already used, the Report Generator will add a number to the file name (for example, Report01.CMR). The file will be saved into the REPORTS subdirectory.

The timeout limit determines how many minutes to wait for systems to respond. All the systems that have responded by this time will be included in the report. The default is 10 minutes, but this is normally excessive — you could set it to 1 minute.

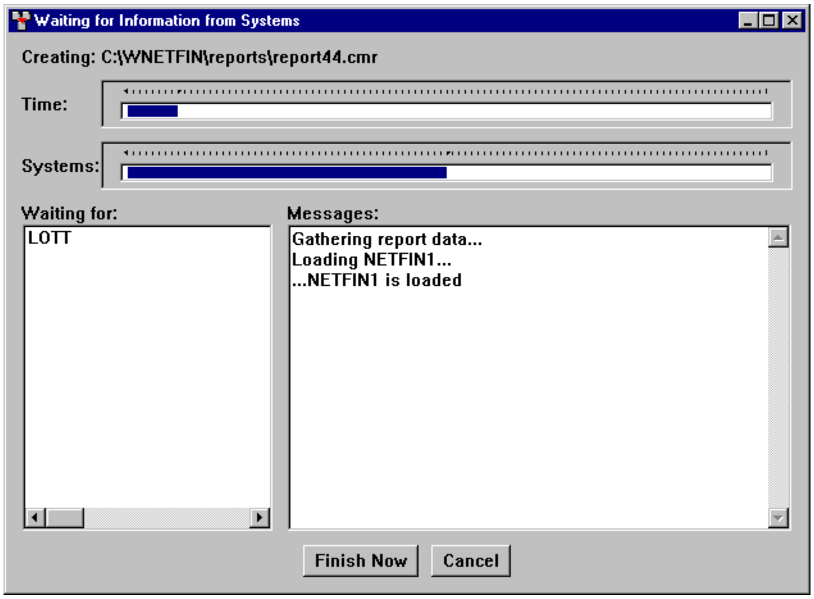
The reasons a system does not respond to a Generate request are:

- The remote system is powered off.
- NETFBASE is not running on the remote system.
- The network connection is down.

- Security has not been enabled on the remote system to allow incoming access to the Capacity Manager service.
- Security has not been enabled on the local system to supply a valid user ID and password for access to the remote system's Capacity Manager service.
- If you get the message "CMBase not running", it could be because you do not have sufficient virtual memory.

See 6.3.2, "Setting Netfinity Manager Security" on page 159 for details on the security settings required.

Click the **Generate** button to start the process. Figure 134 on page 173 appears showing you the progress of the gathering request:



Creating: C:\WNETFIN\reports\report44.cmr

LOTT

Gathering report data...
Loading NETFIN1...
...NETFIN1 is loaded

Figure 134. Generating Report

Figure 134 shows the following information:

- Time — the time elapsed since the request was issued; 100% is the number of minutes you specified in Figure 133 on page 172.
- Systems — the number of systems that have already responded; 100% is the total number of systems you selected in Figure 132 on page 171.
- Waiting for — the Netfinity Manager names of the systems that have yet to respond to the request.
- Messages — information about what events have occurred so far.

If some systems have not responded, you can either wait for the wait time to complete, or you can click the **Finish Now** button, which will terminate the gathering process and display the report with the data already gathered. Clicking **Cancel** will abort the gathering process and return you to the Generate Reports window.

Once all the systems have responded (or the Finish Now button has been clicked), the data will be processed and the report will be displayed. The Report Viewer is described in the next section.

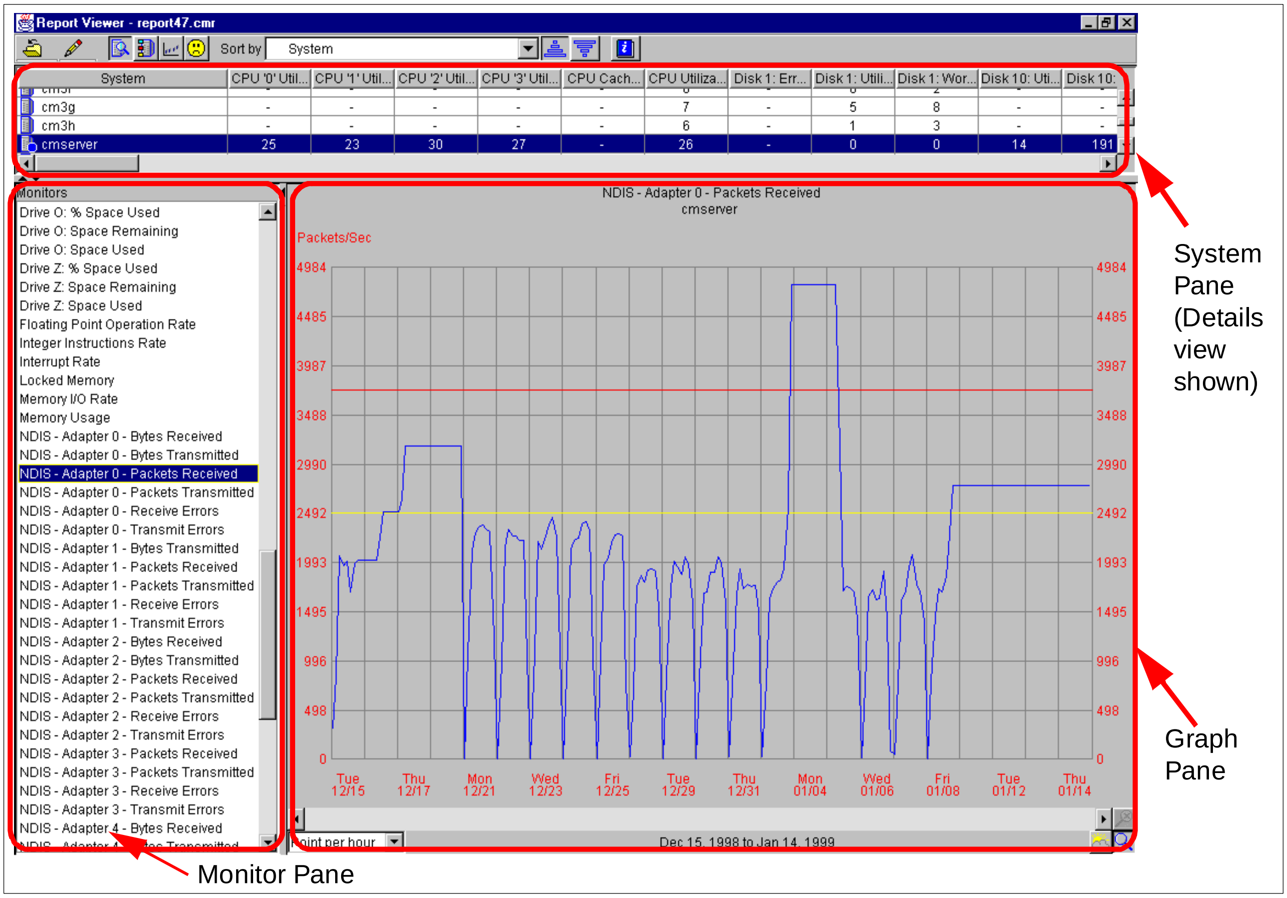
6.6 Viewing a Report

View

The report viewer is used to examine reports you have requested to be gathered immediately (as described in 6.5, “Generating a Report Immediately” on page 164) or to examine old reports or those you gathered using the scheduler function (6.8, “Scheduling a Report” on page 186).

To view an existing report, click the **View** button in Figure 126 on page 163. You will then be prompted to specify a report file (.CMR).

A typical Report Viewer window is shown in Figure 135. As you can see, it is made up of three window panes:



Report Viewer - report47.cmr

Sort by: System

System	CPU '0' Util...	CPU '1' Util...	CPU '2' Util...	CPU '3' Util...	CPU Cach...	CPU Utiliza...	Disk 1: Err...	Disk 1: Utili...	Disk 1: Wor...	Disk 10: Uti...	Disk 10:
cm3g	-	-	-	-	-	7	-	5	8	-	-
cm3h	-	-	-	-	-	6	-	1	3	-	-
cmserver	25	23	30	27	-	26	-	0	0	14	191

Monitors

Drive O: % Space Used
Drive O: Space Remaining
Drive O: Space Used
Drive Z: % Space Used
Drive Z: Space Remaining
Drive Z: Space Used
Floating Point Operation Rate
Integer Instructions Rate
Interrupt Rate
Locked Memory
Memory I/O Rate
Memory Usage
NDIS - Adapter 0 - Bytes Received
NDIS - Adapter 0 - Bytes Transmitted
NDIS - Adapter 0 - Packets Received
NDIS - Adapter 0 - Packets Transmitted
NDIS - Adapter 0 - Receive Errors
NDIS - Adapter 0 - Transmit Errors
NDIS - Adapter 1 - Bytes Transmitted
NDIS - Adapter 1 - Packets Received
NDIS - Adapter 1 - Packets Transmitted
NDIS - Adapter 1 - Receive Errors
NDIS - Adapter 1 - Transmit Errors
NDIS - Adapter 2 - Bytes Received
NDIS - Adapter 2 - Bytes Transmitted
NDIS - Adapter 2 - Packets Received
NDIS - Adapter 2 - Packets Transmitted
NDIS - Adapter 2 - Receive Errors
NDIS - Adapter 2 - Transmit Errors
NDIS - Adapter 3 - Packets Received
NDIS - Adapter 3 - Packets Transmitted
NDIS - Adapter 3 - Receive Errors
NDIS - Adapter 3 - Transmit Errors
NDIS - Adapter 4 - Bytes Received

System Pane (Details view shown)

Graph Pane

Monitor Pane

Figure 135. The Three Panes of the Report Viewer Main Window

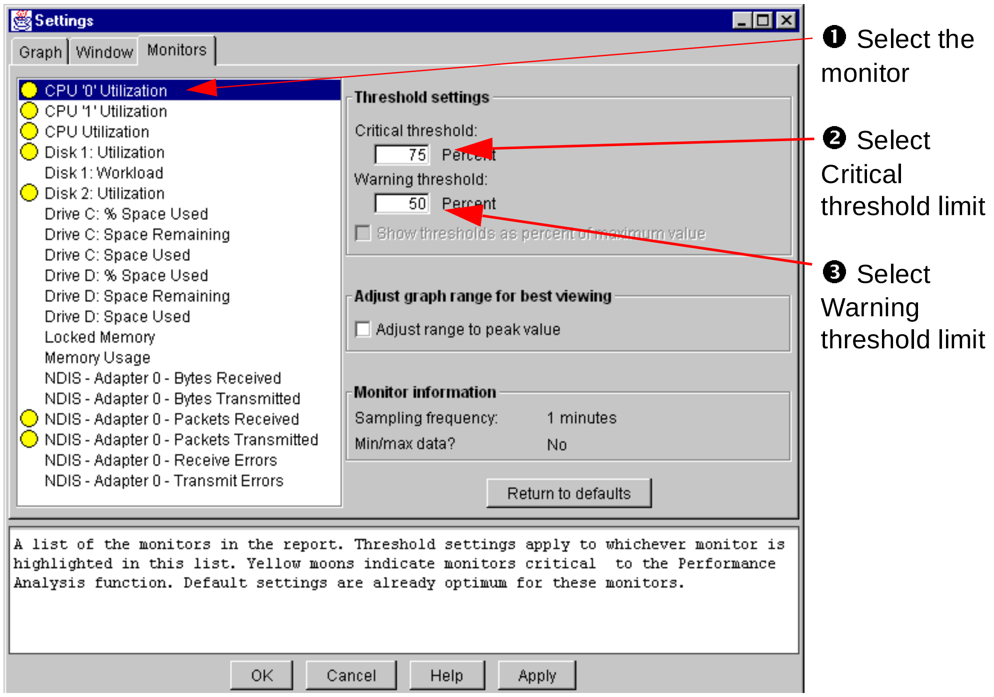
You can adjust the space each pane takes up on the screen by dragging the border between two panes with the mouse.

6.6.1 Setting Thresholds

You may find it useful to set thresholds for particular monitors. Capacity Manager lets you set a warning threshold, which it displays in yellow, and a critical threshold, which it displays in red.

The red and yellow markers appear in the System pane (both the HyperGraph and details views as described in 6.6.2, “The System Pane” on page 176) and in the Graph pane.

To set the thresholds, click ✏ **-> Settings -> Monitors**. Figure 136 appears:



Settings

- CPU '0' Utilization
- CPU '1' Utilization
- CPU Utilization
- Disk 1: Utilization
- Disk 1: Workload
- Disk 2: Utilization
- Drive C: % Space Used
- Drive C: Space Remaining
- Drive C: Space Used
- Drive D: % Space Used
- Drive D: Space Remaining
- Drive D: Space Used
- Locked Memory
- Memory Usage
- NDIS - Adapter 0 - Bytes Received
- NDIS - Adapter 0 - Bytes Transmitted
- NDIS - Adapter 0 - Packets Received
- NDIS - Adapter 0 - Packets Transmitted
- NDIS - Adapter 0 - Receive Errors
- NDIS - Adapter 0 - Transmit Errors

Threshold settings

Critical threshold: 75 Percent

Warning threshold: 50 Percent

□ Show thresholds as percent of maximum value

Adjust graph range for best viewing

□ Adjust range to peak value

Monitor information

Sampling frequency: 1 minutes

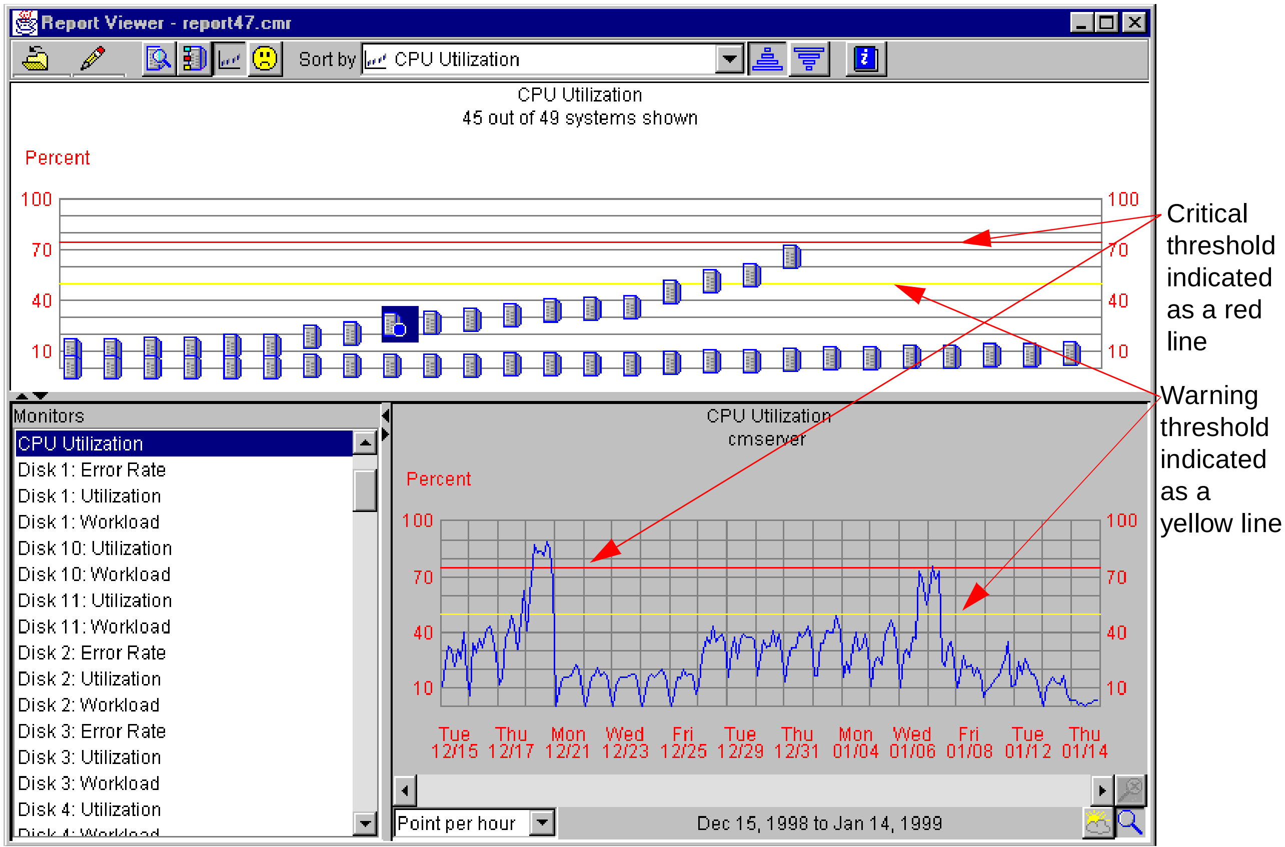
Min/max data? No

```
A list of the monitors in the report. Threshold settings apply to whichever monitor is
highlighted in this list. Yellow moons indicate monitors critical  to the Performance
Analysis function. Default settings are already optimum for these monitors.
```

OK
Cancel
Help
Apply
❶ Select the monitor
❷ Select Critical threshold limit
❸ Select Warning threshold limit

Figure 136. Selecting Threshold Limits

When you set the thresholds, you will see markers in both the System pane and the Graph pane as shown in Figure 137:



Report Viewer - report47.cmr

Sort by CPU Utilization

Figure 137. Warning (Yellow) and Critical (Red) Thresholds

6.6.2 The System Pane

The System pane underneath the toolbar shows the systems you have chosen in your report. There are four ways of viewing the systems in the system pane:

- Details view, the default
- Icon view
- HyperGraph view
- Performance Analysis

These choices are available from the **Edit** menu or the toolbar icons as shown in Figure 138:

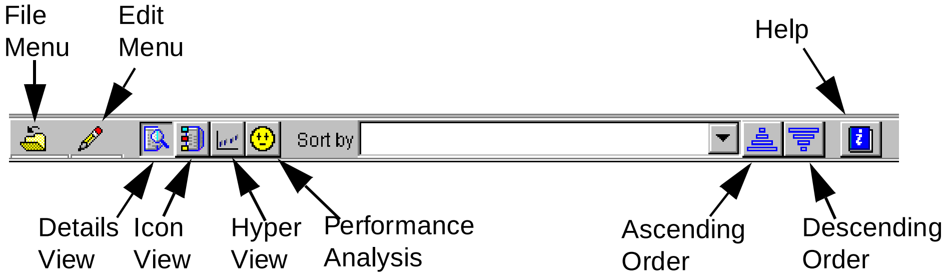


Figure 138. View Buttons

You can select one or more systems in the System pane. Doing so assigns a colored circle, triangle or square to each system that acts as the legend for the display in the Graph pane. This allows you to distinguish between systems when you have multiple systems selected.

You select more than one system using either the Shift or Ctrl keys.

6.6.2.1 Details View

The details view, shown in Figure 135 on page 174, lists the average values for all of the monitors you have selected plus system information parameters such as bus type and processor speed. The monitors are also repeated in the Monitor pane.

If you click one of the monitor values for a particular system, the Graph pane will automatically display that monitor for that system.

You will notice in Figure 135 on page 174 that there are dashes instead of values for monitors of some systems. This is because that particular monitor is not relevant or not available for that particular system. An example of this is “Disk 2: Error Rate” for system WTRAS1 per Figure 135 on page 174. This is because WTRAS1 does not have a disk 2.

You may also see a question mark against some monitors for some systems. If, for example, a system has just been installed and has not collected enough data points for the requested period, then you would see a “?” instead of the average value in the view. You may also get a “?” if the SLT file is corrupted.

There are also a number of adjustments that can be made to the way the information is displayed in the details view:

- Sorting by column

You can sort the systems by any of the columns in the details view by selecting from the **Sort By** drop-down menu. You can also click the Ascending or Descending buttons sort order to adjust the way the systems are displayed.

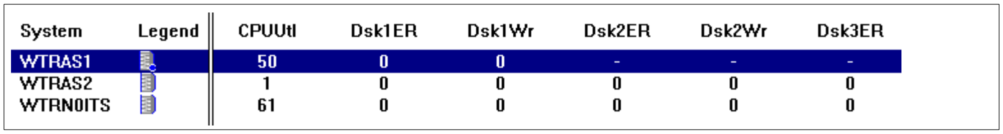
- Changing the size of the legend icon

  By default, the details view shows large icons, which means that only a few systems are visible without vertically scrolling the display. You can set small icons by clicking **View -> Settings -> Window** and checking **Use small icons for systems**.

- Shortening the column titles

  By default, the full monitor name or system parameter name is displayed at the top of each column in the details view. This means that you have to scroll horizontally to see all the monitor values. You can specify that only an abbreviation of the column heading be used by clicking **View -> Settings -> Window**, checking **Abbreviate column headings** then specifying the number of abbreviated characters.

  Figure 139 shows both small icons and abbreviated column headings for the same data shown in Figure 135 on page 174 (both figures show small headings).

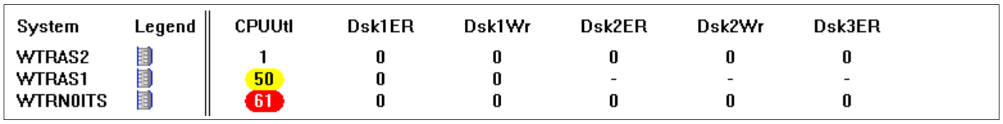


System	Legend	CPUUtl	Dsk1ER	Dsk1Wr	Dsk2ER	Dsk2Wr	Dsk3ER
WTRAS1	▤	50	0	0	-	-	-
WTRAS2	▤	1	0	0	0	0	0
WTRNOITS	▤	61	0	0	0	0	0

Figure 139. Small Icons and Abbreviated Column Headings

- Thresholds

  When you set warning and critical thresholds levels (as described in 6.6.1, “Setting Thresholds” on page 174), they will appear in the details view as yellow and red circles around the monitor values. For example, if we set a warning CPU threshold at 50% and a critical one at 60%, then Figure 140 on page 177 will appear:



System	Legend	CPUUtl	Dsk1ER	Dsk1Wr	Dsk2ER	Dsk2Wr	Dsk3ER
WTRAS2	▤	1	0	0	0	0	0
WTRAS1	▤	50	0	0	-	-	-
WTRNOITS	▤	61	0	0	0	0	0

Figure 140. Warning (Yellow) and Critical (Red) Thresholds

6.6.2.2 Icon View

Clicking the **Icon View** button on the toolbar converts the System pane into a view just showing the names of the systems, such as in Figure 141 on page 177. This view is useful when you have a lot of systems to display and you are interested only in the Graph pane.

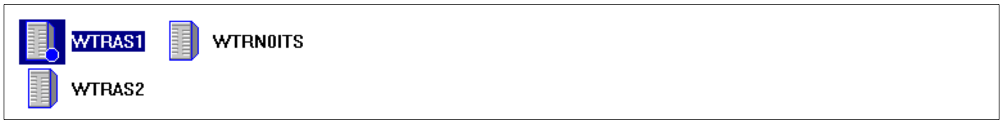


Figure 141. Icon View (Large Icons)

6.6.2.3 HyperGraph View

The HyperGraph view displays average values of the selected monitor for all the systems in the report. If you click the **Descending** button, those systems with the highest average value will be at the top of the report. If you click the **Ascending** button, those systems with the lowest average value will be at the top of the report.

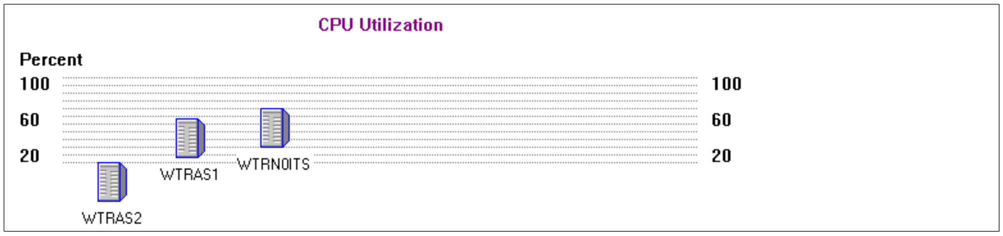


Figure 142. HyperGraph View

The tops of the icons mark the values being displayed. If you have defined thresholds, then they will appear as horizontal lines in the HyperGraph view.

Tip: You can change the height of the System pane by dragging down the border between it and the other two panes.

6.6.2.4 Performance Analysis

This new function lets you analyze your system for bottlenecks and offers possible ways to improve performance. See 6.7, “Performance Analysis” on page 181 for more details.

6.6.3 The Monitor Pane

The Monitor pane in the lower left-hand side of the Report Viewer window (Figure 135 on page 174) lists the monitors you have chosen in the Report Generator. All the monitors that apply to *any* of the systems you selected will be displayed on the screen.

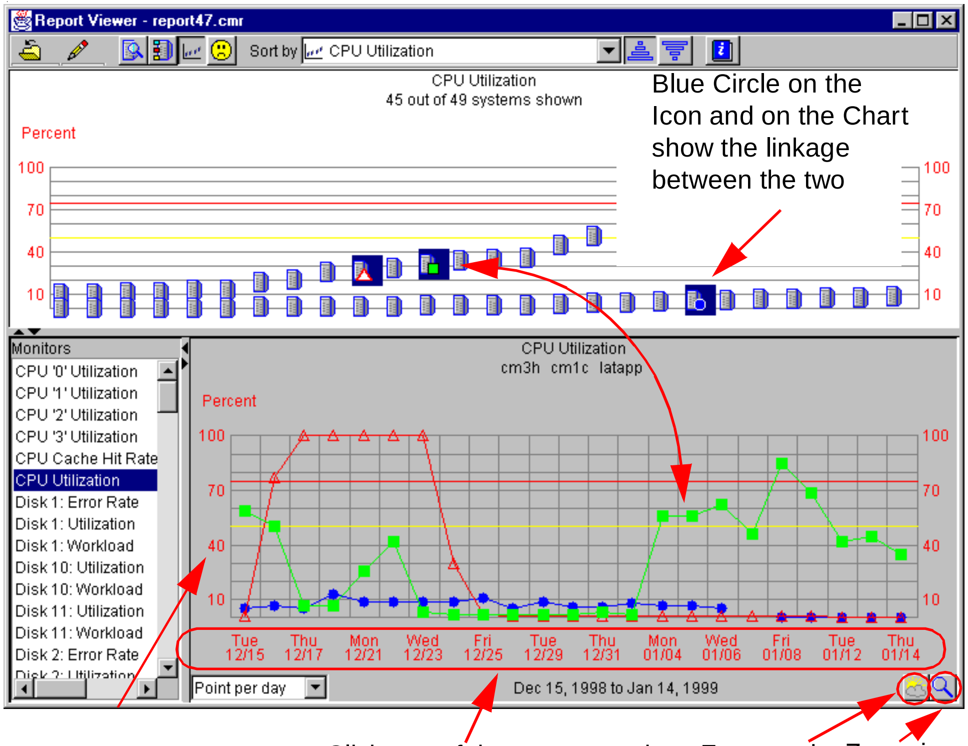
You can select only one monitor at a time. The monitor you select is displayed in graphical format in the Graph pane for the systems you’ve selected in the System pane.

6.6.4 The Graph Pane

The lower right-hand side of the Report Viewer window is the Graph pane (see Figure 135 on page 174). To make the graph larger, select the edge of the pane with your mouse and drag the panel up.

To display data on the graph, select a monitor from the Monitor pane, then one or more systems from the System pane (select more than one system with the Shift or Ctrl keys).

Figure 143 shows the CPU Utilization monitor selected and three systems selected:



Blue Circle on the Icon and on the Chart show the linkage between the two

Specify how many data points to display

Click any of these to zoom in to that time period

Forecast is available

Zoom is available

Figure 143. CPU Utilization of Multiple Systems

If you have three systems selected, your graph should now show three lines (blue, green and dotted red as shown in Figure 143). To change the time scale, select a new value in the **Point per** drop-down list box in the lower right portion of the graph. This will show more data on the screen but may make it too cluttered if you have many systems displayed.

You can show a legend box showing the names of each of the lines in the graph. To do so, click **View -> Settings -> Graph** then check **Show the legend**.

6.6.4.1 Forecast

The forecast function allows you to see Capacity Manager's prediction of the performance of your selected systems. See 6.7.4, "Forecast" on page 185 for more information.

6.6.4.2 Zoom

To look more closely at a particular time period, use the zoom function, represented by a magnifying glass in the bottom-right corner of Figure 143. Flyover help will tell you when zoom is available.

If zoom is available, you can click any of the time periods on the x-axis of the graph. This will then expand that time period to the full graph allowing you to see much more detail. You may be able to zoom multiple times, depending on the report you generated.

If you do not zoom in, then the data that is displayed at each time period is the average of the values for that period.

You can return to the previous state by clicking the **Zoom undo** icon (which will appear in the bottom-right corner) or by right-clicking the x-axis. You can scroll forward and backward to earlier or later times by selecting the arrow keys surrounding the Zoom undo icon.

6.6.4.3 Showing Minimum and Maximum Values

As stated in 6.6.4.2, "Zoom" on page 179, if you do not zoom in, then the data that is displayed at each time period is the average of the values for that period.

When you have only one system selected, you can also display the minimum and maximum values in this situation by clicking **View -> Settings -> Graph** then clicking **Show minimum and maximum lines when averaging**. This will show a red line for the maximum value within that time period and a green line for the minimum value within that time period.

An example is shown in Figure 144.

Warning

If you wish to display minimum and maximum values in the Report Viewer, we strongly recommend you first turn on the collection of min/max data in the report definition file (6.5.1, "Step 1: Report Definition" on page 165). If you don't collect the min/max data but choose to display the min/max values anyway, then the graphs displayed will be approximations based on incomplete data and are likely to be inaccurate.

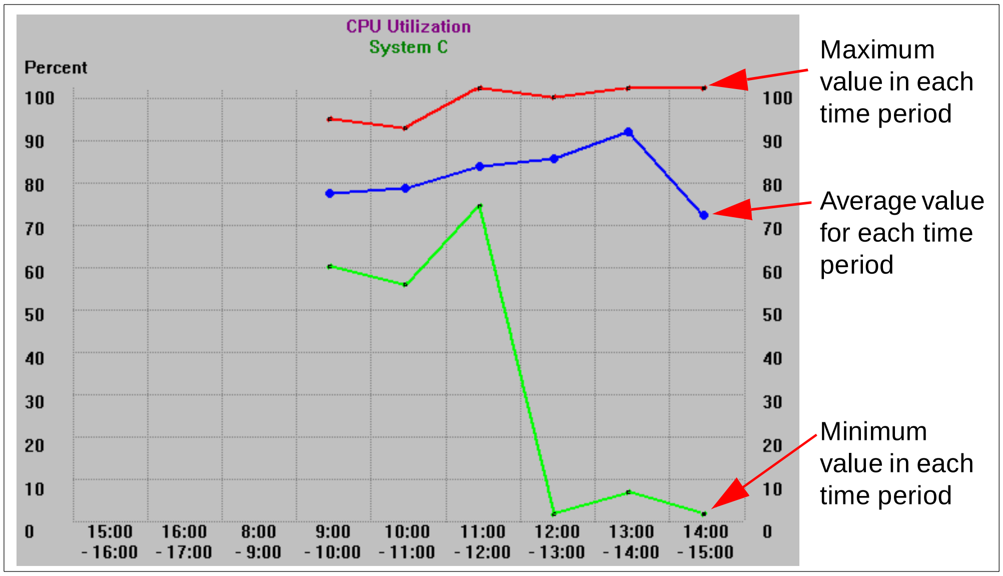


Figure 144. Minimum and Maximum Values

Note: Minimum and maximum values do not appear if you have more than one system selected nor do they appear when you are at the maximum zoom level.

6.6.4.4 Trend Graph

For small numbers of systems, it is appropriate to show a line on the graph for each system. However, with large systems, this can become unmanageable. To compensate for this, Capacity Manager can be configured to group all systems into one graph line and show minimum and maximum values for that time period for all systems. This is shown in Figure 145 on page 181:

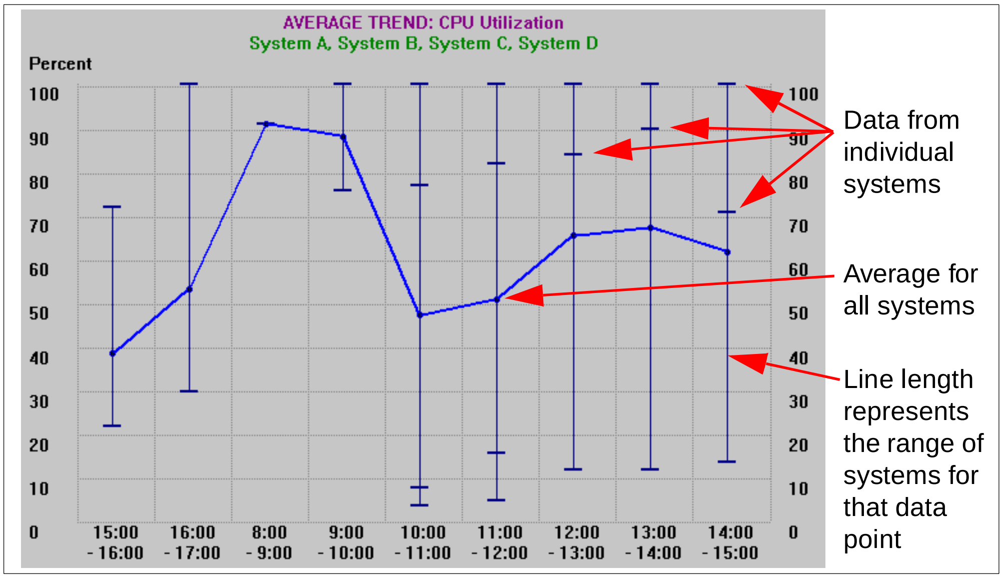


Figure 145. A Sample Trend Graph

The trend graphs plot the average value of the selected monitor for all of the systems you have chosen.

For each time period, there is a vertical line:

- Data from individual systems is represented as dashes.
- The length of the vertical line represents the range of all the selected systems' utilization data points.
- Clusters of points on the line represent concentration of data.

Capacity Manager will automatically switch a graph to a trend graph when the number of systems selected exceeds a specified number. That number is set by clicking **View -> Settings -> Graph** and change the field **Maximum systems to graph individually**. The default is 3. Capacity Manager can graph up to nine systems on the chart at once. Any number above nine is automatically trended.

6.7 Performance Analysis

Performance analysis is a new feature added to Capacity Manager in Netfinity Manager V5.2 or later. The function probes for bottlenecks in server hardware performance, diagnoses the problem and suggests ways to improve performance. The Performance Analysis algorithm is based on practices of experts. The algorithm can find many but not all system problems. A minimum of a month's worth of data is needed to make accurate predictions.

The algorithm monitors four server functions:

- Memory
- Disk subsystem
- CPU subsystem
- LAN subsystem

All of the above except network utilization are required for generating a Performance Analysis report. While network utilization is not required, omitting it could mean that performance analysis will miss some system problems.

Currently, only Windows NT has all the required monitors, therefore, performance analysis is not available on other operating systems. Each of the above monitors has a critical threshold and a warning threshold, both of which are important to the performance of performance analysis.

6.7.1 Reports Produced

The report produced by the Performance Analysis function consists of two main sections:

- Recommendations: a summary of the actions that are recommended
- Details: all analysis results

A bottleneck that is reported in the details section will appear in the recommendations section if it meets one of the following criteria:

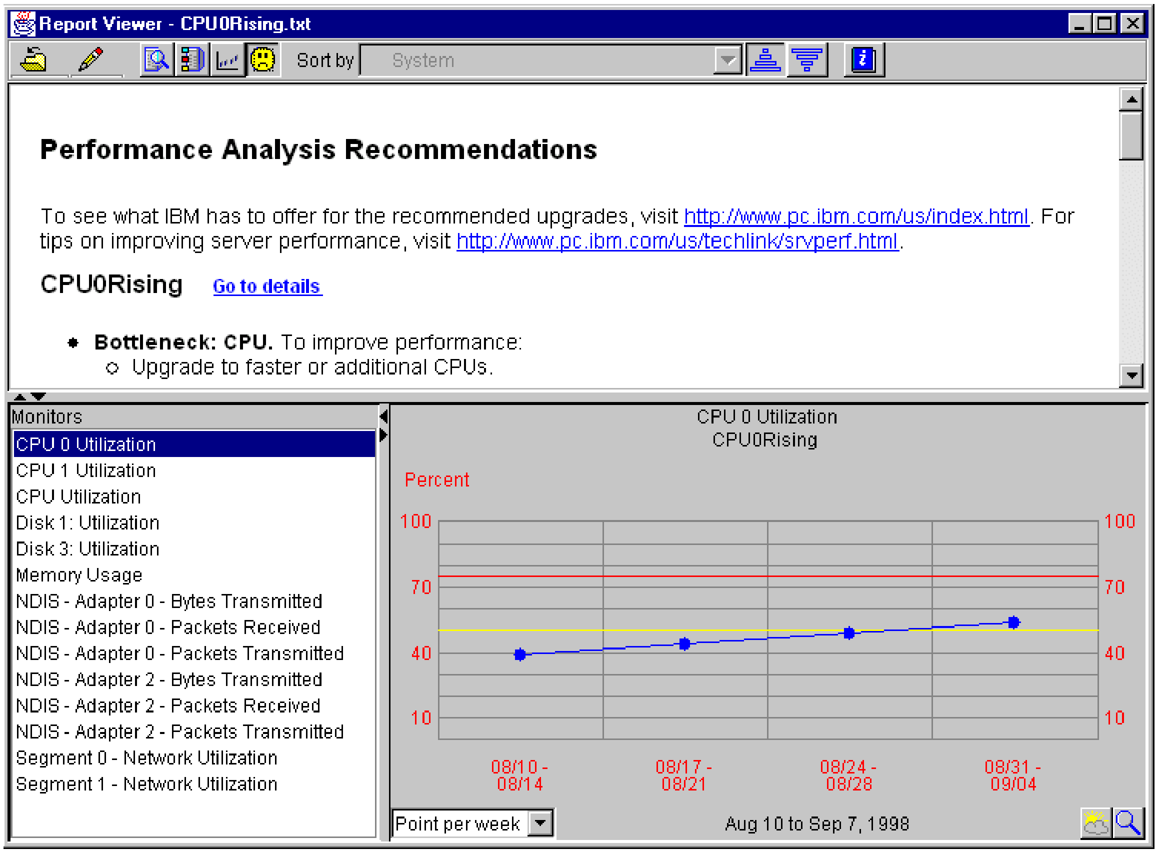
- It occurred on the last day of the report.
- It occurred more than 25% of the time, plus it occurred more than any other bottleneck for that particular system.
- It appears that it will occur in the future; this prediction is based on Performance Analysis having enough data for the system to make a reliable forecast.

The Performance Analysis function button appears as one of four icons as shown in Table 37, each of which represents a different meaning:

Table 37. Performance Analysis Buttons

Icon	Meaning
🙂	The Performance Analysis report is ready. There are no bottlenecks listed in the Recommendations section, but some may be listed in the Details section.
😑	The Performance Analysis report is still being prepared.
😵	The Performance Analysis report could not be prepared because you are missing one or more critical monitors.
☹	The Performance Analysis report is not ready, and you have system bottlenecks discussed in Recommendations.

To see the results of the Performance Analysis on your data, click the button that appears on the toolbar (Table 37). A window similar to Figure 146 appears. The Performance Analysis report is available online and as an HTML file.



Sort by: System

Performance Analysis Recommendations

To see what IBM has to offer for the recommended upgrades, visit http://www.pc.ibm.com/us/index.html. For tips on improving server performance, visit http://www.pc.ibm.com/us/techlink/srvperf.html.

CPU0Rising   Go to details

- **Bottleneck: CPU.** To improve performance:
  - Upgrade to faster or additional CPUs.

Monitors

- CPU 0 Utilization
- CPU 1 Utilization
- CPU Utilization
- Disk 1: Utilization
- Disk 3: Utilization
- Memory Usage
- NDIS - Adapter 0 - Bytes Transmitted
- NDIS - Adapter 0 - Packets Received
- NDIS - Adapter 0 - Packets Transmitted
- NDIS - Adapter 2 - Bytes Transmitted
- NDIS - Adapter 2 - Packets Received
- NDIS - Adapter 2 - Packets Transmitted
- Segment 0 - Network Utilization
- Segment 1 - Network Utilization

Figure 146. Performance Analysis Report

The report presents the bottleneck information first as a summary of the recommendations, then in a more detailed format. It also has links to the supporting graphic data. Keep in mind that bottleneck detection and analysis are complicated. If a monitor seems to be missing in one bottleneck, it may be because it is contributing to another one.

The report can also be saved to disk. Four files are created (where x is the file name the user specifies when saving):

- An x.HTML file that contains links to the Performance Analysis view information, the report information and the table view information.
- An xANALYSIS.HTML file contains the Performance Analysis recommendations, which list remedies for the described bottlenecks and latent bottlenecks.
- An xINFORMATION.HTML file covers the report information, which includes the file name, the analysis start and end dates, days of the week and hours of coverage. Any systems not included are listed at the bottom.
- The xTABLE.HTML file includes the same system and monitor data, which is available in the report viewer's table view. You may bring this file up in a spreadsheet as well as in a Web browser, but it prints better from a spreadsheet.

6.7.2 Types of Bottlenecks

Bottlenecks are detected when one or more monitors exceed a programmed threshold setting for an extended period of time. You can adjust these threshold settings, but the default settings, particularly those that are critical for the integrity of the Performance Analysis, are best not changed.

- Bottlenecks

  A bottleneck that is currently happening is sometimes called a realized bottleneck or just a bottleneck. A bottleneck occurs on a system when one or more devices are constrained.

- Latent Bottlenecks

  Often when you fix one bottleneck, there will be another waiting to happen, but it did not occur because the system was slowed down by the first bottleneck. If one or more of a device's monitors are above the warning threshold while another device is constrained, it is considered a latent bottleneck.

- Forecasted Bottlenecks

  The Performance Analysis algorithm scans for bottlenecks on each system. If no bottlenecks are found for a given system, then Performance Analysis scans forward, using the forecasted graph.

  The forecast is the same length as the report period. For example, a report period of one month can have a forecast of one month into the future. The forecast is used only if no bottlenecks are found in the real data. Only the first bottleneck that is found in the forecast is reported.

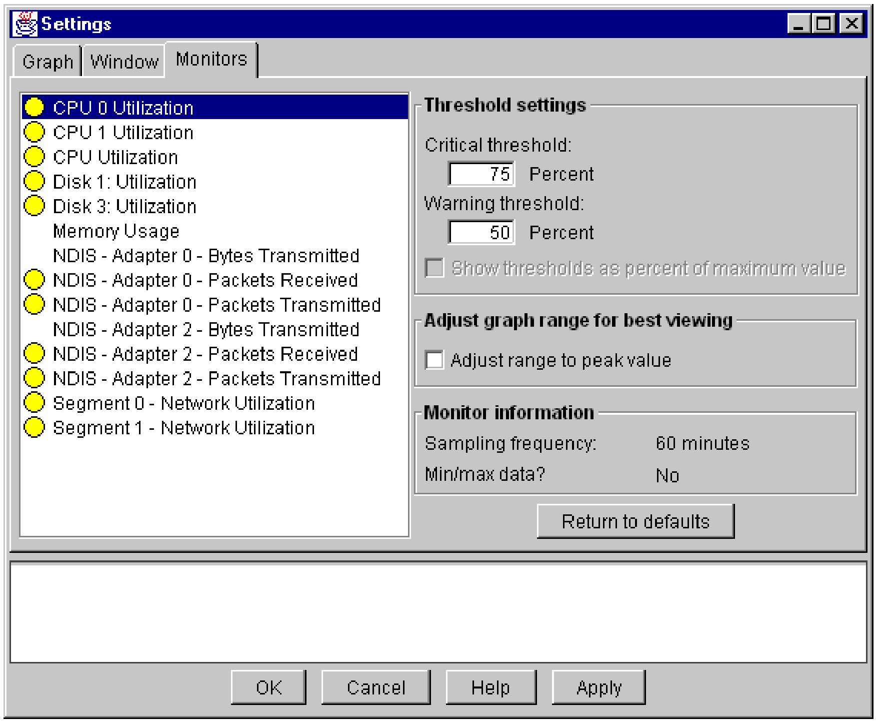
6.7.3 Setting Critical and Warning Threshold Values

The report viewer provides two thresholds, warning (yellow) and critical (red), used to determine quickly which systems exceed preferred levels. These threshold values appear in three places: as red and yellow cells in table view, as red and yellow lines on the hypergraph and on the graphs in the graph pane, and in the function of performance analysis.

Warning: Several of the monitors listed in the monitor window have a yellow moon beside them. The threshold settings for these monitors are critical to the optimum function of the performance analysis. If you change the threshold settings for these monitors, the effect on performance analysis will be unpredictable.

To set the Warning and Critical thresholds:

Click ✏
Click **Settings**
Click the **Monitors** tab. Figure 147 appears:



- CPU 0 Utilization
- CPU 1 Utilization
- CPU Utilization
- Disk 1: Utilization
- Disk 3: Utilization
- Memory Usage
- NDIS - Adapter 0 - Bytes Transmitted
- NDIS - Adapter 0 - Packets Received
- NDIS - Adapter 0 - Packets Transmitted
- NDIS - Adapter 2 - Bytes Transmitted
- NDIS - Adapter 2 - Packets Received
- NDIS - Adapter 2 - Packets Transmitted
- Segment 0 - Network Utilization
- Segment 1 - Network Utilization

Threshold settings

Critical threshold: 75 Percent

Warning threshold: 50 Percent

□ Show thresholds as percent of maximum value

Adjust graph range for best viewing

□ Adjust range to peak value

Monitor information

Sampling frequency:	60 minutes
Min/max data?	No

Figure 147. Threshold Settings

When you are at the Monitor screen you will see the monitors listed in box to the left and the input boxes for the threshold settings to the right. Help for a setting is displayed in the area at the bottom. Click a monitor in the box then enter a value into the Critical threshold or Warning threshold field.

Note: When setting Critical and Warning thresholds for the monitors, some monitor thresholds are expressed as a percent, and some have an alternative setting, such as megabytes free or packets/sec. When an alternative setting is available, the box labeled “Show thresholds as percent of maximum value” will be available. Decide which units are most appropriate for your threshold settings, and select or clear the box as appropriate.

To return other monitors to their default settings click the **Return to defaults** button. Only your currently selected monitor will be reset to its default threshold settings, the other monitors will be unaffected. Repeat for each monitor that you want to return to its default settings.

6.7.4 Forecast

The forecast function is available by clicking the ⛅ button while viewing the Capacity Manager report. The function allows you to see Capacity Manager's prediction of the future performance of your selected systems.

To create its forecast, Capacity Manager uses a linear regression based on a least squares fit with a confidence interval of 95%. For the forecast to be valid, Capacity Manager needs a minimum of 21 days of previously collected data where the system monitors have been running at least 50% of the time.

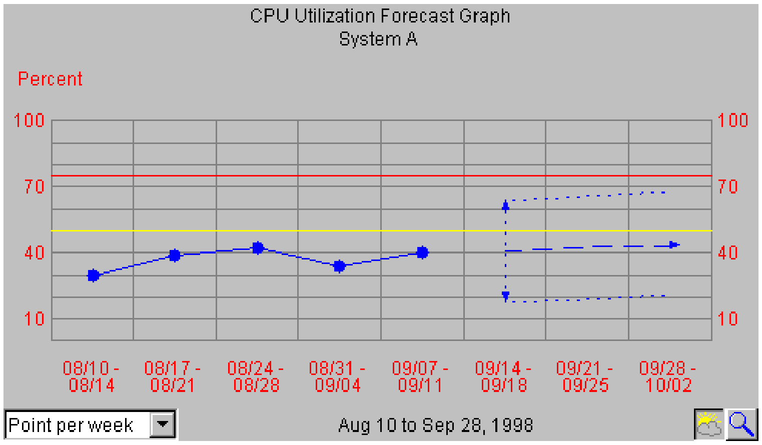


Figure 148. Forecast Graph

To see the forecast for your selected systems, click the **Forecast** icon in the lower-right corner of the screen. A graph similar to Figure 148 appears. The forecast is for whatever monitor you currently have selected. To see a forecast for another monitor, click its name in the monitor box.

Note: You cannot use both Zoom and Forecast at the same time; they are mutually exclusive such that one is turned off when the other is turned on.

The forecast line is a dashed line with an arrow at the end. The forecast interval is a multiple of your data collection period. The default prediction period is set to the same length as the data collection period. For example, if you have a month of collected data, the forecast will be for a month into the future.

The confidence interval is represented by the dotted lines above and below the forecast line. The vertical bar at the beginning of the forecast data depicts the range. The gap between the actual collected data and the beginning of the predicted data serves as a separator between these two data sets.

Capacity Manager will display one of two warnings if your forecast is not valid. Invalid forecasts should not be used to make decisions about your systems.

- “Data collection period too short for a valid forecast.” To generate a valid forecast, you need at least 21 days of data.
- “System 'X' does not have enough data for forecasting”, or “Multiple systems do not have enough data for forecasting.” One of these two messages will appear when you have a sufficiently long period for data collection, but one or more monitors were not on for at least 50% of the time during the data collection period.

Note: The forecast is more meaningful for individually graphed systems than for those shown in a trend graph. To change your graph from a trend graph to a graph of individual systems, either set your trend graph threshold to a higher number or select fewer systems to graph at one time.

6.8 Scheduling a Report

You can schedule a report to be generated later by using the Report Scheduler. In the following section, we will discuss the three steps involved in using the Report Scheduler:

1. Use Netfinity Manager Scheduler to select systems.
2. Define the report to use with Report Generator.
3. Schedule times and dates with Netfinity Manager.

Unlike other methods of gathering data, you do not have to have the keyword SVC:CAPMGT specified. If you don't use SVC:CAPMGT, you will still get the following message, but you can click **OK** and continue:

```
There are no Netfinity system groups defined for Capacity Management
(keyword SVC:CAPMGT).  Open the Remote System Manager to set up the
appropriate groups and restart the Report Generator.  If you are generating
reports from the Event Scheduler, you may proceed.  See Report Generator
help for more information.
```

Before you can proceed you must have one or more Netfinity Manager groups defined with the SVC:CAPMGT keyword and the necessary security to access the remote systems you want. See 6.3, "Before You Begin" on page 158 for details.

6.8.1 Step 1: Selecting Systems

Click the **Schedule** button from the Capacity Manager main window. Figure 149 appears:

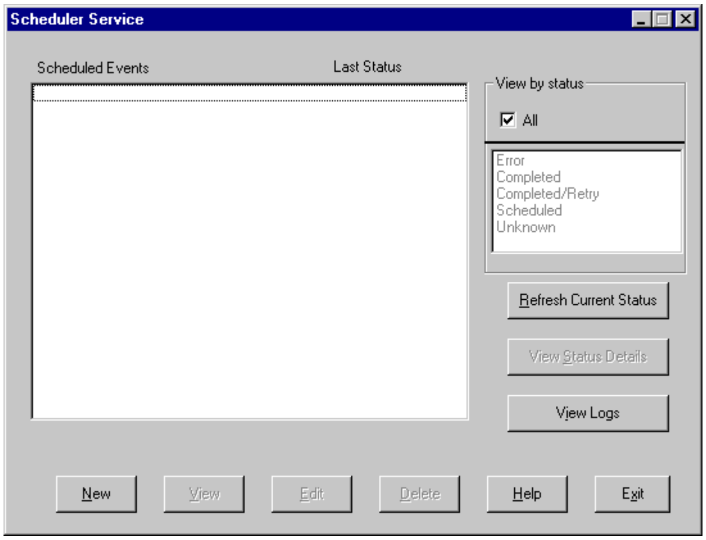
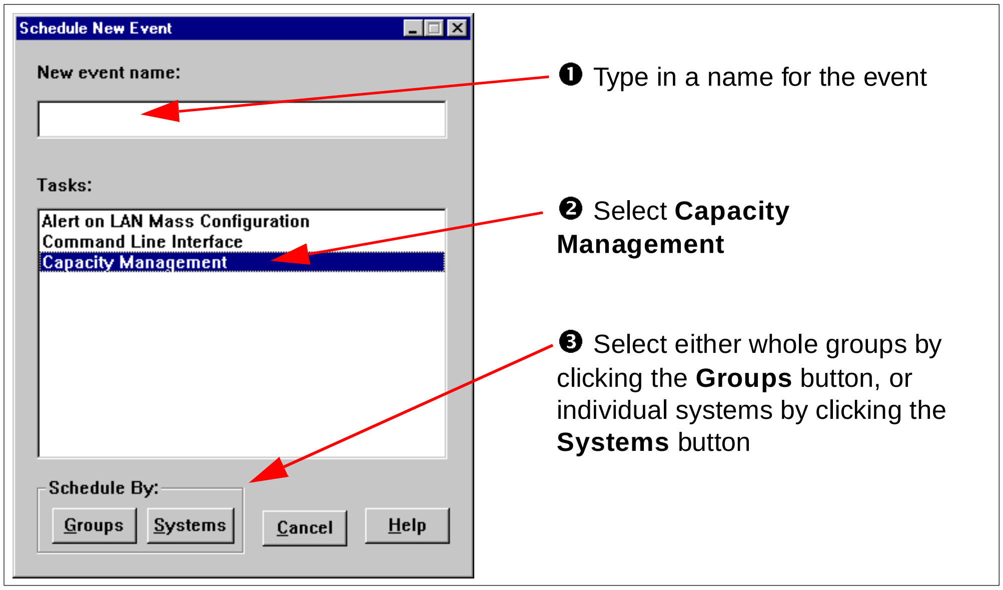


Figure 149. Netfinity Manager Scheduler Service

This window is the Event Scheduler function of Netfinity Manager. Click on **New** to create a new event. Figure 150 appears:



❶ Type in a name for the event

❷ Select **Capacity Management**

❸ Select either whole groups by clicking the **Groups** button, or individual systems by clicking the **Systems** button

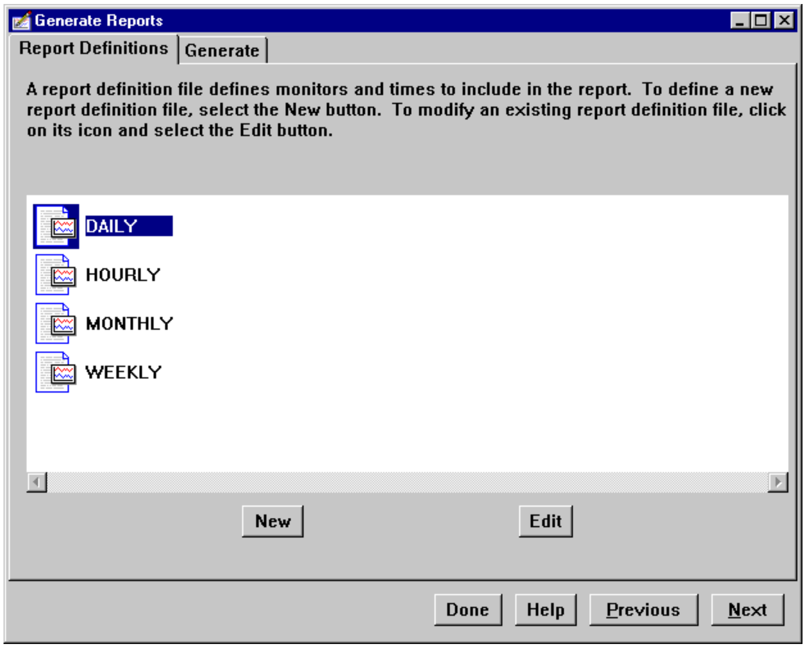
Figure 150. Selecting Systems

Type in the name of the new event, then select **Capacity Management**, then select the systems by clicking either **Groups** or **Systems**. If you want to select all systems in a group, then click **Groups**. If you want to select individual systems from one or more groups, click **Systems**.

Once you have selected the systems you want, click the **Schedule** button.

6.8.2 Step 2: Define the Report

At this point, you will see Figure 151 on page 188 where you can either select or edit an existing Capacity Manager report or you can create a new report. This is the same as previously discussed in 6.5.1, “Step 1: Report Definition” on page 165.



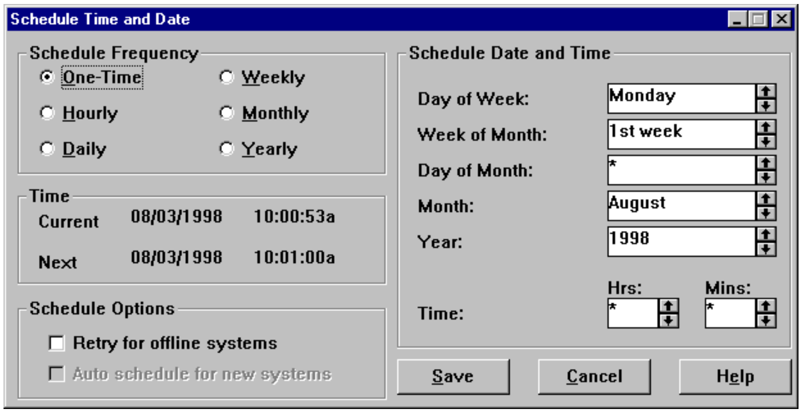
A report definition file defines monitors and times to include in the report. To define a new report definition file, select the New button. To modify an existing report definition file, click on its icon and select the Edit button.

Figure 151. Selecting the Report for the Schedule

Once you select the report, you can click the **Next** button or the **Generate** tab to change the file name for the report and the timeout setting. Once you are finished, click the **Done** button. Figure 152 appears.

6.8.3 Step 3: Scheduling the Time and Date

Now you need to specify when the event is to occur.


Schedule Time and Date

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

Time
Current 08/03/1998 10:00:53a
Next 08/03/1998 10:01:00a

Schedule Options
□ Retry for offline systems
□ Auto schedule for new systems

Schedule Date and Time
Day of Week: Monday
Week of Month: 1st week
Day of Month: *
Month: August
Year: 1998
Time: Hrs: * Mins: *

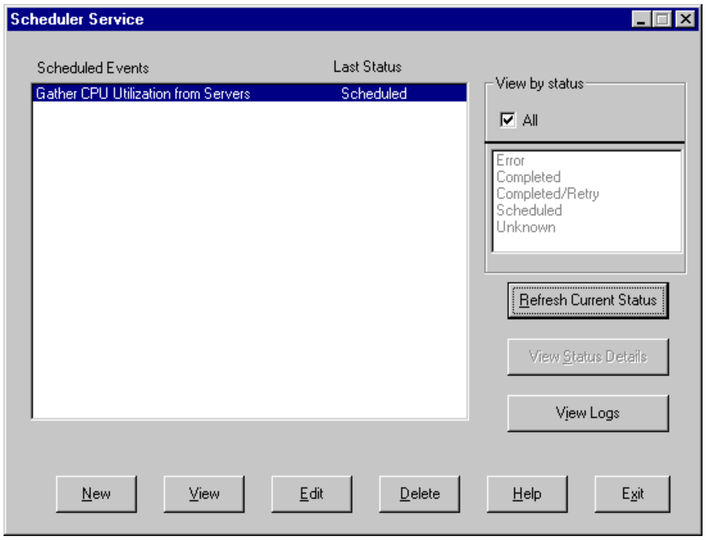
Figure 152. Schedule Time and Date

After you work with the Capacity Management report definition files, you can schedule the time and date for reports to be generated. Using the Netfinity Schedule Time and Date window, you can set specific time and date intervals for your reports to be created, such as:

- Frequency of reports to be generated, such as hourly, daily, or weekly
- Date and time settings
- Schedule options

The time settings should default to today's date and time.

Once you are finished with these settings, click the **Save** button. At this point you will see the status window (Figure 153) where you can monitor the scheduled event:


Scheduler Service

Scheduled Events	Last Status
Gather CPU Utilization from Servers	Scheduled

View by status
☑ All

Error
Completed
Completed/Retry
Scheduled
Unknown

Figure 153. Scheduler Status with Our Event Scheduled

Once the event has been completed, the status window will list it as Completed. You can then click the **View** button in the Capacity Manager main window to examine the report that was generated per 6.6, “Viewing a Report” on page 174.

6.9 CMMERGE

CMMERGE is a command-line program in the \WNETFIN directory where you install Netfinity Manager. It has two functions:

1. A command-line version of the Report Generator (the Report Generator is described in 6.5, “Generating a Report Immediately” on page 164).
2. Merge multiple CMR files together to produce one CMR file or convert a CMR file to a tab-delimited TXT file.

The syntax and limitations of these two functions are different from each other. Each is now described in detail.

6.9.1 Command-Line Report Generator

The syntax of CMMERGE when using it as a command-line version of the Report Generator is as follows:

```
CMMERGE [/options] OutputFile.CMR ReportDefFile.MON [group | /s:system
[/s:system ...]]
```

The parameters of CMMERGE when used in this way are:

OutputFile

OutputFile is the CMR (Capacity Manager Report) file that will be created. If you don’t specify an extension for OutputFile, it defaults to .CMR.

The CMR file will be saved in the REPORTS subdirectory of the *current* directory (that is, from where you run CMMERGE) and you cannot specify any other path. If the REPORTS subdirectory doesn’t already exist it will automatically be created. If you do specify a path, CMMERGE will hang and you will have to press Ctrl-C or Ctrl-Break to terminate it.

If the CMR file already exists, then a two-digit number will be appended to the end of the file name. For example, if you specify OUTPUT.CMR and that file already exists, then OUTPUT01.CMR, OUTPUT02.CMR and so on, will be used instead.

ReportDefFile

ReportDefFile is the name of the MON file that describes what monitors to gather from the systems requested. You must type in the .MON file extension. The MON file must be stored in the MONFILES subdirectory where Netfinity Manager is installed and you cannot specify any path. If you specify a path, CMMERGE will return an error message.

The MON file must already exist and you can use one of the predefined ones (Hourly.MON, Daily.MON, Weekly.MON and Monthly.MON as described in 6.5.1.2, “Predefined Reports” on page 170) or you can create a new MON file as described in 6.5.1.1, “Creating a New Report” on page 166.

Group

Group specifies the name of the Netfinity Manager you have defined to contain the systems from where you want data gathered. All systems in the group will be accessed. See 6.3.1, “Creating Capacity Manager Groups” on page 158 for details.

Note: The group you specify must have the special keyword `SVC:CAPMGT` (all capitals). If you don’t include the special keyword, CMMERGE will finish immediately with no results.

/s:system

/s:system specifies an individual system to gather data from rather than a whole group of systems. You can specify multiple /s:system options on the command line if you want to gather data from multiple individual systems. However each /s takes only one system. System is the value in the System Name field in the Network Driver Configuration window of Netfinity Manager. The system parameter is not case-sensitive.

Note: The system you specify must be part of at least one Netfinity Manager group with the special keyword `SVC:CAPMGT` (all capitals). If it is not, the CMMERGE command will finish immediately with no results.

Options

The options are:

/t:mm — sets the time to wait, in minutes (the default is 10 minutes).

/k — When you specify a group, this option saves (keeps) the report files from individual systems in a subdirectory of the REPORTS directory with the same name as the CMR file that was created.

/v — automatically invokes the Report Viewer to view the output file.

/w — displays the progress of gathering data in a window rather than in the Command Prompt console.

The options can appear anywhere on the command line, not just at the beginning.

6.9.2 Merging and Converting CMR Files

The syntax of CMMERGE when using it to merge multiple CMR files together or to convert CMR to TXT files is as follows:

```
CMMERGE [/options] OutputFile InputFile [InputFile ...]
```

You can merge only “like” CMR or TXT files. For example, you cannot merge two files with different days of the week recorded, or two files with different hours of the day recorded.

The parameters of CMMERGE when used in this way are:

OutputFile

OutputFile is the CMR (Capacity Manager Report) or TXT (tab-delimited text) file that will be created.

If you don't specify an extension for outputFile, it defaults to .CMR. If you don't specify a path, it will default to the current directory. If the OutputFile already exists (either CMR or TXT) it will be overwritten.

InputFile

You can specify one or more InputFiles. If you specify more than one, they are merged together. InputFiles can be either TXT (tab-delimited text, as created by CMMERGE) or CMR files. You can mix TXT and CMR files as inputs when merging.

The InputFiles must be in the current directory (that is, where you run CMMERGE from) and you cannot specify a path to them. If you don't specify a file extension it defaults to .CMR.

If you want to merge one CMR into a cumulative CMR file, you should specify the cumulative CMR file as both the OutputFile and one of the InputFiles. For examples:

```
CMMERGE ONGOING.CMR ONGOING.CMR MONTHLY.CMR
```

Options

The options are:

/v — automatically invokes the Report Viewer to view the output file.

/w — displays the progress of gathering data in a window rather than in the Command Prompt console.

6.10 Automatically Collecting Data Longer Than One Month

It is quite likely that you would want to continually gather data from your servers and continually grow the same .CMR report file so that you can work on long-term trend analysis.

We recommend the following process:

1. Set up the .MON report definition file to gather the monitors you want for an entire month.

   You may want to gather all monitors if you have plenty of disk space. As a rule of thumb, if you want to gather all monitors for a single Windows NT system for a month, the .CMR file will be about 1 MB in size.

   By default, Capacity Manager has four report definition files created: Hourly, Daily, Weekly and Monthly. Using the Report Generator, you can create either a new monthly report or simply edit the existing Monthly.MON file.

   See 6.5.1, "Step 1: Report Definition" on page 165 for details on how to edit or create a new report definition file. Write down the file name and directory where you save the MON file.

2. Set up a Netfinity Manager group to contain all the systems from which you want to gather data.

   See 6.3.1, "Creating Capacity Manager Groups" on page 158 for details.

Note: This process will gather data from *all* systems in the group, so once you create the group with the appropriate keywords, delete any systems from which you don’t want to gather data.

3. Set up a Netfinity Manager scheduled command to ERASE the MONTH.CMR file that is about to be created in Step 4.

   This needs to be done just before Step 4 (say at 11:20 p.m. on the first of the month) so that the CMR file name will be the same each time, and not MONTH01 or MONTH02 and so on.

4. Set up a Capacity Manager schedule to gather data from your systems at 11:30 p.m. on the first of every month to generate a monthly MONTH.CMR file.

   Note: Ensure you have the appropriate security access set up to let your system gather data from the servers. See 6.3.2, “Setting Netfinity Manager Security” on page 159 for details.

5. Set up a Netfinity Manager schedule to run CMMERGE at 11:45 p.m. on the first of every month to merge the monthly MONTH.CMR into the cumulative ONGOING.CMR file. See 6.9, “CMMERGE” on page 190 for details.

Chapter 7. Example Scenarios

This chapter provides a number of example scenarios that use the features of the servers, the Advanced System Management processor and adapters, and Netfinity Manager to maintain a high level of availability to users and to ensure that when down time occurs, it is kept to a minimum.

The following example scenarios are covered:

1. Air conditioning failure (Page 196) — using Netfinity Manager and the ASM processor in a Netfinity 5000 to notify when temperature thresholds have been exceeded and ultimately to shut down the server.
2. Drive failure in an array (Page 205) — 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 organization that a disk needs replacing.
3. Power failure (Page 215) — using Netfinity Manager and PowerChute on our UPS to notify when power to the server room fails. Shuts down the server if power is not restored within a certain time.
4. Power supply failure (Page 222) — uses the Advanced System Management PCI Adapter to notify when one of the redundant power supplies on a Netfinity 7000 M10 fails. The alert is transmitted via the Ethernet port of the adapter to a remote Netfinity Manager system.
5. Operating system hang (Page 225) — uses an ASM device and Netfinity Manager to notify when the operating system hangs. Also automatically restarts the server.
6. POST timeout and remote POST console (Page 229) — notifies if a timeout occurs and restarts the server if the POST process take too long to complete. Uses the remote POST console to view the POST process to perform problem determination.
7. Application failure and restart (Page 235) — uses Netfinity Manager to monitor an application and alert when it stops, then automatically restarts it.
8. Remote BIOS Update (Page 239) — uses Netfinity Manager and the Advanced System Management service to remotely flash the system BIOS of the Netfinity 5500.
9. Dial out via a modem and the RS-485 (Page 244) — describes how to configure a group of servers on an ASM interconnect bus so that they share a modem to send out alerts.
10. Rebooting a server via a Web browser (Page 250) — uses a Web browser to access a Netfinity 7000 M10 and a Netfinity 5000 via the ASM interconnect bus and then reboot the 5000.
11. Accessing a remote server’s POST via Telnet (Page 260) — uses a Telnet client to monitor the POST messages and to perform diagnostics on a remote Netfinity 7000 M10.

7.1 Example 1: Air Conditioner Failure

In this example, the air conditioning in the server room has failed. We have a Netfinity 5000 with an Advanced System Management Processor 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 38.

Table 38. 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
Danger	66°C	Power off the machine

Note: The values to which you set these thresholds will depend on the location and the environment in which your server is working. For example, if your server is in a chilled server room the temperature thresholds will be different from a regular office environment.

At the 40°C mark, we want the administtor to be paged with an information message. With the second event, the 50°C mark, we want him/her to be paged again with an error message. The final event will be at 65°C, which will power down the machine. The 65°C mark is hard-coded in the microcode in the ASM processor.

In this example the operating system choice should not make a difference.

These are the steps involved to set up the scenario:

1. Install the ASM device driver and Netfinity Manager

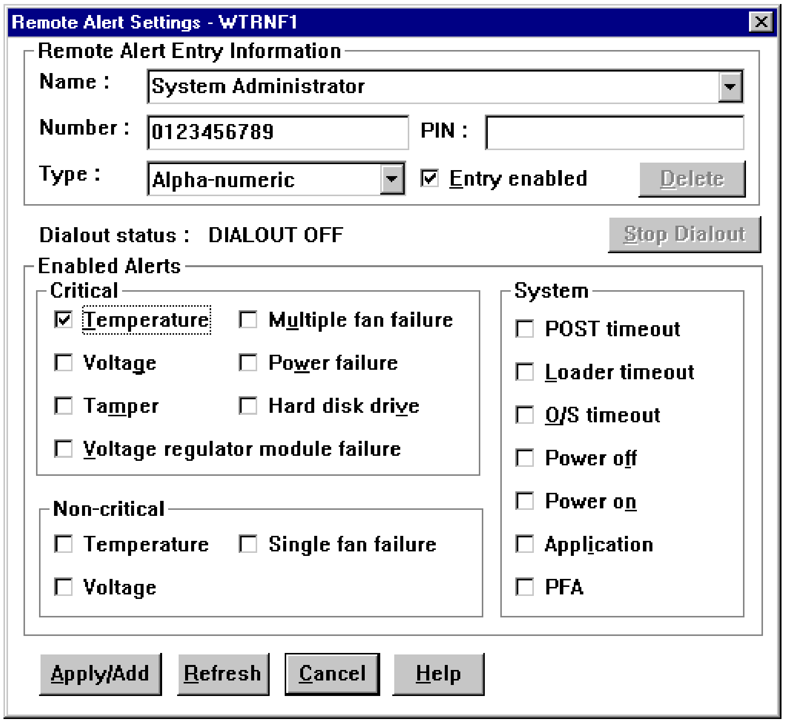
   Install the device driver before installing Netfinity Manager. If you do not install the driver first, Netfinity Manager will not be able to communicate with the ASM processor. See 2.2, “Installing Netfinity Manager” on page 6 for information on how to set up Netfinity Manager under your chosen operating system. Ensure you install Advanced System Management support.

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 up this example so that the modem is connected to Port 1 which is shared with the operating system as COM 1.

3. Configure the ASM processor

   Using the installed Netfinity Manager, configure the dialout settings for the service processor. When configuring the ASM processor, 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 154 and further details can be found in 4.2.6, “Remote Alert Settings” on page 117.



Remote Alert Entry Information

Name : System Administrator

Number : 0123456789 PIN :

Type : Alpha-numeric ☑ Entry enabled

Dialout status : DIALOUT OFF

Enabled Alerts

Critical

- ☑ Temperature
- ☐ Multiple fan failure
- ☐ Voltage
- ☐ Power failure
- ☐ Tamper
- ☐ Hard disk drive
- ☐ Voltage regulator module failure

Non-critical

- ☐ Temperature
- ☐ Single fan failure
- ☐ Voltage

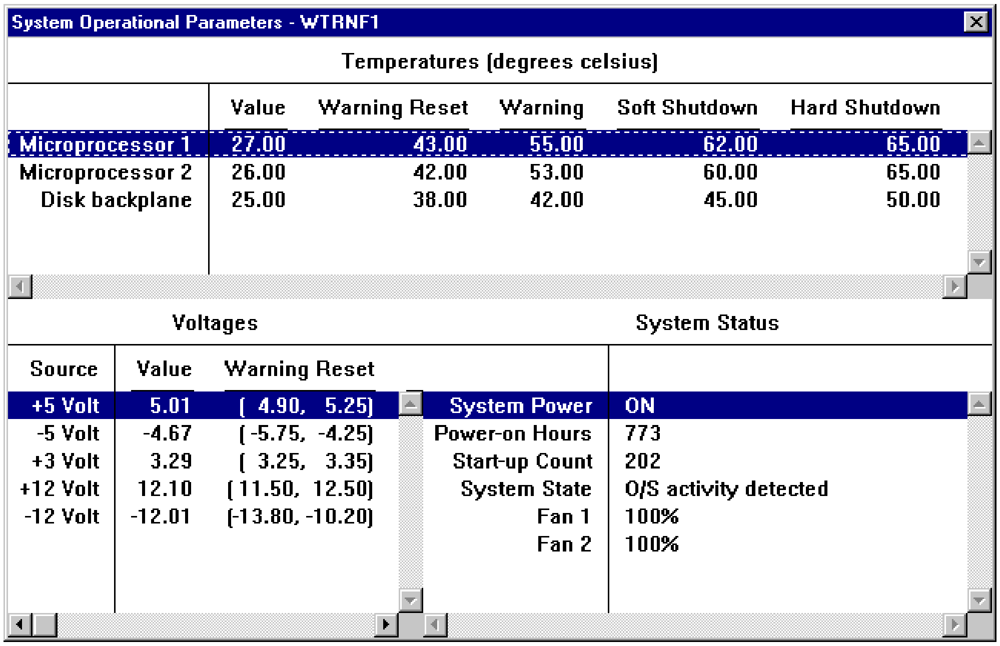
System

- ☐ POST timeout
- ☐ Loader timeout
- ☐ O/S timeout
- ☐ Power off
- ☐ Power on
- ☐ Application
- ☐ PFA

Figure 154. ASM Processor Dialout Settings

4. Configure System Monitor

   The ASM processor Operational Parameters window shows five temperature sensors on the server as shown in Figure 155. The ASM processor has a threshold associated with each of these temperature sensors. If the temperature exceeds any one of these thresholds for more than one minute then the system will be powered off by the processor.



Temperatures (degrees celsius)

	Value	Warning Reset	Warning	Soft Shutdown	Hard Shutdown
Microprocessor 1	27.00	43.00	55.00	62.00	65.00
Microprocessor 2	26.00	42.00	53.00	60.00	65.00
Disk backplane	25.00	38.00	42.00	45.00	50.00

Voltages

Source	Value	Warning Reset
+5 Volt	5.01	(4.90, 5.25)
-5 Volt	-4.67	(-5.75, -4.25)
+3 Volt	3.29	(3.25, 3.35)
+12 Volt	12.10	(11.50, 12.50)
-12 Volt	-12.01	(-13.80, -10.20)

System Status

System Power	ON
Power-on Hours	773
Start-up Count	202
System State	O/S activity detected
Fan 1	100%
Fan 2	100%

Figure 155. ASM Processor Operational Parameters

System Monitor will display two of these temperatures as monitors which you can set thresholds on:

– CPU 1 Area Temperature (Celsius or Fahrenheit)
– CPU 2 Area Temperature (Celsius or Fahrenheit)

5. Create a threshold for the system temperature

   The threshold can be set up for each of the monitors and allows you to set a limit, above which it will generate an alert. We use System Monitor to configure the thresholds per 7.1.1, “Configuring Thresholds” on page 198.

6. 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 7.1.2, “Configuring Actions” on page 200.

7.1.1 Configuring Thresholds

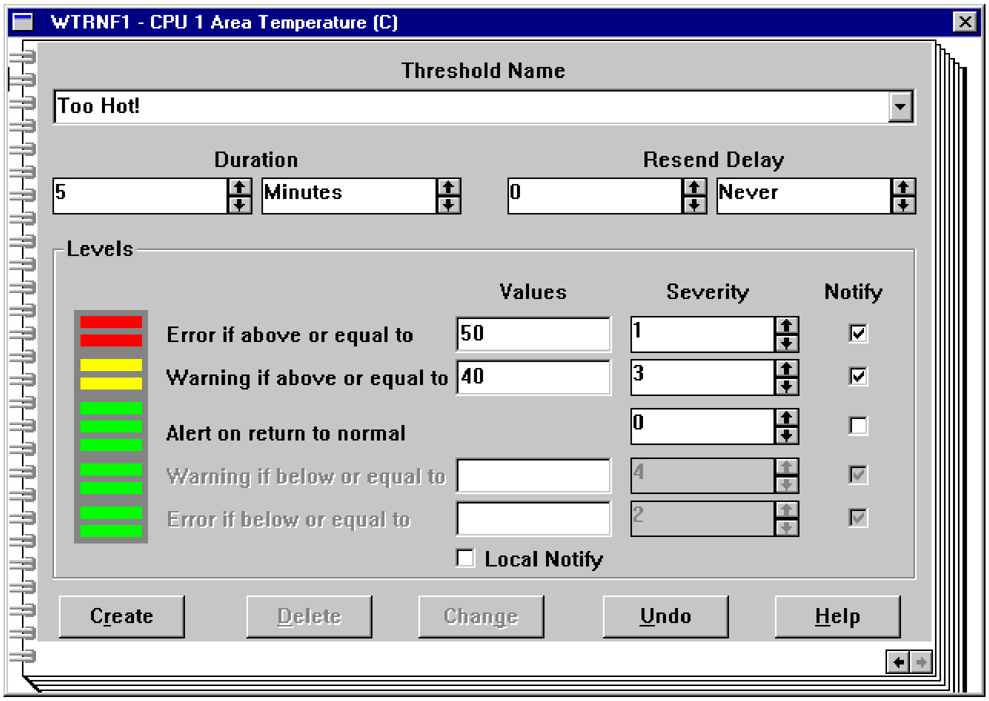
To configure the threshold in Netfinity Manager, complete the following steps:

1. Start System Monitor and select **Windows -> Show Monitors...** This will show a list of all the available monitors.

2. Select the **CPU 1 Area Temperature (C)** monitor and select **OK**.

   Note: If the temperature monitor is not in the list of available monitors, then it is likely you installed the ASM processor after you installed Netfinity Manager. You will need to reinstall Netfinity Manager.

3. Open the threshold settings window by either double-clicking the monitor or right-clicking the monitor and selecting **Open -> Threshold**. Figure 156 appears:



WTRNF1 - CPU 1 Area Temperature (C)

Threshold Name: Too Hot!

Duration: 5 Minutes

Resend Delay: 0 Never

Levels

	Values	Severity	Notify
Error if above or equal to	50	1	☑
Warning if above or equal to	40	3	☑
Alert on return to normal		0	□
Warning if below or equal to		4	☑
Error if below or equal to		2	☑

□ Local Notify

Figure 156. System Temperature Threshold Settings

You now need to configure the threshold, as shown in Figure 156.

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 156. For an example of how to use this see 7.7, “Example 7: Application Failure and Restart” on page 235.

   The **Local Notify** check box in Figure 156 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 its Alert Manager to respond to the alert), mark the **Local Notify** check box.

   We don’t use this option in this example. See 7.7, “Example 7: Application Failure and Restart” on page 235 for an example of when this is used.

10. Select alert on a return to normal temperature

    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** check box. We will not be using this option but it may be a useful item in your environment.

11. Save the threshold by clicking **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.

7.1.2 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 respond automatically 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 25 for more information on alerts and alert profiles.

7.1.2.1 Configuring Alert Profile

To configure the alert profiles do the following:

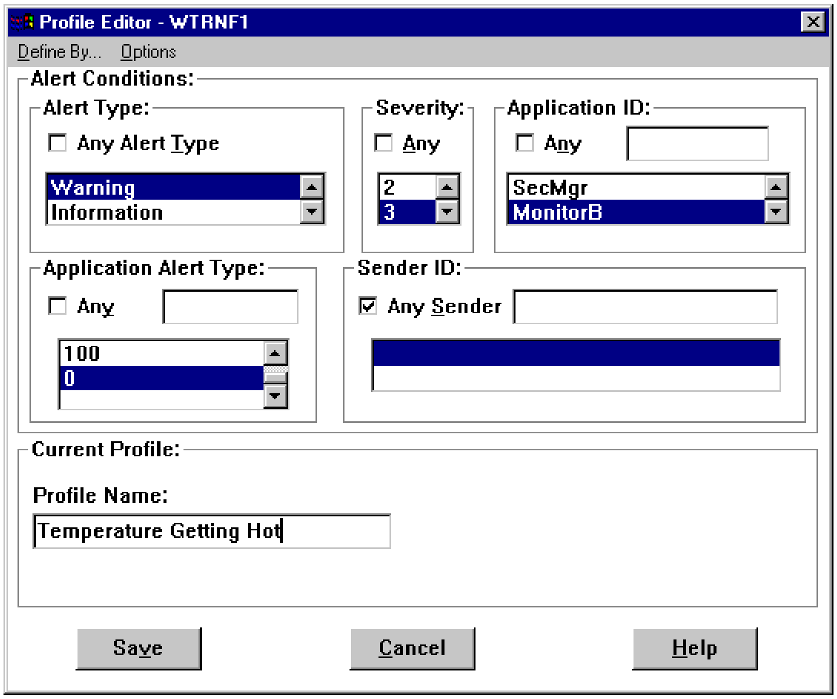
1. Open the Alert Manager on the server.
2. Click the **Profiles** button.

   We need to define an 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 7.1.1, “Configuring Thresholds” on page 198, 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 65°C point. The specifics of the alerts are shown in Table 39:

Table 39. 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 for the 40°C mark can be seen in Figure 157:



Alert Conditions:

Alert Type:

□ Any Alert Type

Warning
Information

Severity:

□ Any

2
3

Application ID:

□ Any

SecMgr
MonitorB

Application Alert Type:

□ Any

100
0

Sender ID:

☑ Any Sender

Current Profile:

Profile Name:

Temperature Getting Hot

Figure 157. 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.

   Per Table 39, 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 per Table 39. 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 check box to specify that it is from any sender. If we wanted the local machine only, we would select either the network address of the local machine or the blank line.

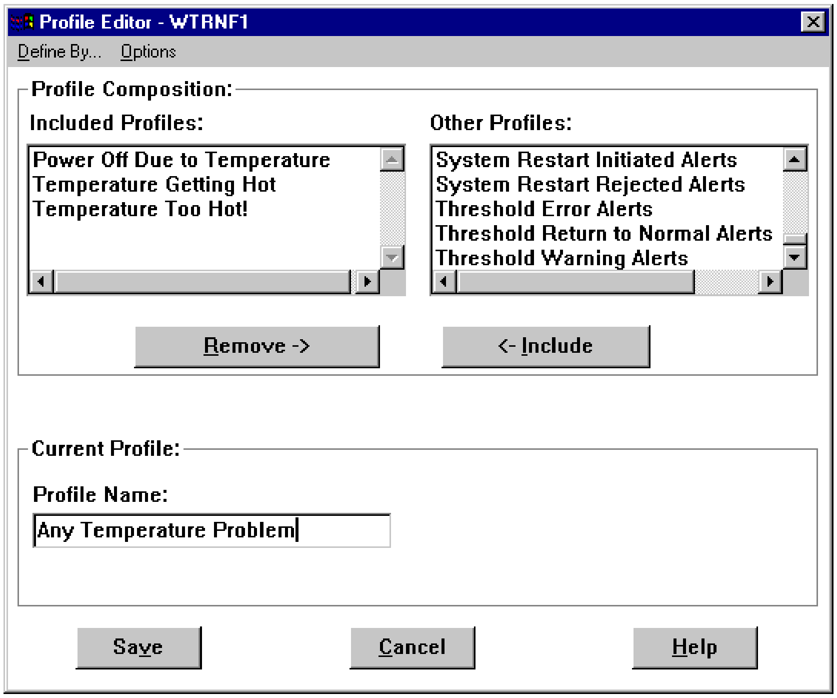
10. Name the Profile.

    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 157 at this point.

12.Repeat Steps 3 to 11 but this time for the 50°C Alert and the Power Off Alert. Refer to Table 39 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 158. To get to the window shown in Figure 158, from the Alert Profiles window select **New**, then the menu option **Define By... -> Profile Composition**.



Profile Composition:

Included Profiles:
Power Off Due to Temperature
Temperature Getting Hot
Temperature Too Hot!

Other Profiles:
System Restart Initiated Alerts
System Restart Rejected Alerts
Threshold Error Alerts
Threshold Return to Normal Alerts
Threshold Warning Alerts

Current Profile:

Profile Name: Any Temperature Problem

Figure 158. Creating a Profile to Log All Temperature Alerts

7.1.2.2 Configuring Alert Actions

Now that we have set up 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.

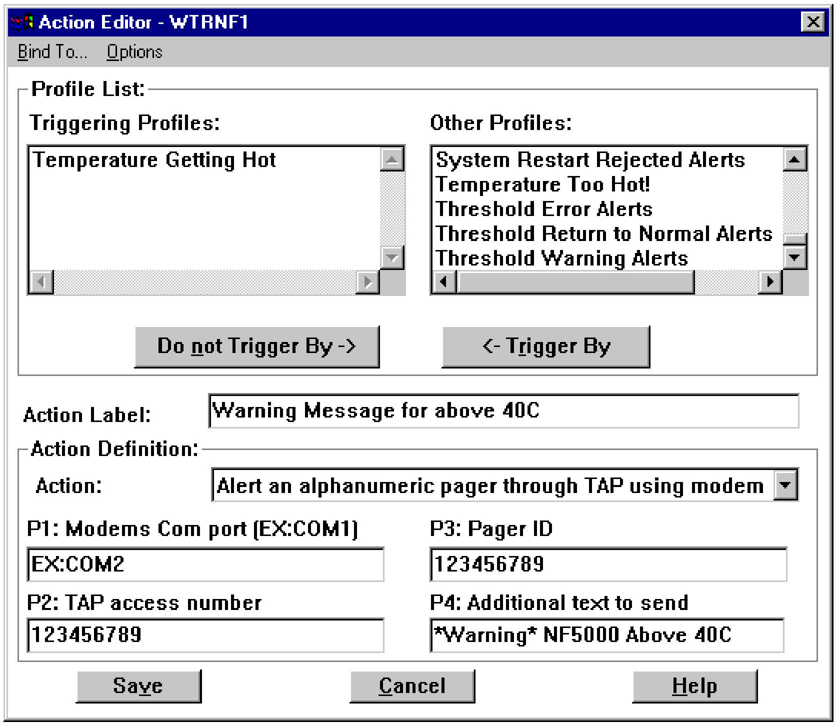
When it receives an alert, Alert Manager checks each of the alert conditions to see if it meets the specifications for a defined action. For this example we are using only profiles:

1. Click the **Actions** button from the Alert Log window and then click **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 per Figure 159.
   - Set an Action Definition.

In this case we want to set the action **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:
System Restart Rejected Alerts
Temperature Too Hot!
Threshold Error Alerts
Threshold Return to Normal Alerts
Threshold Warning Alerts

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

P2: TAP access number: 123456789

P3: Pager ID: 123456789

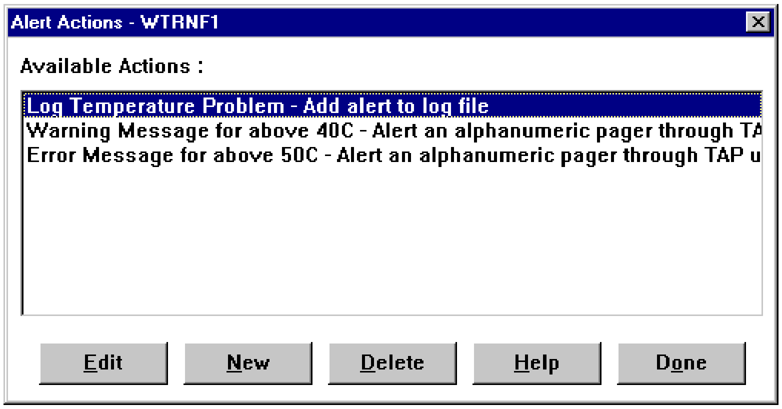
P4: Additional text to send: *Warning* NF5000 Above 40C

Figure 159. Profile Editor Setup for the 40°C Setup

4. Set up the Triggering Profiles and Action Definition as shown in Figure 159 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 Temperature Problem and set the action to **Add alert to log file**. Figure 160 shows the three profiles now bound to these actions:



Available Actions :

Log Temperature Problem - Add alert to log file
Warning Message for above 40C - Alert an alphanumeric pager through TA
Error Message for above 50C - Alert an alphanumeric pager through TAP u

Figure 160. Alert Actions Defined

7.1.3 Summary

The server has now been configured to send alerts to the administrator’s pager as the temperature rises. Table 40 shows the actions of the machine as the temperature rises:

Table 40. Summary of Actions

Threshold Reached	Action to Be Taken
40°C	Alert from System Monitor is picked up by Alert Manager and two actions are performed: 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 performed: 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.
66°C	The following actions are performed: 1. The ASM processor 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 adapter's own error log. 4. The system is powered off. 5. The ASM processor 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 powers off.

7.2 Example 2: Drive Failure in a RAID-5 Array

In this example, we have a Netfinity 5000 with Netfinity Manager installed. We have a ServeRAID II RAID adapter installed which connects an EXP15 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 automatically. We want a message to be logged and displayed on the server itself and 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 and contact us to arrange to purchase a new drive (or replace it under warranty if the failure is covered).

7.2.1 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:

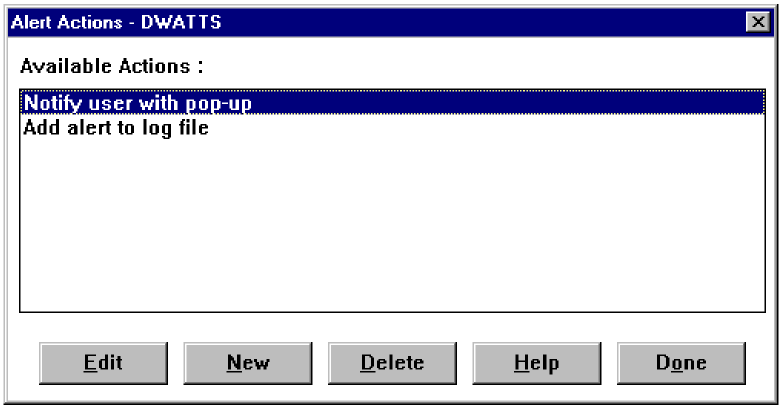


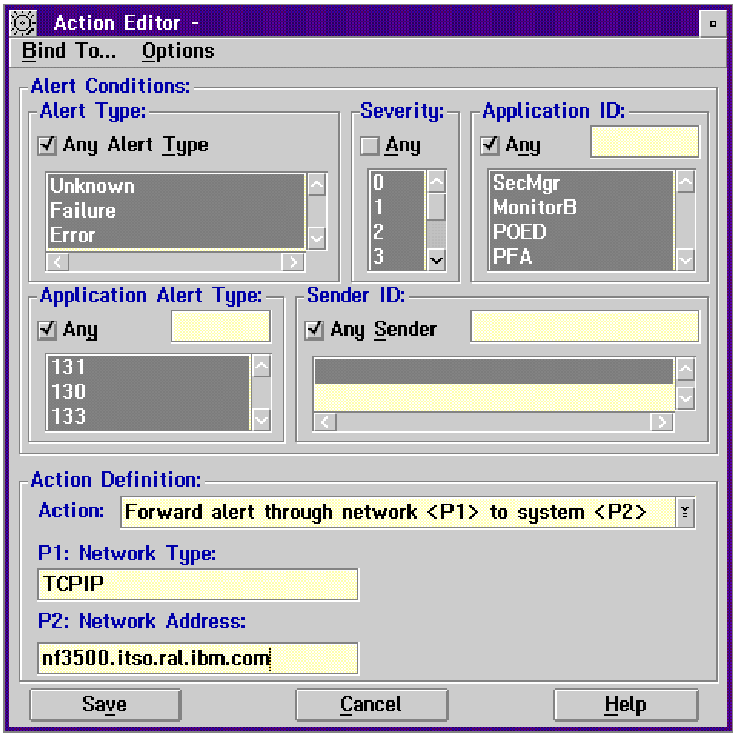
Figure 161. Standard Actions

We want to send all messages to the administrator's workstation so he/she is informed of all errors. We also want to send one message per failure to the dealer to contact us to replace it.

7.2.1.1 Notifying the Administrator

To notify the administrator, we set up an action to transmit all alerts to his/her workstation. To configure this action to happen on the alert conditions:

1. Open the **Alert Manager**.
2. Click the **Action** button to display the existing actions.
3. Click the **New** button to create a new action.
4. Set up the actions window as in Figure 162.



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: Forward alert through network <P1> to system <P2>

P1: Network Type: TCPIP

P2: Network Address: nf3500.itso.ral.ibm.com

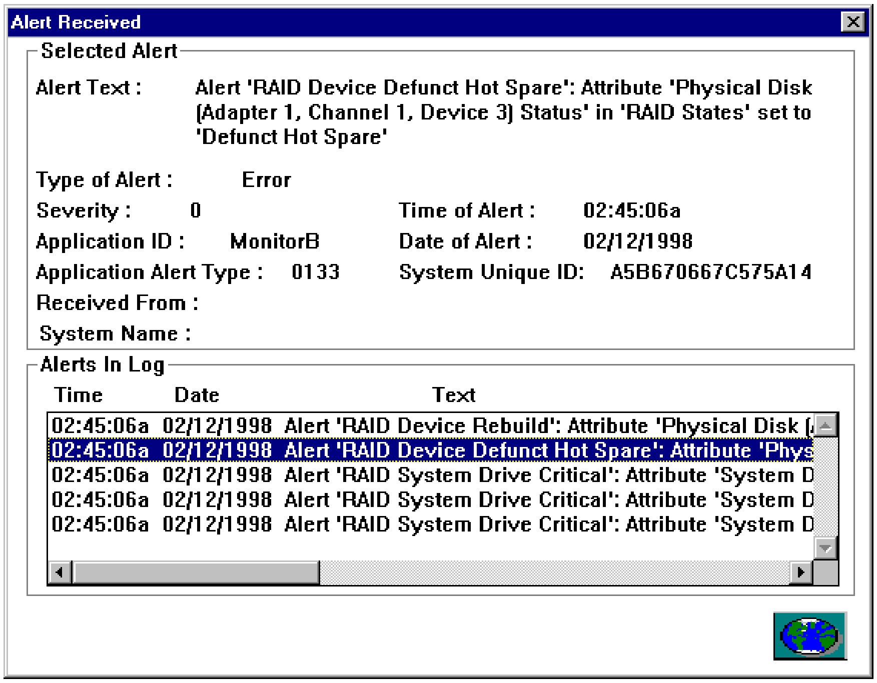
Figure 162. Configuring an Action to Send All Alerts to the Administrator

In our example, we want to forward only alerts of Severity 5 or higher. This will prevent “informational” messages from being sent to his/her workstation.

5. Click the **Save** button then **Yes** to save the action. The action now appears in the list.

7.2.1.2 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 163.



Alert Received

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 :

Alerts In Log

```
Time        Date        Text
02:45:06a  02/12/1998  Alert 'RAID Device Rebuild': Attribute 'Physical Disk (A
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 163. 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 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:

- Three messages, one from each logical drive, as each has now gone critical
- One message stating the rebuild process has started
- One message saying the failed drive has been marked as a “Defunct Hot Spare”

We want to transmit only one alert to the dealer's machine for this event rather than all five. Likewise once the rebuild has completed we want to send only 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.

As described in 2.4, “Alerts” on page 25, 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 41:

Table 41. Alerts Received When a Drive Fails

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

Alert Message	Alert Type	Severity	Application ID	Application Alert Type
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 42:

Table 42. Alert Details When Rebuild Has Completed

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 164:

Figure 164. 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:

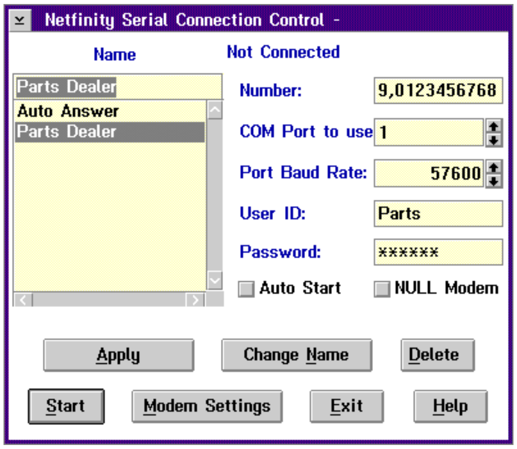
Type of Alert Failure or Error
Severity 0
Application ID MonitorB
Application Alert Type0130 or 0133

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 **Serial Control** from the main Netfinity Manager window.
2. You will see a window similar to Figure 165.

   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: ******

□ Auto Start □ NULL Modem

Figure 165. 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 by which the local Netfinity Manager knows the system.

4. Fill out the phone number, the COM port your modem is connected to and the port baud rate at which you will be connecting. The port baud rate must be the same on the dealer's machine.

5. Fill out the user ID and password that are defined on the dealer's Netfinity Manager Serial Control.

Security Implications

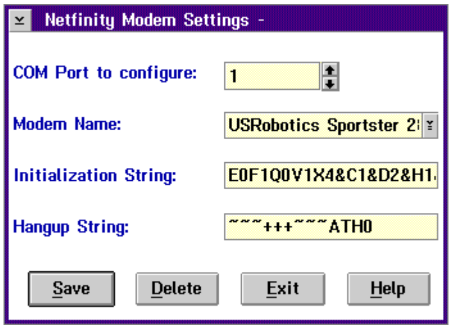
If you do not wish to let your dealer (or anyone else) dial in to your server, you should prevent the Auto Answer connection from starting. To do this, highlight the **Auto Answer** connection, then click the **Auto Start** check box to deselect it.

At the dealer's Netfinity Manager system, Auto Answer must be enabled and the user ID and password must be set. The dealer should also ensure that all access to Netfinity Manager functions is through specific user IDs and passwords. That is, all access through <PUBLIC> is removed.

Note: User IDs and passwords are case-sensitive.

6. Click 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 166:



COM Port to configure: 1

Modem Name: USRobotics Sportster 2

Initialization String: E0F1Q0V1X4&C1&D2&H1

Hangup String: ~~~+++~~~ATH0

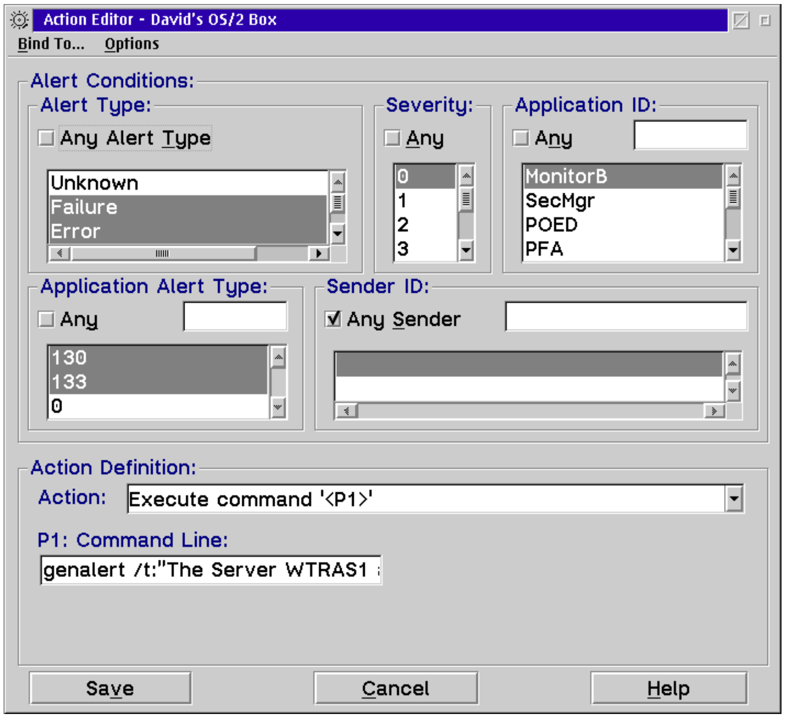
Figure 166. Serial Control Modem Settings

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 **Save** to save the modem configuration to the port displayed then **Exit** to leave the window.

8. Click 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 configure Alert Manager to send just 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 that can then be forwarded to the dealer:

1. Open the **Alert Manager**.
2. Click the **Action** button to display the existing actions.
3. Click the **New** button to create a new action.
4. Set up the actions window as in Figure 167. These correspond with the value we determined to be appropriate on Page 208.



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 167. 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:

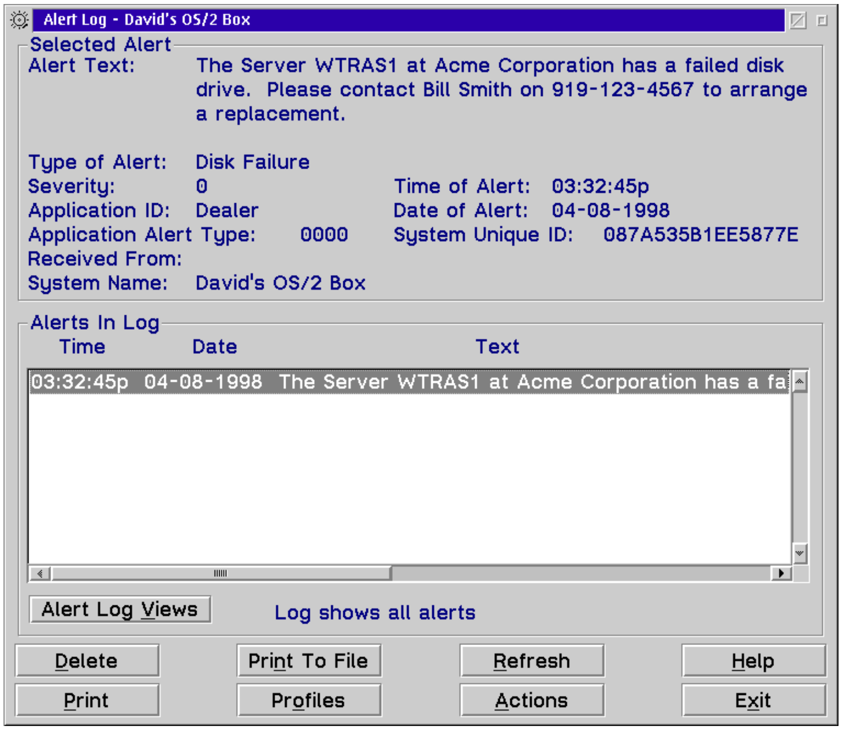
```
GENALERT /t:"The Server WTRAS1 at Acme Corporation has a failed disk
drive.  Please contact Bill Smith on 919-123-4567 to arrange a
replacement." /app:Dealer /sev:0 /type:dskflt
```

You can either put the GENALERT command in the Command Line field (as shown in Figure 167), 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 168.



Alert Log - David's OS/2 Box

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
Application ID: Dealer
Application Alert Type: 0000
Received From:
System Name: David's OS/2 Box
Time of Alert: 03:32:45p
Date of Alert: 04-08-1998
System Unique ID: 087A535B1EE5877E

Alerts In Log

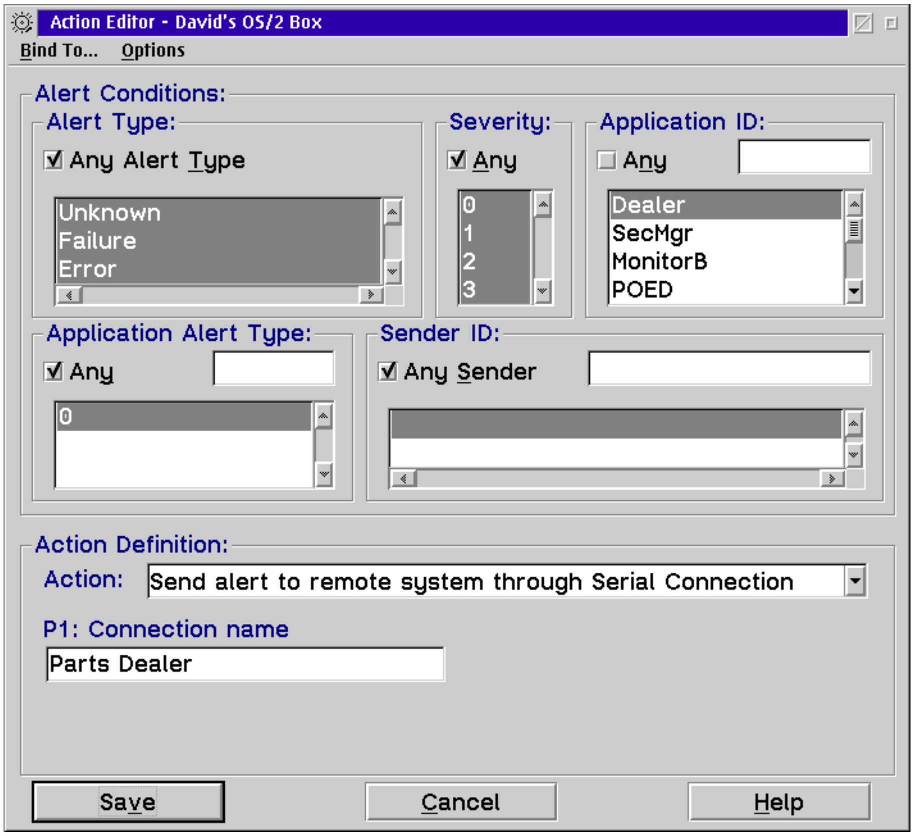
```
Time         Date          Text
03:32:45p  04-08-1998  The Server WTRAS1 at Acme Corporation has a fa
```

Log shows all alerts

Figure 168. 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 169.



Alert Type: ☑ Any Alert Type — Unknown, Failure, Error

Severity: ☑ Any — 0, 1, 2, 3

Application ID: □ Any — Dealer, SecMgr, MonitorB, POED

Application Alert Type: ☑ Any — 0

Sender ID: ☑ Any Sender

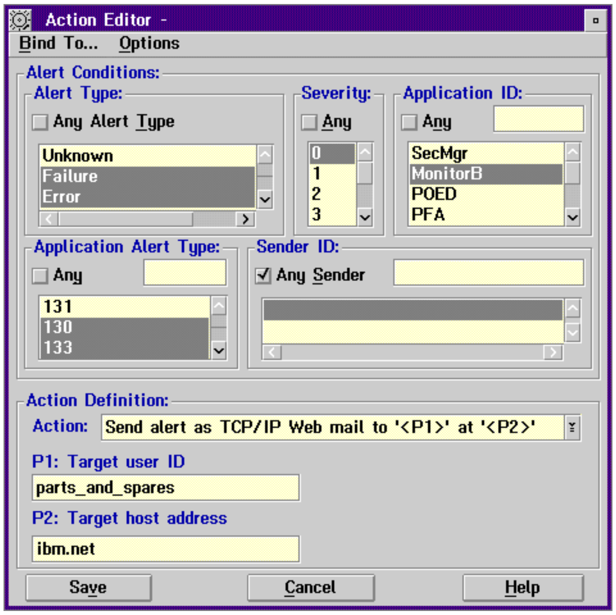
Action: Send alert to remote system through Serial Connection

P1: Connection name: Parts Dealer

Figure 169. 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 e-mail. Netfinity Manager offers a variety of e-mail actions as described in Table 6 on page 34.

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 170:



Action Editor -

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 170. Sending Alerts to the Dealer Using E-Mail

7.2.2 Summary

The setup is now complete. When a drive fails, this is what will happen:

- The alerts are stored in the 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 administrator's workstation.
- The alert locally causes the dealer’s Netfinity Manager system to be dialed by the server and the alert routed to their machine.

7.3 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 five minutes before the server shutdown sequence is started.
- The server will be shut down safely 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.

7.3.1 Configuring the Server

Connect the UPS to the server, including the serial control interface. We suggest that you 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.

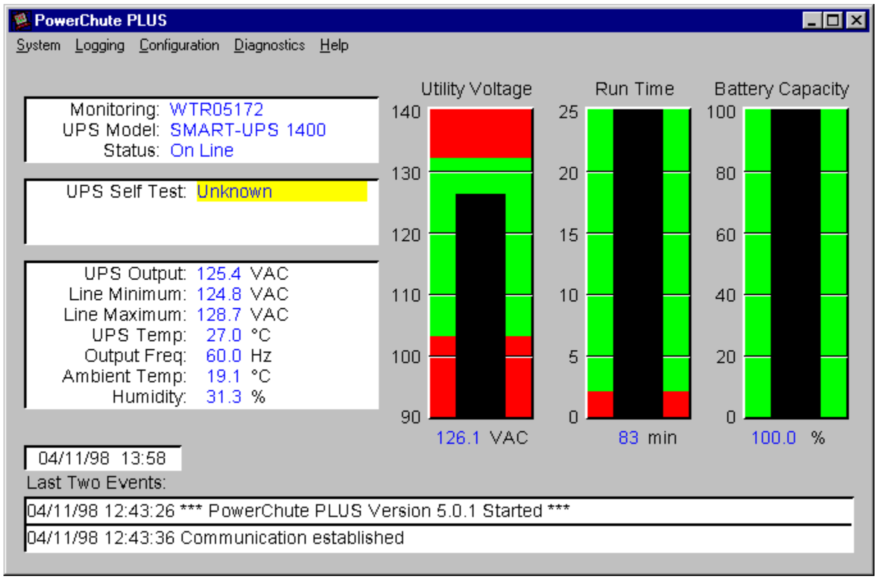
Install the necessary software on the server in the following order:

1. Netfinity Manager, per 2.2, “Installing Netfinity Manager” on page 6
2. PowerChute, per 2.5.1, “Installing PowerChute” on page 36
3. PowerXtend, per 2.5.2, “Installing PowerXtend” on page 38

7.3.2 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 **Attach**. The main window appears (Figure 171):



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 171. PowerChute Main Window

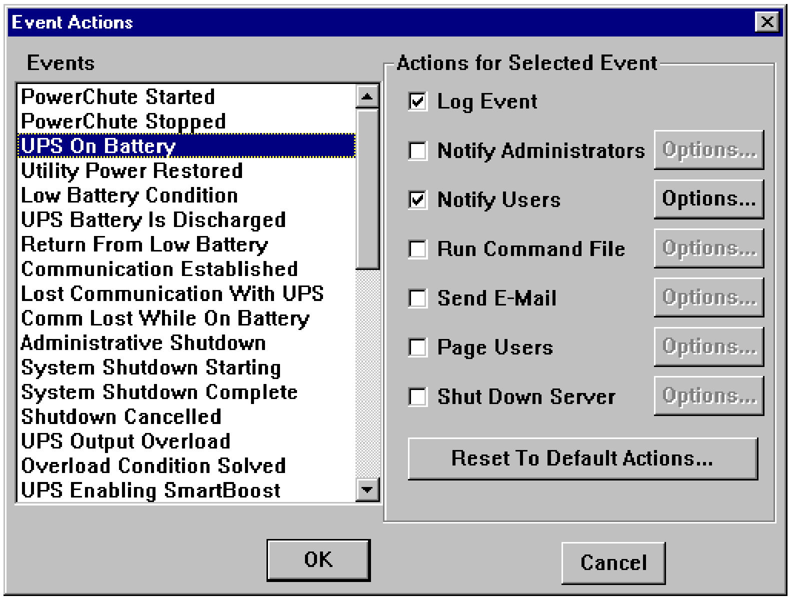
We need to configure the following events:

- UPS on Battery
- Low Battery Condition

7.3.2.1 Configuring UPS on Battery

Follow these steps to configure UPS on Battery:

1. Click **Configuration -> Event Actions**. Figure 172 appears:

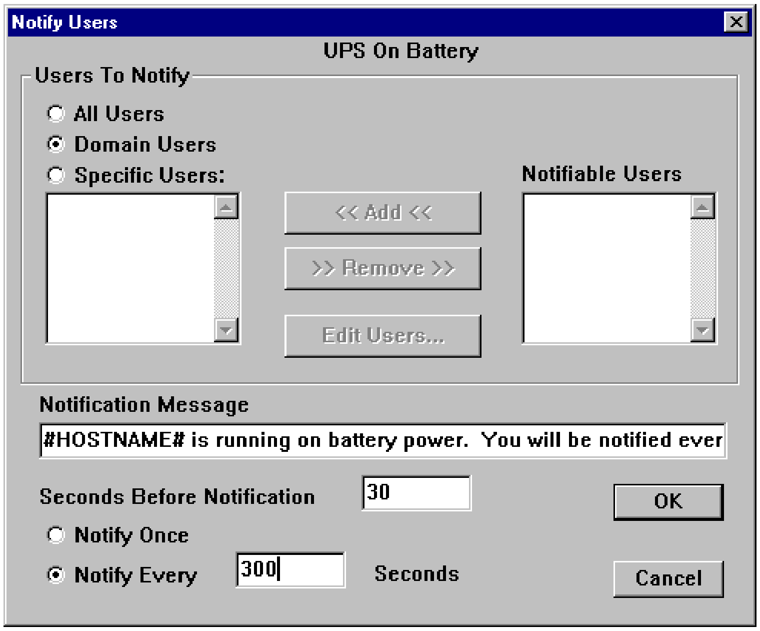


PowerChute Started
PowerChute Stopped
UPS On Battery
Utility Power Restored
Low Battery Condition
UPS Battery Is Discharged
Return From Low Battery
Communication Established
Lost Communication With UPS
Comm Lost While On Battery
Administrative Shutdown
System Shutdown Starting
System Shutdown Complete
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 172. 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 **Options** to the right of **Notify Users**. Figure 173 appears:



Notify Users

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 173. Setting the Options for Notify Users

We want all users logged onto the domain to receive a pop-up message from PowerChute when the server is running on battery. We want to wait 30 seconds before the first broadcast (in case someone bumps the power cord) and then we want the users to be notified every five minutes (300 seconds).

5. Configure the notification per Figure 173.

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 43.

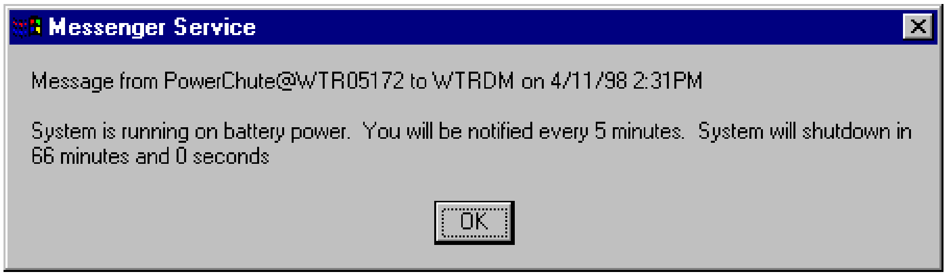
   Note: Variables must be used in uppercase.

Table 43. 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
#SHUTDOWN_DELAY#	The delay from the start of the shutdown process until the actual shutdown
#TIME_REMAINING#	The time until the shutdown process starts in minutes and seconds
#USER_COMMENT#	The user-defined description for the Measure-UPS contact

Variable	Description
Note: The following variables are available only when using the 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 174:



Message from PowerChute@WTR05172 to WTRDM on 4/11/98 2:31PM

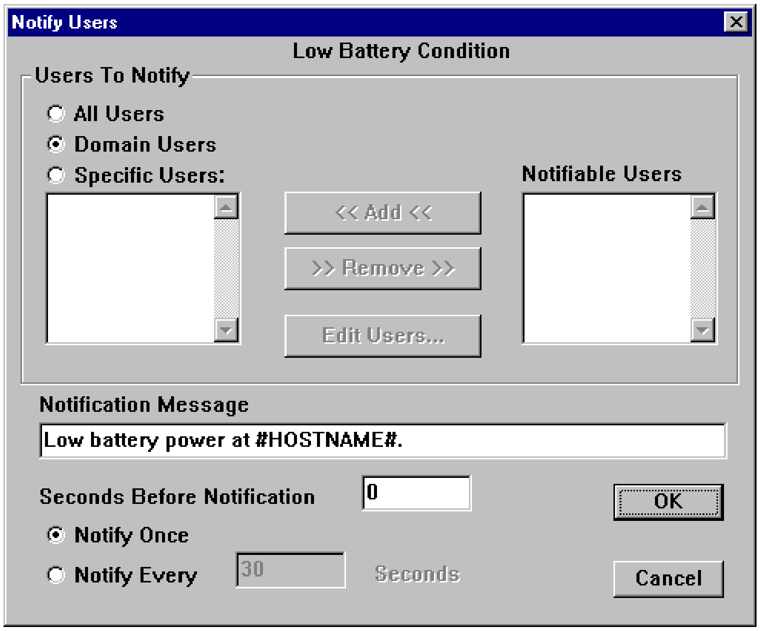
System is running on battery power. You will be notified every 5 minutes. System will shutdown in 66 minutes and 0 seconds

Figure 174. User Message When Power to the Server Fails

7.3.2.2 Configuring Low Battery Condition

Follow these steps to configure the Low Battery Condition event:

1. From the Event Actions window (Figure 172), select the **Low Battery Condition** event.
2. Ensure check marks are on **Log Event**, **Notify Users** and **Shut Down Server** but not the others.
3. Click **Options** to the right of **Notify Users**. Figure 175 appears:



○ All Users
● Domain Users
○ Specific Users:

Notification Message: Low battery power at #HOSTNAME#.

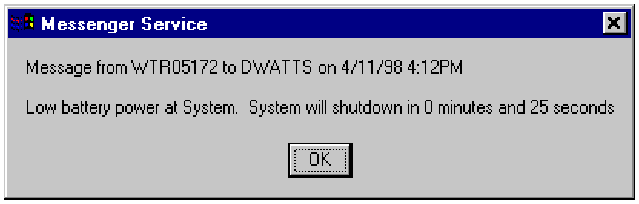
Seconds Before Notification: 0

● Notify Once
○ Notify Every 30 Seconds

Figure 175. Setting the Options for Notify Users

4. We are leaving the default message 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 176:



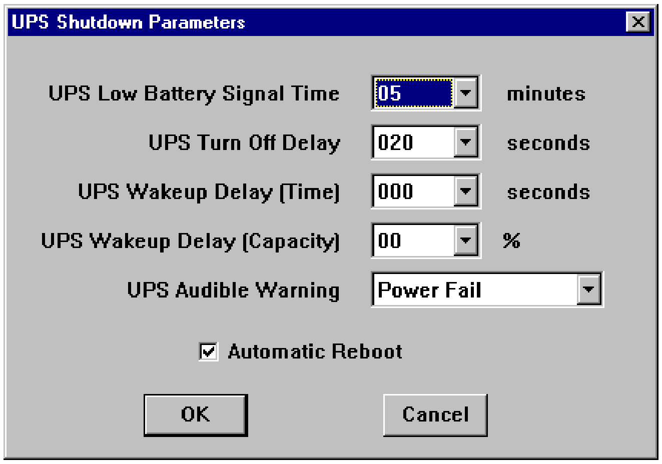
Message from WTR05172 to DWATTS on 4/11/98 4:12PM

Low battery power at System. System will shutdown in 0 minutes and 25 seconds

Figure 176. User Message When Shutdown Is Imminent

5. Specify when a Low Battery condition 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 177:



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 177. 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 down your server.

   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
   ```

7.3.3 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 shut down due to the battery’s draining.

Each of these is done through Alert Manager:

1. Open **Alert Manager**.
2. Click **Actions**.

3. For each of the four actions we want, click **New** and fill in the Action Editor per Table 44. Figure 178 shows the settings for the first action, to transfer all alerts to the administrator's workstation:

Table 44. 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

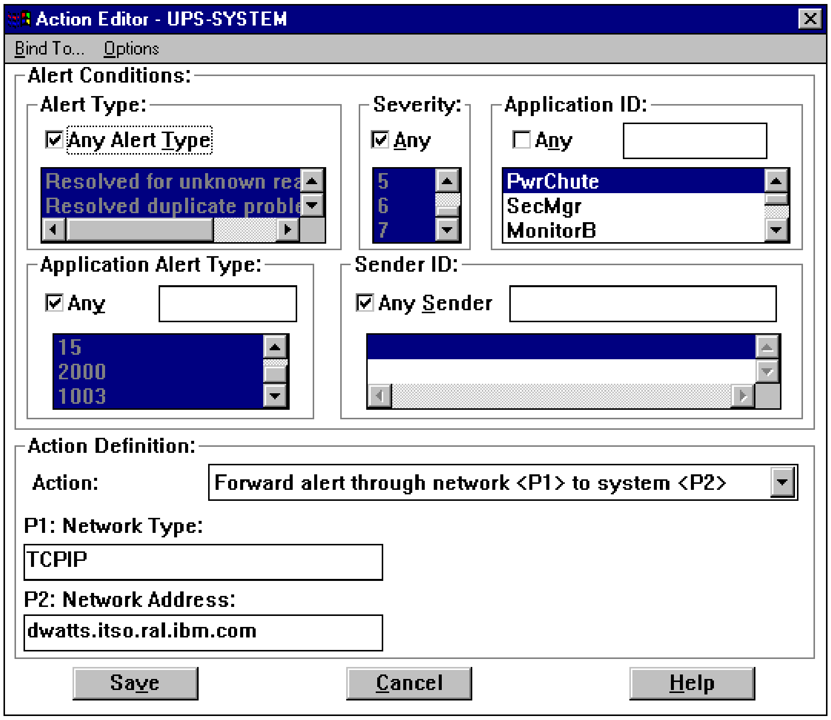
Refer to Table 7 on page 42 for a list of all Application Alert Types.

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 178. Transferring All Alerts to the Administrator's Workstation

4. Click **Save** to save each of the actions.

7.3.4 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 with which you may not want them to be concerned. 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.

7.4 Example 4: Power Supply Failure on Netfinity 7000 M10 Server

This example shows you how to set up an alert when a power supply fails on a Netfinity 7000 M10 server. In this scenario, we use the Advanced System Management PCI Adapter to alert the administrator since the system may have shut down, preventing the local Netfinity Manager from sending the alert.

In this example, the ASM PCI adapter is connected to the Ethernet network through its Ethernet port (see 3.1, “Advanced System Management PCI Adapter” on page 64). We will configure the adapter to send an alert via TCP/IP to a remote Netfinity Manager system when a power supply fails. Before you do, ensure you have TCP/IP configured on the adapter. See 4.2.5, “Network Settings” on page 116 for details.

Note: The power supply failure alerts are only supported on Netfinity servers with redundant power supplies.

On a Netfinity 7000 M10 server, redundant power can be achieved with two, three or four power supplies depending on the server configuration. In a correctly configured server, if one power supply fails, the remaining are sufficient enough to keep the server alive.

If two power supplies fail in a configuration of three, leaving only one active, a fully populated Netfinity 7000 M10 server will stay up for only a few minutes before the operating system shuts down and the server powers off.

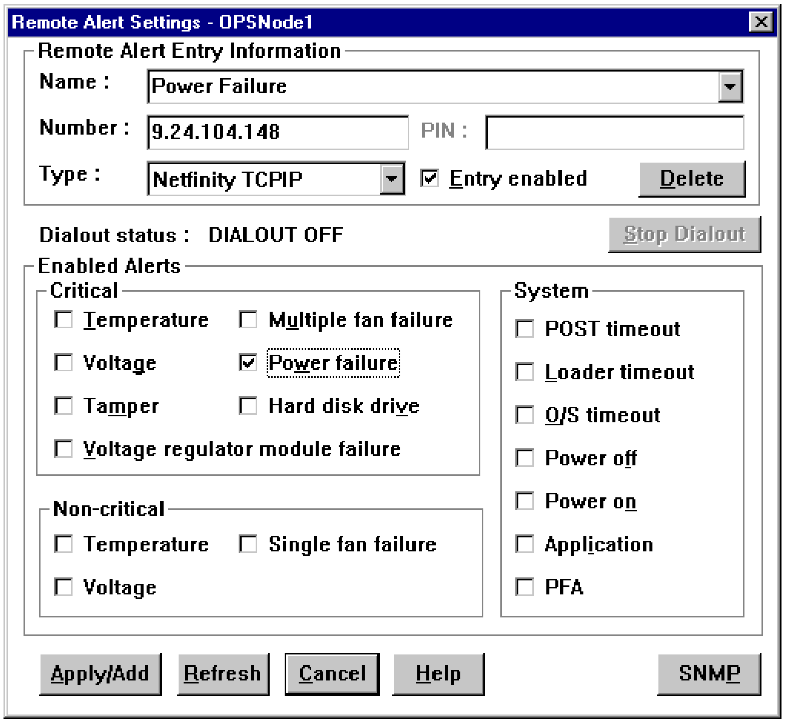
If all power supplies fail on the Netfinity 7000 M10, no alert will be issued by the ASM PCI adapter unless you install the optional external power supply option, part 83H6739. Alternatively, we recommend you use Netfinity Manager's Remote System Manager on another machine to monitor the server and notify the administrator when it goes offline.

In this example, our 7000 M10 has two power supplies.

7.4.1 Advanced System Management Settings

In order to send an alert, you need to configure your ASM PCI adapter for TCP/IP if you haven’t done so already. See 4.2.5, “Network Settings” on page 116 for details.

From the Advanced System Management service in Netfinity Manager, double-click **Remote Alert Settings** to enable the alerts you want to be sent to your remote Netfinity Manager system. Figure 179 appears. See 4.2.6, “Remote Alert Settings” on page 117 for details of this window.



Remote Alert Settings - OPSNode1

Remote Alert Entry Information

Name : Power Failure

Number : 9.24.104.148 PIN :

Type : Netfinity TCPIP ☑ Entry enabled

Dialout status : DIALOUT OFF

Enabled Alerts

Critical

□ Temperature □ Multiple fan failure
□ Voltage ☑ Power failure
□ Tamper □ Hard disk drive
□ Voltage regulator module failure

Non-critical

□ Temperature □ Single fan failure
□ Voltage

System

□ POST timeout
□ Loader timeout
□ O/S timeout
□ Power off
□ Power on
□ Application
□ PFA

Figure 179. Service Processor Dial-Out Setting for Power Failure

Here, we want the ASM PCI adapter to issue an alert via its Ethernet connection upon a power failure, so we selected **Power failure** as the only alert to be sent out. To set up your ASM PCI adapter, perform the following:

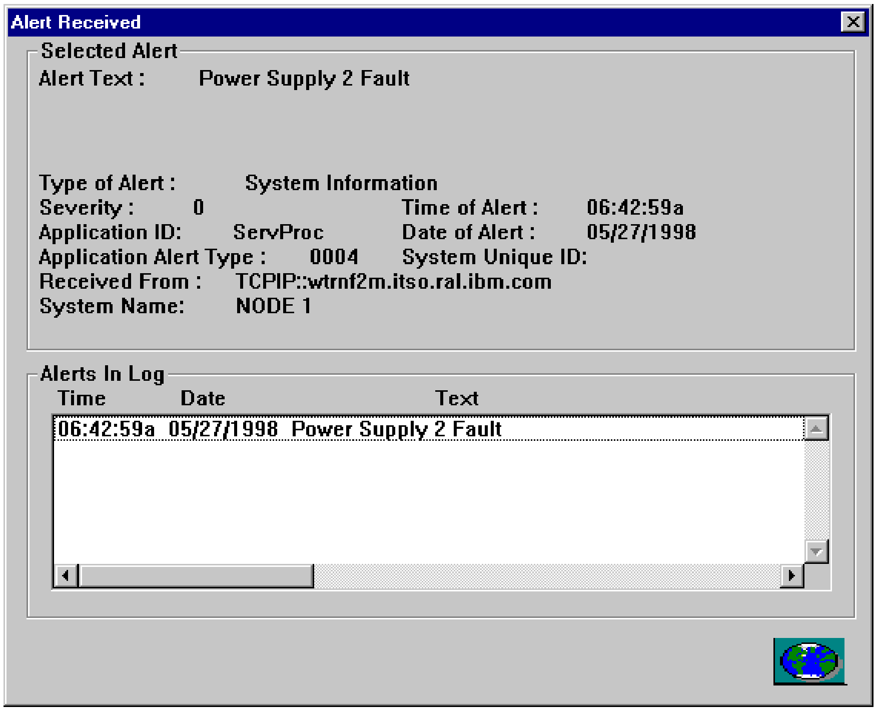
1. Enter a name of the alert entry.
2. Enter the TCP/IP of the target system (or a phone number if you are dialing out using a modem).
3. Select the type of alert that will be sent out. We are dialing a remote Netfinity Manager system, so we've selected **Netfinity TCPIP**. Other options are numeric, alphanumeric pagers and Netfinity serial.
4. Check the **Entry enabled** box.
5. Check any box for other alerts you want forwarded. You may want to select other alerts for your system.
6. Click **Apply/Add** to store the settings.

7.4.2 Receiving the Alert

Since we are sending the alert via TCP/IP, the remote Netfinity Manager system should receive the alert automatically.

The ASM PCI adapter will poll the power supplies every 90 seconds or so. In case a power supply fails, the adapter will attempt to forward an alert to all enabled remote alert entries. As we specified the recipient to be a Netfinity Manager system, it will receive a standard alert similar to Figure 180.

The administrator can then configure further actions to occur as necessary based on that alert.



Selected Alert

Alert Text : Power Supply 2 Fault

Type of Alert : System Information
Severity : 0
Time of Alert : 06:42:59a
Application ID: ServProc
Date of Alert : 05/27/1998
Application Alert Type : 0004
System Unique ID:
Received From : TCPIP::wtrnf2m.itso.ral.ibm.com
System Name: NODE 1

Alerts In Log

Time	Date	Text
06:42:59a	05/27/1998	Power Supply 2 Fault

Figure 180. Power Supply Failure Pop-Up Message

7.5 Example 5: Operating System Timeout

This example describes how to set up the management processor to generate a dial-out alert in the event of an operating system timeout.

If your server’s operating system traps, abends, or hangs, the management 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 management processor to do this:

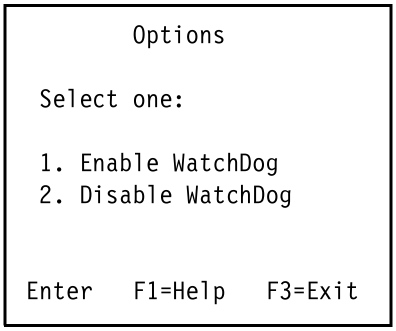
1. For the ASM ISA adapter, you need to enable the O/S WatchDog Timer using the configuration diskette. For the ASM PCI adapter and ASM processor, this step is not necessary.
2. Set the OS Timeout value in the Advanced System Management service.
3. Create a dial-out entry in the Advanced System Management service.

7.5.1 Enable the OS WatchDog (ASM ISA Adapter Only)

This section applies only to users of the Advanced Systems Management Adapter.

Before you can configure the OS WatchDog, you must first enable it. If it has 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.

7.5.2 Configure the OS WatchDog

Now you need to configure the OS WatchDog in the Advanced System Management service in Netfinity Manager:

1. Start Netfinity Manager.
2. Double-click Advanced System Management. Figure 181 appears.

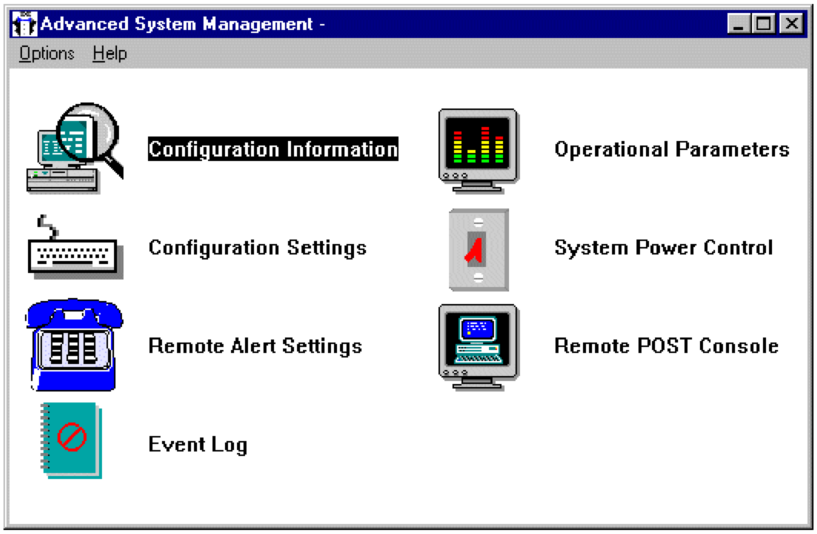
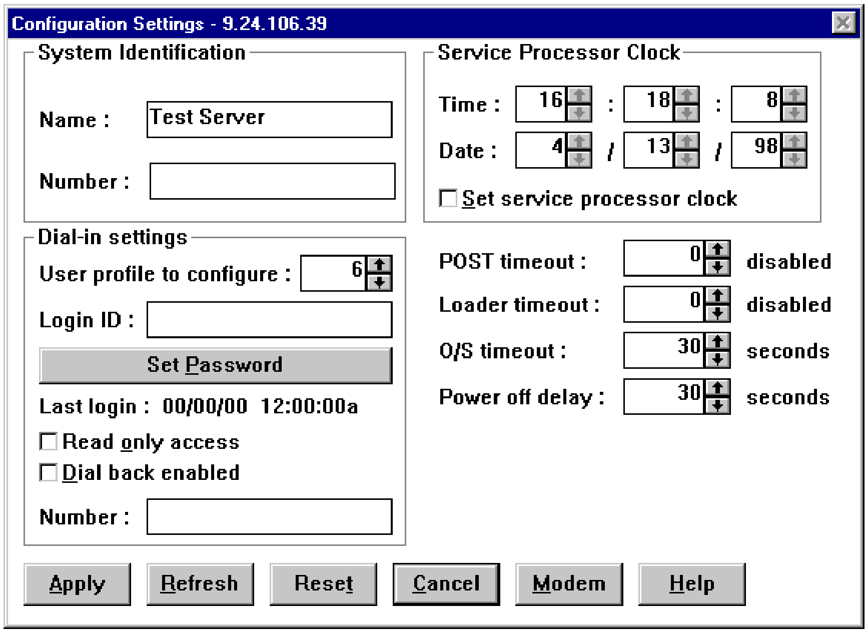


Figure 181. Advanced System Management Window

3. Double-click **Configuration Settings**. Figure 182 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 182. 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 an O/S timeout event. Since we have enabled the WatchDog timer, if the O/S takes longer than the configured amount of time to respond, the management 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.

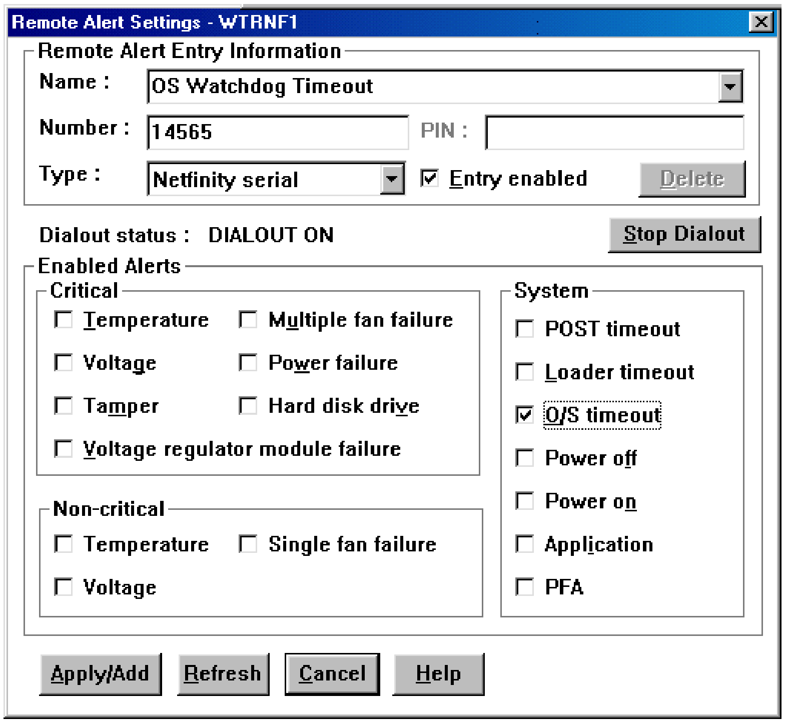
See 4.2.3, “Configuration Settings” on page 108 for information about the rest of this window.

5. Click **Apply** then **Cancel** to close the window.

7.5.3 Configuring a Dial-Out Entry

Now that the management processor 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 Advanced System Management window, double-click **Remote Alert Settings**. Figure 183 appears:



Remote Alert Settings - WTRNF1

Remote Alert Entry Information

Name : OS Watchdog Timeout

Number : 14565 PIN :

Type : Netfinity serial ☑ Entry enabled

Dialout status : DIALOUT ON

Enabled Alerts

Critical

□ Temperature □ Multiple fan failure
□ Voltage □ Power failure
□ Tamper □ Hard disk drive
□ Voltage regulator module failure

Non-critical

□ Temperature □ Single fan failure
□ Voltage

System

□ POST timeout
□ Loader timeout
☑ O/S timeout
□ Power off
□ Power on
□ Application
□ PFA

Figure 183. Remote Alert Settings

2. Type in a phone number and a descriptive name.
3. Select **Netfinity serial** 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 **Apply/Add** to add the entry then **Cancel** to exit the window.

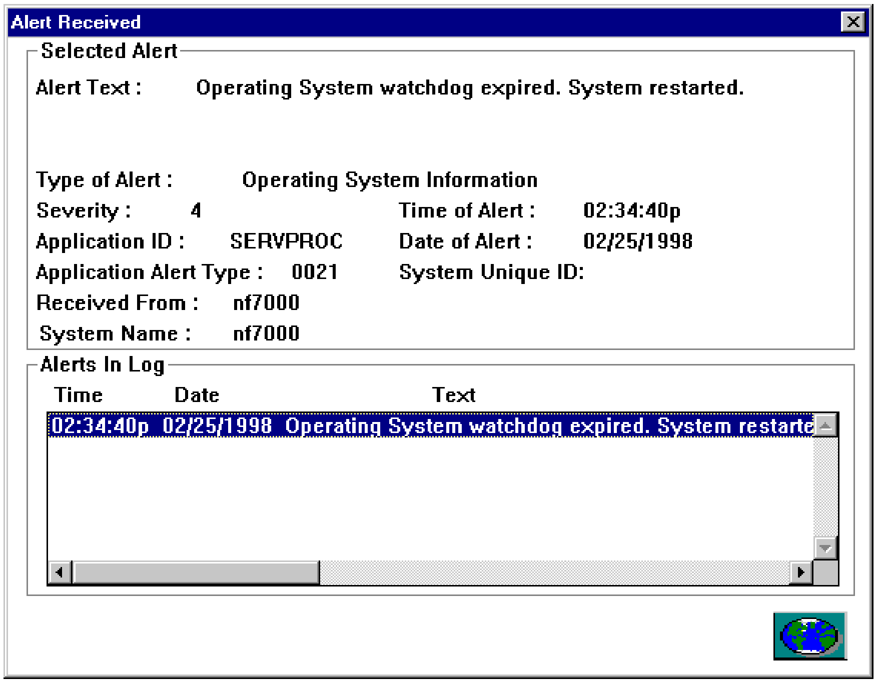
For more information about this window see 4.2.6, “Remote Alert Settings” on page 117.

The modem used to dial out with the alert can be connected locally to the server or it can be attached to another server provided the two servers are connected together in an ASM interconnect network. The sharing of modems across the ASM interconnect bus is described in 3.4.5, “Sending Alerts Through Shared Resources” on page 84.

7.5.4 Running the Scenario

The management 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 management processor assumes an operating system timeout.

If this happens, the WatchDog process will wait for the amount of time you selected in O/S timeout and initiate a system restart. A message as seen in Figure 184 will be forwarded to the remote Netfinity Manager system:



Alert Received

Selected Alert

Alert Text : Operating System watchdog expired. System restarted.

Type of Alert : Operating System Information

Severity : 4

Application ID : SERVPROC

Application Alert Type : 0021

Received From : nf7000

System Name : nf7000

Time of Alert : 02:34:40p

Date of Alert : 02/25/1998

System Unique ID:

Alerts In Log

```
Time        Date        Text
02:34:40p  02/25/1998  Operating System watchdog expired. System restarte
```

Figure 184. Service Processor O/S Timeout Alert

You could then process the alert as follows:

- Send a message via network messaging to all users logged on to the domain informing them of the restarted server.
- Notify the administrator so he/she can ensure the server is restarted correctly.

7.6 Example 6: POST Timeout and Remote POST Console

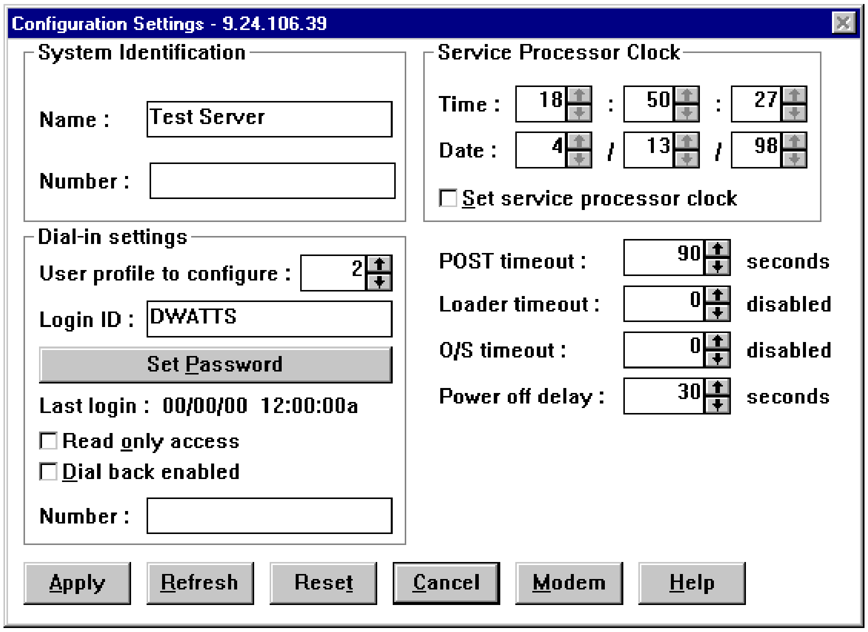
In this scenario, we have a Netfinity 5000 and we want to be notified when the POST process takes too long to complete. Upon notification, we will use the ASM processor's Remote POST Console function to watch remotely the POST to determine where the problem lies.

Note: The POST timeout function is available on all systems with the ASM PCI adapter and ASM processor installed and only the Server 325 and Server 330 with an ASM ISA adapter installed. The Remote POST Console is currently available only on systems with an ASM PCI adapter or ASM processor and the Netfinity 7000, Server 325 and Server 330.

7.6.1 Configuring the POST Timeout

Follow these steps to configure your Service Processor for POST Timeout:

1. From Netfinity Manager, start the **Advanced System Management** service.
2. Open **Configuration Settings**. Figure 185 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

Set Password

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

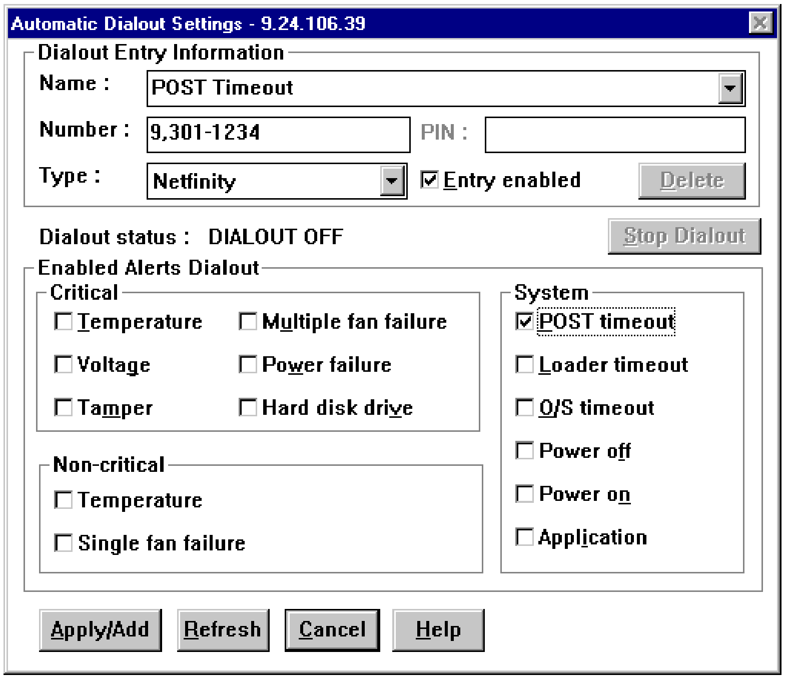
Power off delay : 30 seconds

Figure 185. 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 **Apply**.

Now, you want to configure the ASM device to dial out with a Netfinity Manager alert when the POST timeout occurs:

1. Open **Remote Alert Settings**. Figure 186 appears:


Automatic Dialout Settings - 9.24.106.39

Dialout Entry Information

Name : POST 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 186. Remote Alert Settings

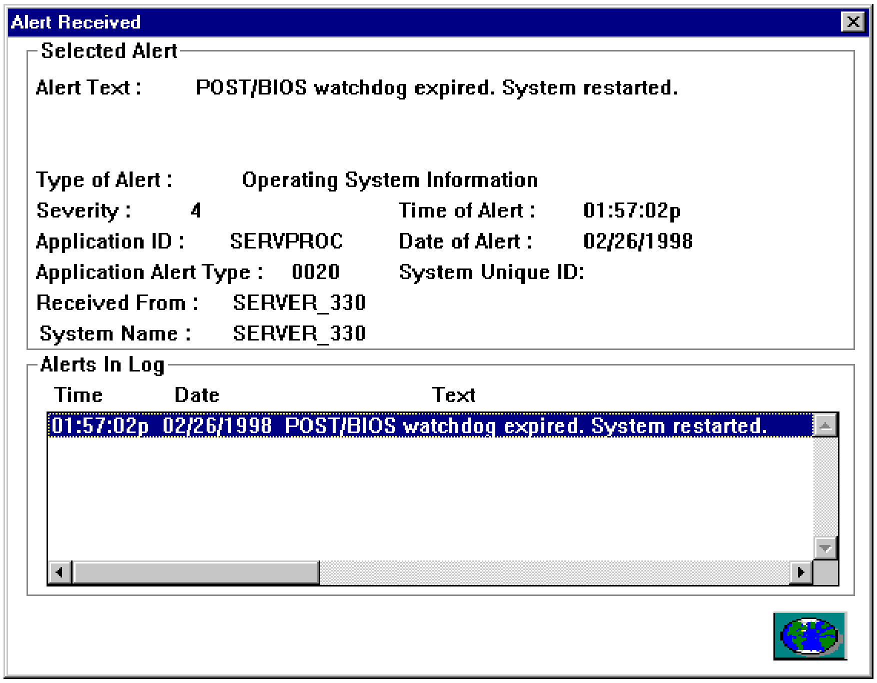
2. Enter a phone number and set the Type to **Netfinity**.
3. Put a check mark in **Entry enabled**.
4. Put a check mark in **POST timeout**.
5. Adjust any other settings.
6. Click **Apply/Add** to save the settings and then **Cancel** to close the window.

See 4.2.6, “Remote Alert Settings” on page 117 for details on other settings in this window.

Your system is now set to monitor the POST for timeout.

7.6.2 What Happens

The ASM device monitors the system startup process. It will measure the POST time and compare it with the value you set in the Configuration Settings window. If the time for POST takes longer, the ASM device assumes the system experienced a problem and attempts to restart the system. Simultaneously, it will forward an alert to your remote system. Figure 187 shows an example of a POST timeout alert:



Alert Text : POST/BIOS watchdog expired. System restarted.

Type of Alert : Operating System Information
Severity : 4
Application ID : SERVPROC
Application Alert Type : 0020
Received From : SERVER_330
System Name : SERVER_330
Time of Alert : 01:57:02p
Date of Alert : 02/26/1998
System Unique ID:

```
Time       Date         Text
01:57:02p  02/26/1998  POST/BIOS watchdog expired. System restarted.
```

Figure 187. Service Processor POST Timeout Alert

7.6.3 Using the Remote POST Console

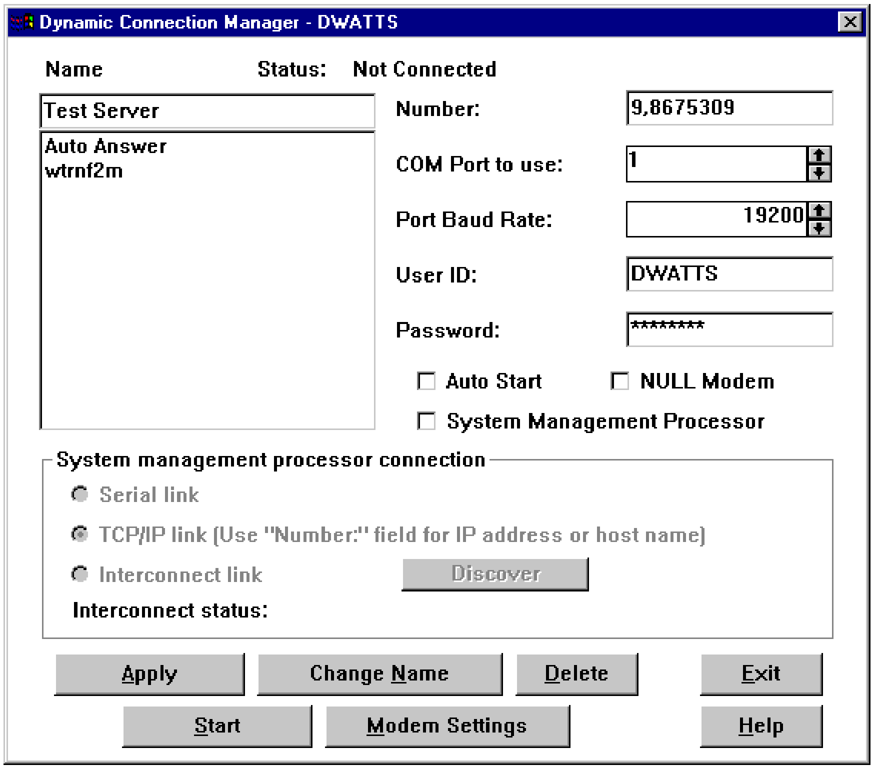
The ASM device has the ability to redirect the POST through the adapter and serial link to a remote system. The Remote POST Console is a full-functioning mirror of the actual system.

As described in 4.2.10, “Remote POST Console” on page 124, in order to run Remote POST Console, you need to connect to a remote system via one of the following:

- Modem or null modem
- Serial connection
- TCP/IP link via Telnet or Netfinity Manager
- RS-485 link via TCP/IP or serial link only

Follow these steps to set up a connection:

1. If you have not done so already, create a new entry in Dynamic Connection Manager per Figure 188.



Dynamic Connection Manager - DWATTS

Name: Test Server

Auto Answer
wtrnf2m

Status: Not Connected

Number: 9,8675309

COM Port to use: 1

Port Baud Rate: 19200

User ID: DWATTS

Password: ********

□ Auto Start □ NULL Modem

□ System Management Processor

System management processor connection

○ Serial link

● TCP/IP link (Use "Number:" field for IP address or host name)

○ Interconnect link

Interconnect status:

Figure 188. Configuring a Serial Connection

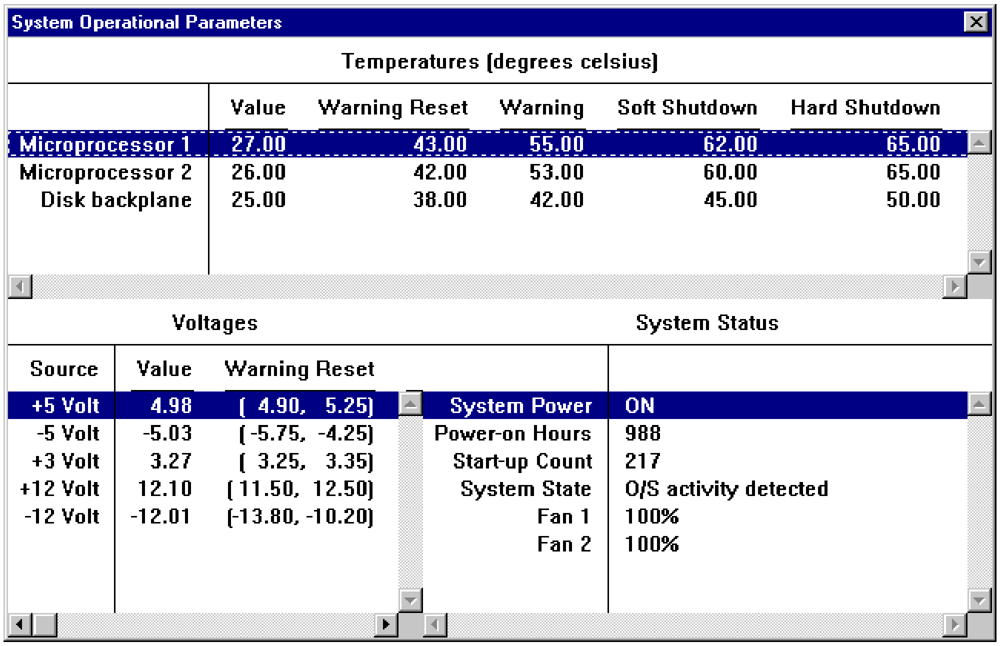
2. Save your new entry by clicking **Apply**.

   The user ID and password you set here must match the ones set in the dial-in settings in the Configuration Settings window as shown in Figure 185.

3. Click **Start** to establish the connection.

4. Click **Exit** to close the Dynamic Connection Manager window.

5. Open **Operational Parameters** from the Advanced System Management window. Figure 189 appears.



System Operational Parameters

Temperatures (degrees celsius)

	Value	Warning Reset	Warning	Soft Shutdown	Hard Shutdown
Microprocessor 1	27.00	43.00	55.00	62.00	65.00
Microprocessor 2	26.00	42.00	53.00	60.00	65.00
Disk backplane	25.00	38.00	42.00	45.00	50.00

Voltages

Source	Value	Warning Reset
+5 Volt	4.98	(4.90, 5.25)
-5 Volt	-5.03	(-5.75, -4.25)
+3 Volt	3.27	(3.25, 3.35)
+12 Volt	12.10	(11.50, 12.50)
-12 Volt	-12.01	(-13.80, -10.20)

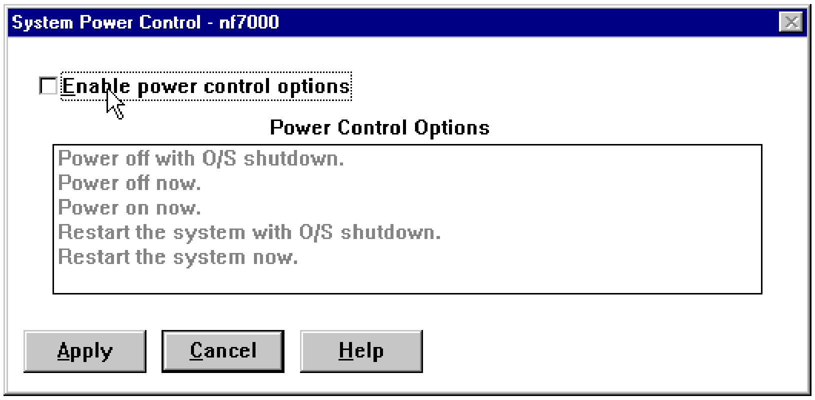
System Status

System Power	ON
Power-on Hours	988
Start-up Count	217
System State	O/S activity detected
Fan 1	100%
Fan 2	100%

Figure 189. Operational Parameters

6. Check the System Power status field — it should indicate the operating system is active.

7. Close the window and open the System Power Control window. Figure 190 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 190. Service Processor System Power Control

8. Check **Enable power control options** and select **Power off now** or **Power off with O/S shutdown**.

9. Click **Apply**.

10. Open **Operational Parameters** again and check System Power status field. Wait until the System power status changes to OFF.

11. Click **Cancel** and open **Remote POST Console**.

12. Leaving the Remote POST Console window open, open **System Power Control**.

13. Enable power control and select **Power on now**.

14. Click **Apply** and then **Cancel**.

15.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 from the remote Service Processor.

7.7 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.

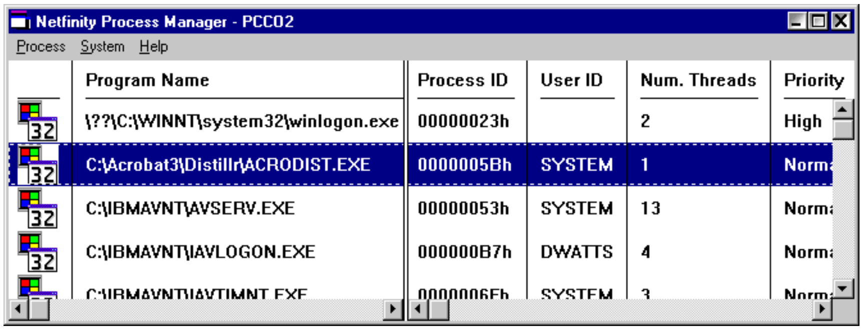
This can be handled easily by Netfinity Manager:

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.
   - Pop up 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.

7.7.1 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 it's better to work remotely in a moment.)

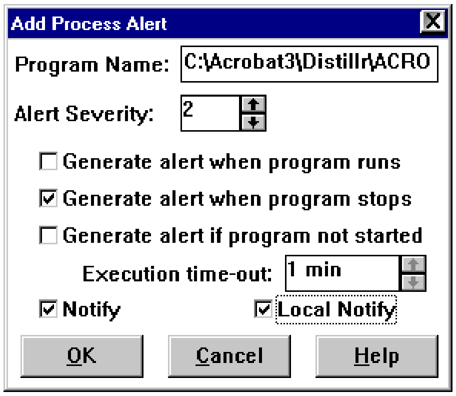
1. If ACRODIST isn't already running, start it using Remote Workstation Control.
2. Double-click the server's **Process Manager** icon and scroll down the list until you see the ACRODIST process as shown in Figure 191:



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	Norm:
C:\IBMAVNT\AVSERV.EXE	00000053h	SYSTEM	13	Norm:
C:\IBMAVNT\IAVLOGON.EXE	000000B7h	DWATTS	4	Norm:
C:\IBMAVNT\IAVTIMNT.EXE	0000006Fh	SYSTEM	3	Norm:

Figure 191. ACRODIST in Process Manager

3. Right-click the ACRODIST process and click **Add Process Alert**. Figure 192 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 192. 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.

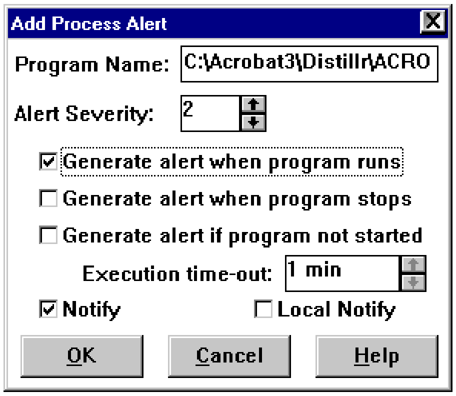
   By working from the administrator's workstation, you get both of these notify check boxes. If you worked locally at the server, you would get only **Notify**.

   Note: If you have neither one *not* selected, no alert will be issued to any Netfinity Manager system.

5. Click **OK** to save the Alert.

6. Right-click the ACRODIST and select **Add Process Alert** again.

7. This time, fill out an alert for when ACRODIST starts or restarts, per Figure 193:



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

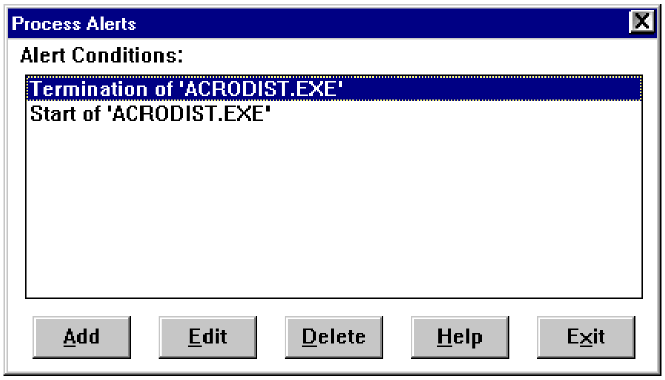
☑ Notify □ Local Notify

Figure 193. 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 **OK** to save the Alert.

Tip: If you want to edit the process alerts once they've been defined, click **Process -> Process Alerts**. Figure 194 appears letting you select and edit each alert:



Termination of 'ACRODIST.EXE'
Start of 'ACRODIST.EXE'

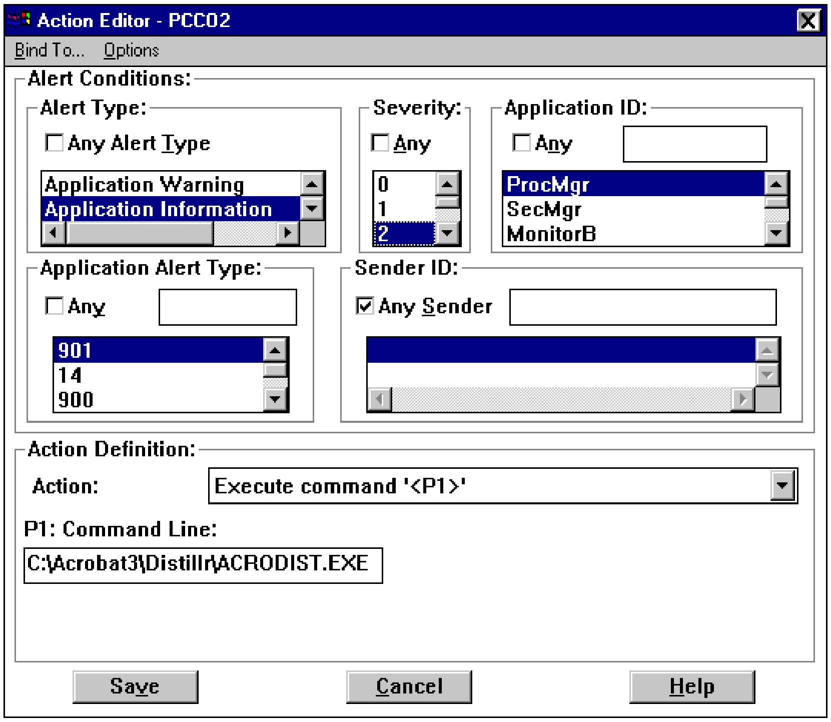
Figure 194. Editing Existing Process Alerts

7.7.2 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 192.
- Pop up a message on the administrator's workstation – already configured since we specified **Notify** in Figure 192 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 **Actions** in Alert Manager yields the Action Editor window, shown in Figure 195:



Alert Conditions:

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 Definition:

Action: Execute command '<P1>'

P1: Command Line:
C:\Acrobat3\Distillr\ACRODIST.EXE

Figure 195. Action Editor

The alert received when the ACRODIST process stops has the following characteristics:

Alert Type: Application Information
Severity: 2
Application ID: ProcMgr
Application Alert Type: 901

We, therefore, configure the action based on those values as shown in Figure 195. Our action is to execute a command, and the P1 field is the command to restart the process.

7.7.3 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 193, there is nothing further to do.

As additional steps, 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.

7.8 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. We will be connecting to the remote server via modems.

Other connections are possible such as RS-485 and TCP/IP connections as listed in 4.2.1, “Remote BIOS Flash” on page 106.

The hardware and software prerequisites for this function are:

- Netfinity Manager 5.10.4 or later on both the workstation and the remote Netfinity 5500
- The installation option, “Advanced 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

7.8.1 The Process

The steps are as follows:

1. Configure dialing into the 5500's Advanced Remote Management processor.
2. Set up dialout from the workstation.
3. Dial in to 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 104 on page 143).

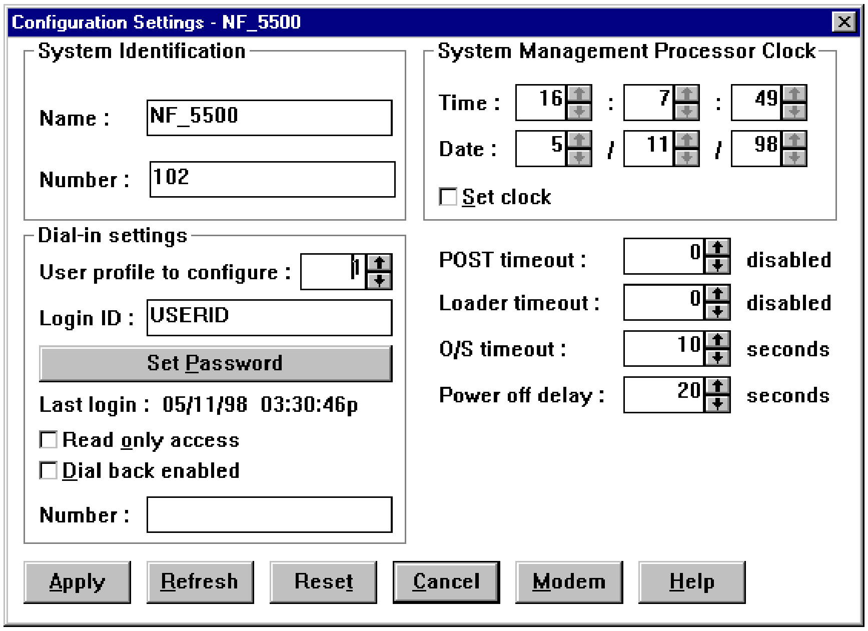
This function is useful because it allows you to recover from a BIOS upgrade that caused errors.

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.

7.8.1.1 Configure Dial-In

Before we can dial in to 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 196 appears:



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

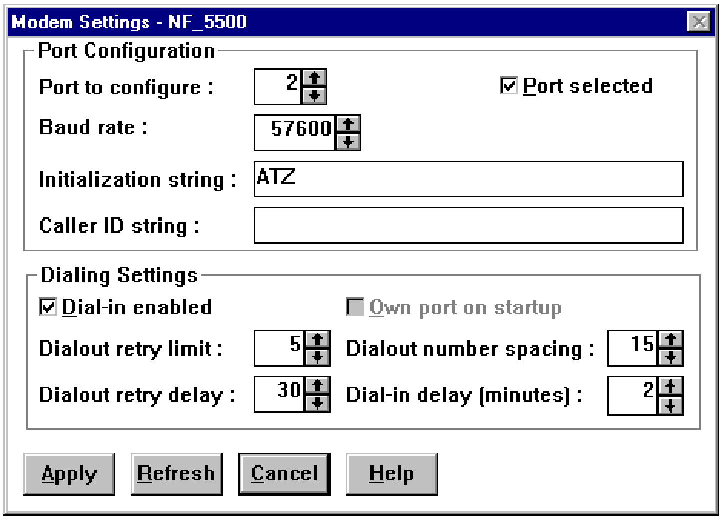
O/S timeout : 10 seconds

Power off delay : 20 seconds

Figure 196. Advanced Remote Management Processor Dial-In Settings

2. Enter a user ID and password that you plan to use to dial in to the Advanced Remote Management processor. See 4.2.3, “Configuration Settings” on page 108 for details on this window.

3. Click **Modem**. Figure 197 appears:



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 197. ASM Processor Modem Settings

4. Configure your own modem. See 4.2.4, “Port and Dialing Settings” on page 112 for details on this window.

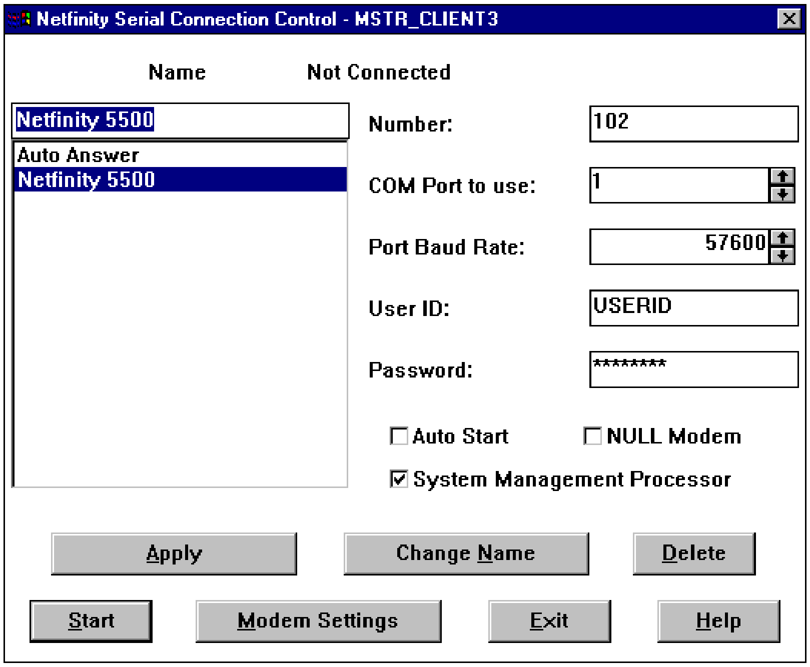
   Notice that port 2 is configured as the one connected to the modem. Port 2 corresponds to COM C, the management port on the Netfinity 5500. Save your modem settings.

5. Click **Apply** to save your dial-in user ID settings.

7.8.1.2 Configure Dialout 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 Netfinity Manager. Figure 198 appears:



Netfinity Serial Connection Control - MSTR_CLIENT3

Name   Not Connected

Netfinity 5500

Auto Answer
Netfinity 5500

Number: 102

COM Port to use: 1

Port Baud Rate: 57600

User ID: USERID

Password: *********

□ Auto Start   □ NULL Modem

☑ System Management Processor

Figure 198. Serial Control Settings

2. Fill in the fields in the window to match the user ID you specified in step 2 in 7.8.1.1, “Configure Dial-In” on page 239 and the phone number and modem parameters of your modem.

3. Put a check in the **System Management Processor** field.

4. Click **Apply** to save the new settings.

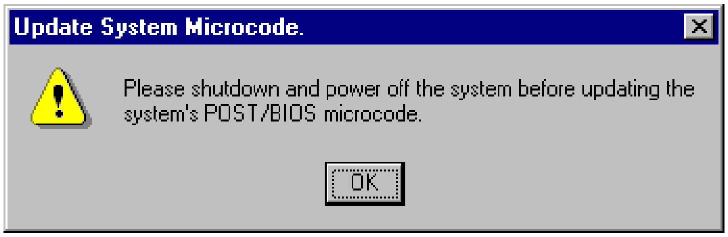
5. Click **Start** to dial the Advanced Remote Management processor on the Netfinity 5500.

   Once the connection is made, you will see `Connected` at the top of the window.

6. Click **Exit** then **OK** to confirm exit without saving changes.

7.8.1.3 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:



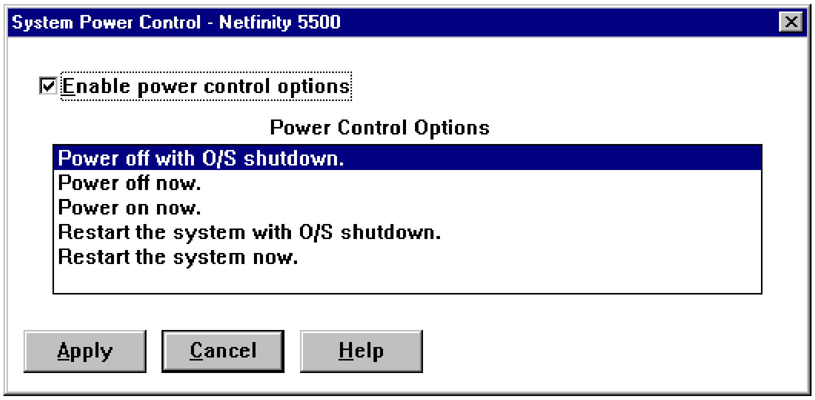
Update System Microcode.

Please shutdown and power off the system before updating the system's POST/BIOS microcode.

Figure 199. Shut Down the Server Before BIOS Update

1. To power down the server, go to the Advanced System Management window and open **System Power Control**. Figure 200 appears.

   As you are already dialed in to the server, you are now controlling it from your local workstation through the Advanced System Management interface.



☑ 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 200. System Power Control on the Netfinity 5500

2. Click **Enable power control options**.
3. Select **Power off with O/S shutdown**.
4. Click **Apply**. The operating system now shuts down and the server powers off.
5. Click **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 opening Serial Connection Control and verifying that `Connected` is still displayed at the top of the window.

7.8.1.4 Flash the BIOS

Now that the server is powered down, the BIOS can be upgraded (*flashed*).

1. From the Advanced System Management window, click **Options -> Update Microcode -> System** as shown in Figure 201:

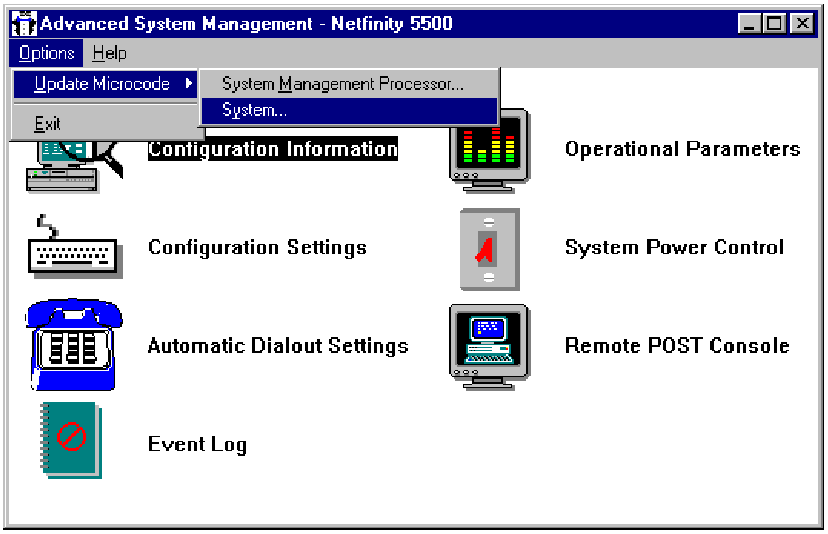


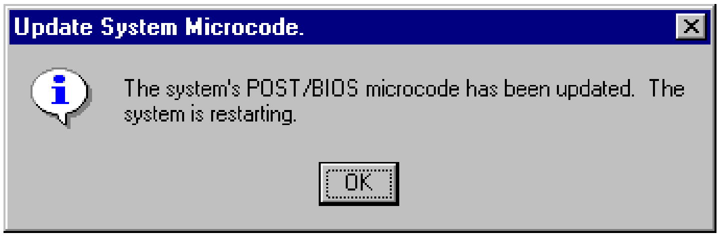
Figure 201. Starting the BIOS Update Process

2. At this point you'll be prompted to confirm the update of the system's BIOS. Click **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 **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 202.

   Note: The actual download of BIOS data to the server can take five to 10 minutes.



The system's POST/BIOS microcode has been updated. The system is restarting.

Figure 202. 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. Examine the System State field.

7.8.2 Summary

The remote update of the Netfinity 5500's BIOS can be performed only when dialled in from another Netfinity Manager workstation. It can also be performed only when the server is powered down.

7.9 Example 9: Dialout via RS-485

This example describes how to set up the ASM processor in the interconnect network to generate alerts and dialout passed through the RS-485 in the event of an operating system timeout.

We have two Netfinity 5000s, one Netfinity 7000 M10 (with ASM PCI adapter) and a modem. If any server fails (operating system traps, abends or hangs), the ASM processor will attempt to restart the server and forward an alert message to a remote system via a modem connected to one of the 5000s.

We will do the following:

1. Connect the servers to the ASM interconnect bus.
2. Set the O/S timeout value in Advanced System Management.
3. Create a dialout entry.
4. Enable remote access.

We will configure all three servers to watch for O/S hangs, and we will configure the modem on one of the 5000s to dial out in case any of the servers hang. The alert will be transmitted via the RS-485 network to the 5000 with the modem.

7.9.1 Install Interconnect Network

Before you can configure the interconnect network, you need three interconnect cable kit options (03K9309), one for each server. If it has been previously configured, you can skip this step.

1. Install interconnect cable kits in each server. For details on installation see 3.4, “ASM Interconnect Network” on page 80.
2. Connect the servers to the ASM interconnect bus using standard UTP cable with RJ-45 connectors at both ends so that the three servers are connected to the ASM interconnect bus as shown in Figure 203:

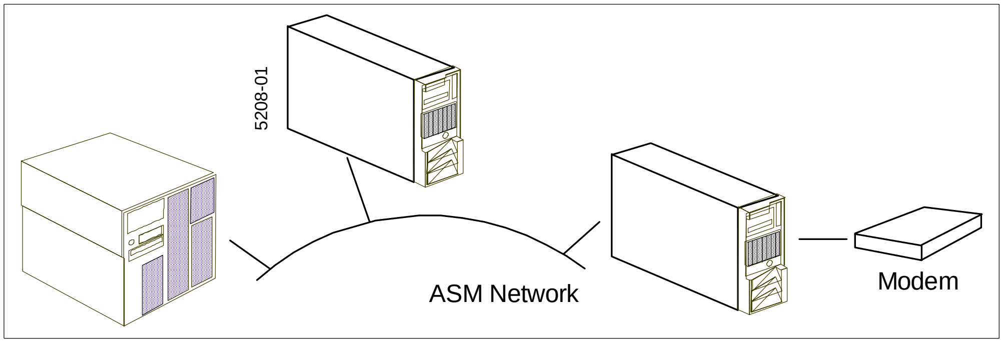


Figure 203. Example Configuration

   Note: The cable length can be at most 300 feet between first and last ASM devices.

3. Attach the modem to one of the servers. In this example, we connected it to the dedicated management serial port, COM C, on one of the Netfinity 5000s.

   Note: For redundancy purposes in a production environment, you could use two modems and connect them to two different servers (such as the COM C ports on the two 5000s or a 5000 and the ASM PCI adapter on the 7000 M10).

7.9.2 Configure the O/S WatchDog on Each Server

You now need to configure the O/S WatchDog in the Advanced System Management in Netfinity Manager for each ASM device.

1. Start Netfinity Manager.
2. Double-click **Advanced System Management**. Figure 204 appears:

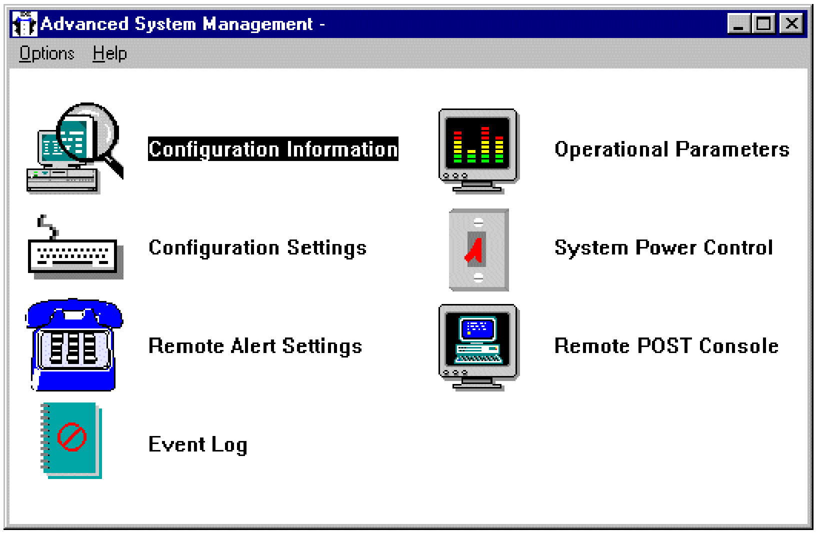
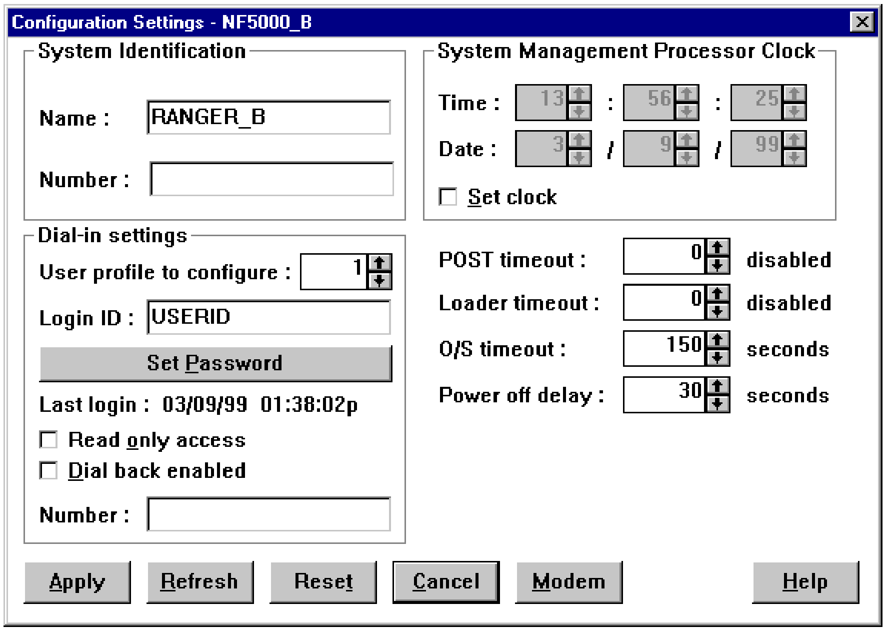


Figure 204. Service Processor Manager Window

3. Double-click **Configuration Settings**. Figure 205 appears:



Configuration Settings - NF5000_B

System Identification

Name : RANGER_B

Number :

System Management Processor Clock

Time : 13 : 56 : 25

Date : 3 / 9 / 99

□ Set clock

Dial-in settings

User profile to configure : 1

Login ID : USERID

Last login : 03/09/99 01:38:02p

□ Read only access

□ Dial back enabled

Number :

POST timeout : 0 disabled

Loader timeout : 0 disabled

O/S timeout : 150 seconds

Power off delay : 30 seconds

Figure 205. Configuration Settings

4. Enter a value in the O/S timeout field.

   This is the number of seconds that the ASM processor will allow for the system's operating system to stop responding before generating an O/S timeout event. Since we have enabled the WatchDog timer, if the O/S takes longer than the configured amount of time to respond, the ASM processor will attempt to restart the system.

The number you set here (the range is 150-255 seconds) 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.

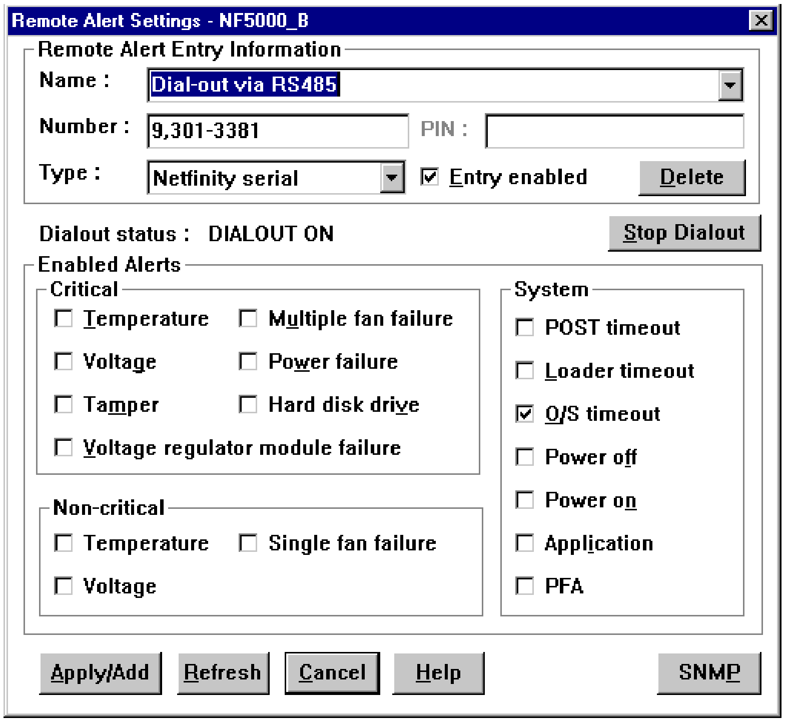
See 4.2.3, “Configuration Settings” on page 108 for information about the rest of this window.

5. Click **Apply** then **Cancel** to exit the window.

7.9.3 Configuring a Dialout Entry

Now that the O/S timeout has been enabled, we now configure an alert to be sent via modem. The modem is attached to the Netfinity 5000, but we configure the alert on all servers on the ASM interconnect bus.

1. From the Advanced System Management window, double-click **Remote Alert Settings**. Figure 206 appears:



Remote Alert Settings - NF5000_B

Remote Alert Entry Information

Name : Dial-out via RS485

Number : 9,301-3381

PIN :

Type : Netfinity serial

☑ Entry enabled

Dialout status : DIALOUT ON

Enabled Alerts

Critical

☐ Temperature
☐ Multiple fan failure
☐ Voltage
☐ Power failure
☐ Tamper
☐ Hard disk drive
☐ Voltage regulator module failure

Non-critical

☐ Temperature
☐ Single fan failure
☐ Voltage

System

☐ POST timeout
☐ Loader timeout
☑ O/S timeout
☐ Power off
☐ Power on
☐ Application
☐ PFA

Figure 206. Dialout Settings

2. Type in a phone number and a descriptive name.

3. Select **Netfinity serial** 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 **Apply/Add** to add the entry then **Cancel** to exit the window.

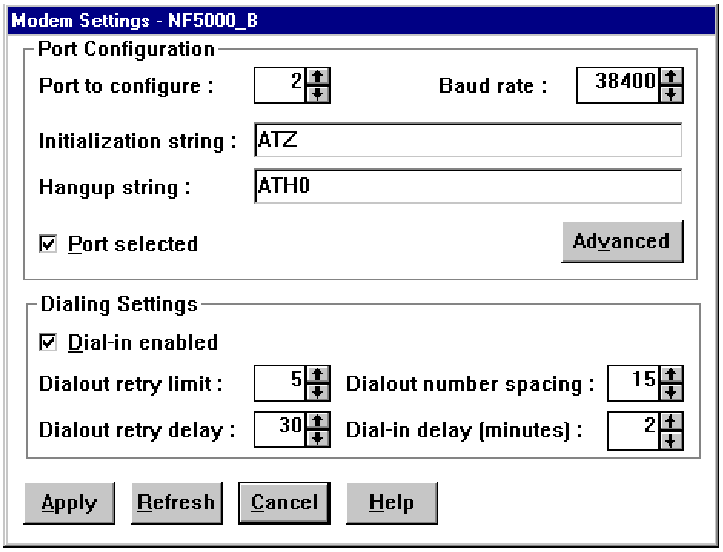
For more information about this window see 4.2.6, “Remote Alert Settings” on page 117.

Note: For configuring another ASM device, you can log on to a selected ASM device using Dynamic Connection Manager. See 3.4.3, “Access with Netfinity Manager” on page 82.

7.9.4 Configure the Modem on the Netfinity 5000

The next step is to configure the modem on the Netfinity 5000 where the modem is attached. The other two servers will be able to use the modem resource automatically because they are all attached to the ASM interconnect bus. See 3.4.5, “Sending Alerts Through Shared Resources” on page 84 for details.

1. From the Advanced System Management service, double-click **Configuration Settings**.
2. Click the **Modem** button for the modem settings. Figure 207 appears:



Modem Settings - NF5000_B

Port Configuration

Port to configure : 2

Baud rate : 38400

Initialization string : ATZ

Hangup string : ATH0

☑ Port selected

Dialing Settings

☑ Dial-in enabled

Dialout retry limit : 5

Dialout number spacing : 15

Dialout retry delay : 30

Dial-in delay (minutes) : 2

Figure 207. Modem Settings

3. Check **Port selected** in the port configuration to enable the port. See 4.2.4, “Port and Dialing Settings” on page 112 for details of this window.
4. Click **Apply** then **Cancel** to close the window.

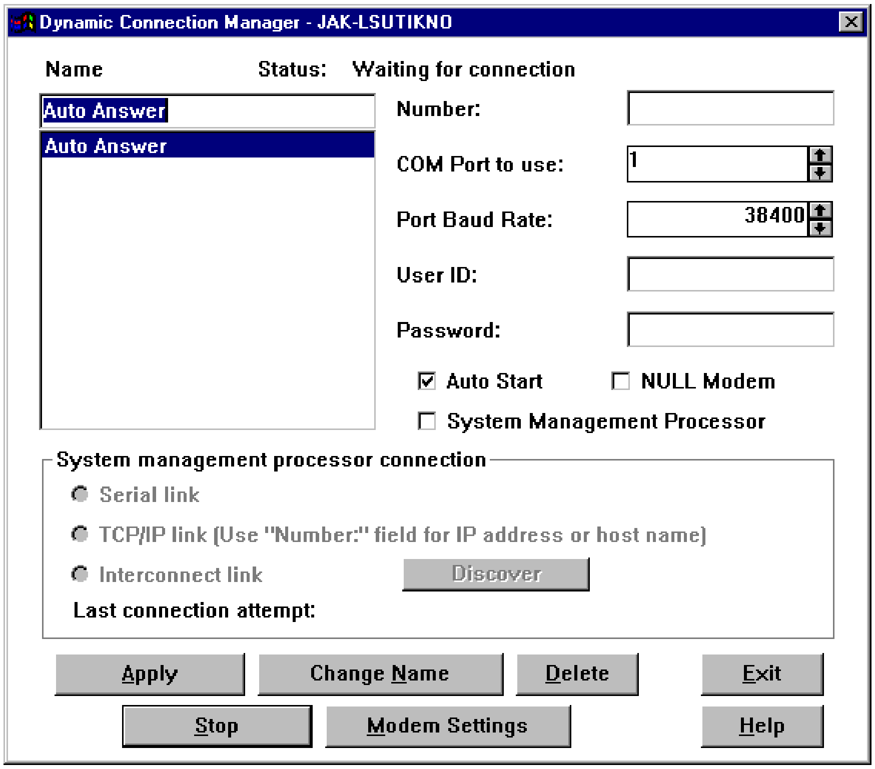
7.9.5 Enabling the Remote Alert Receiver

Now that the servers have been configured to issue the alert via the modem attached to one of them, the next step is to configure the receiving system. This Netfinity Manager system also has a modem attached and will receive the alert from the Netfinity 5000.

To achieve this, the remote system needs to be enabled to auto answer. Once this is set the Dynamic Connection Manager service will automatically answer incoming phone calls (alerts) through the modem and establish a serial link with the calling system through Netfinity Manager.

To set the Dynamic Connection Manager service to auto answer mode on the remote system:

1. Start the Dynamic Connection Manager service. Figure 208 appears:



Dynamic Connection Manager - JAK-LSUTIKNO

Name: Auto Answer

Status: Waiting for connection

Number:

COM Port to use: 1

Port Baud Rate: 38400

User ID:

Password:

☑ Auto Start ☐ NULL Modem

☐ System Management Processor

System management processor connection

○ Serial link

○ TCP/IP link (Use "Number:" field for IP address or host name)

○ Interconnect link

Last connection attempt:

Figure 208. Dynamic Connection Manager

2. Select **Auto Answer** from the Name field. Since we want the Dynamic Connection Manager service to automatically start and wait for incoming calls, click the **Auto Start** check box.

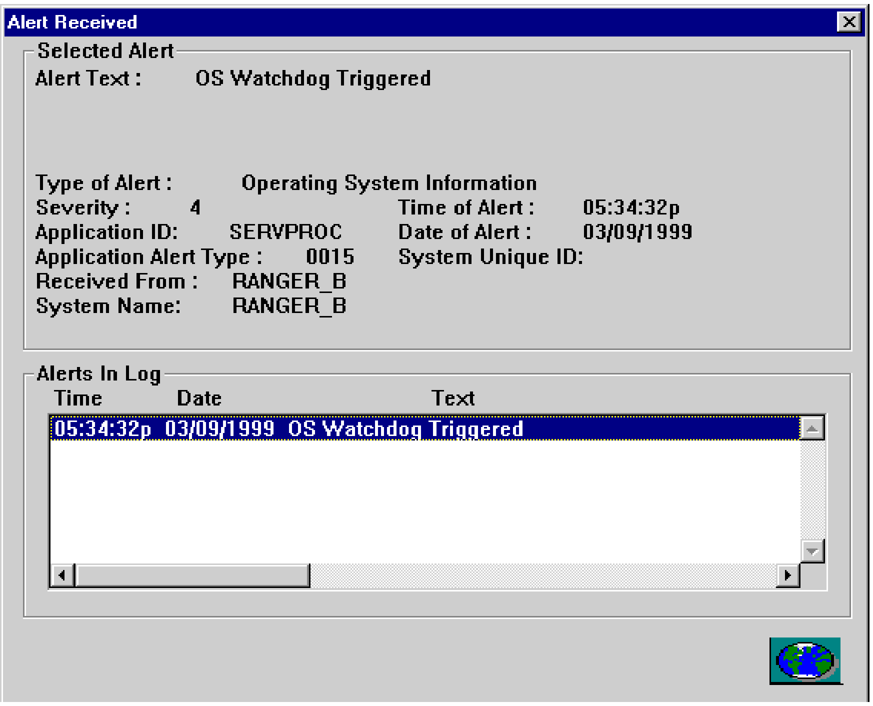
3. Click **Apply** to save the changes then **Start**. The Dynamic Connection Manager service will begin waiting for incoming calls.

   Once “Waiting for connection” appears in the status field, you can click on **Exit**. Dynamic Connection Manager will continue to wait in the background for incoming calls. Click **Stop** if you want to terminate the “Waiting for connection” status.

7.9.6 Running the Scenario

The ASM processor in each of the servers 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 ASM processor assumes an operating system timeout.

If this happens, the WatchDog process will wait for the amount of time you selected in O/S timeout and if no further responses from the operating system are received, it initiates a system restart and sends an alert to the modem on the Netfinity 5000 using the RS-485 ASM interconnect bus. A message similar to the one in Figure 209 will be forwarded to the remote Netfinity Manager system.



Alert Received

Selected Alert

Alert Text : OS Watchdog Triggered

Type of Alert : Operating System Information
Severity : 4
Time of Alert : 05:34:32p
Application ID: SERVPROC
Date of Alert : 03/09/1999
Application Alert Type : 0015
System Unique ID:
Received From : RANGER_B
System Name: RANGER_B

Alerts In Log

Time	Date	Text
05:34:32p	03/09/1999	OS Watchdog Triggered

Figure 209. Service Processor O/S Timeout Alert

You could then process the alert as follows:

- Send a message via network messaging to all users logged on to the domain informing them of the restarted server.
- Notify the administrator so he/she can ensure the server restarted correctly.
- The administrator could dial back in to through the same modem and connect to the failed server through the interconnect network. Diagnostics could then be remotely performed:
  – Using the Event Log, get more information for further diagnostics.
  – Using System Power Control, enable power control options for power off and restart the system.
  – Using Remote POST Console, monitor the boot process and change the configurations as needed to make sure the server goes back to normal operation.

7.10 Example 10: Reboot a Server through a Web Browser Interface

This example uses the following features of the Advanced System Management Processor in the Netfinity 5000 and the Advanced System Management PCI Adapter in the Netfinity 7000 M10:

- Web browser access to the ASM PCI adapter
- RS-485 connection between the ASM PCI adapter and ASM processor
- Ability to remotely shut down and reboot a server

The scenario is as follows. Users complain about printing. Print jobs are stuck and the print queue has filled up. It seems that your NetWare print server (a Netfinity 5000) may not be well. You decided the best course of action is to reboot the print server. Unfortunately, you are in one of your branch offices when you received the phone call and while the branch has an intranet connection, there aren’t any computers with Netfinity Manager installed. There also isn’t anyone near the servers that can help.

The NetWare print server is running IPX only (no TCP/IP). Fortunately, you have another server next to it, a Netfinity 7000 M10. Its ASM PCI adapter is connected to the intranet via the built-in Ethernet port. You’ve also configured the two servers to be connected together via an RS-485 connection.

The solution is as follows:

1. Use a Web browser to connect to the ASM PCI adapter in the 7000 M10.
2. Connect to the ASM processor in the Netfinity 5000 using the RS-485 link.
3. Reboot the server.

For information about the RS-485-based ASM interconnect bus, see 3.4, “ASM Interconnect Network” on page 80. For information about the use of a Web browser, see 3.4.4, “Access with Web Browser/Telnet Client/ANSI Terminal” on page 84.

7.10.1 Configure the ASM PCI Adapter and ASM Processor

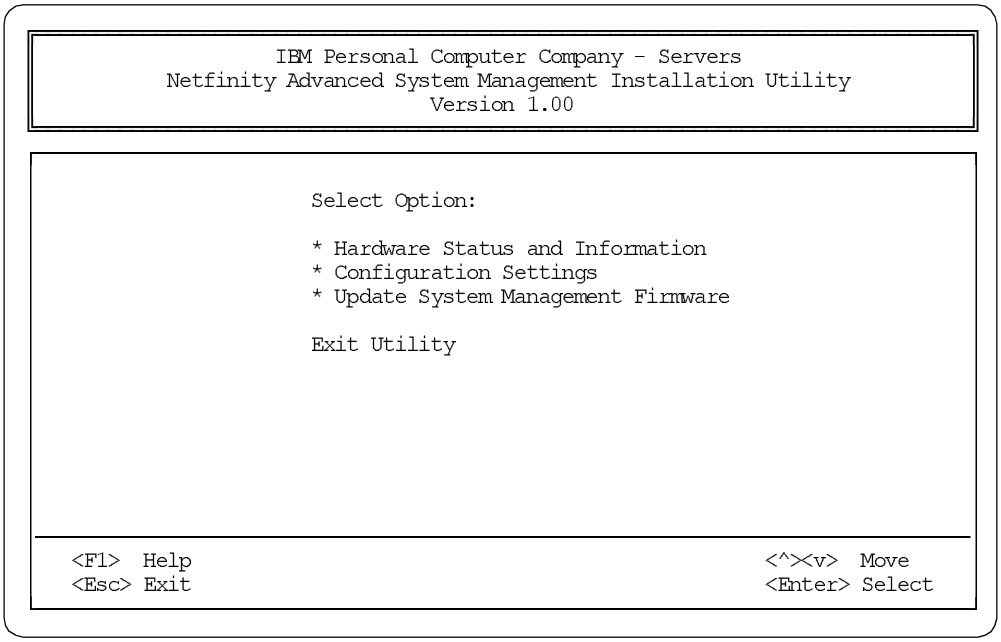
We begin our scenario a couple of days before the phone call.

You’ve just received the Netfinity 5000 and Netfinity 7000 M10 and installed your operating systems. The Netfinity 5000 is a print server only and you didn’t install Netfinity Manager on it. The Netfinity 7000 M10 is the main production server, running Microsoft Windows NT 4.0 with Netfinity Manager installed. You have updated all BIOS and firmware to the latest level.

7.10.1.1 Configure the Netfinity 5000

Perform the following steps:

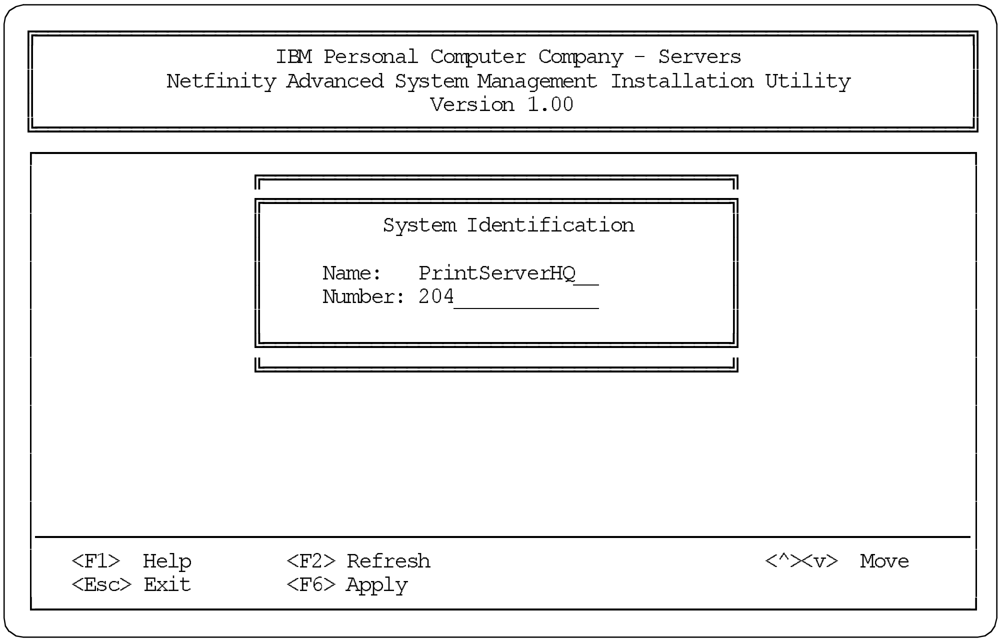
1. Boot your server with the Advanced System Management Installation Utility diskette. Figure 210 appears:



```
                  IBM Personal Computer Company - Servers
         Netfinity Advanced System Management Installation Utility
                               Version 1.00

                        Select Option:

                        * Hardware Status and Information
                        * Configuration Settings
                        * Update System Management Firmware

                        Exit Utility

   <F1>  Help                                             <^><v>  Move
   <Esc> Exit                                             <Enter> Select
```

Figure 210. Main Menu Screen

2. Highlight **Configuration Settings** and press Enter.
3. Highlight **System Identification** and press Enter. Figure 211 appears:



```
                  IBM Personal Computer Company - Servers
         Netfinity Advanced System Management Installation Utility
                               Version 1.00

                         System Identification

                      Name:   PrintServerHQ__
                      Number: 204____________

   <F1>  Help        <F2> Refresh                         <^><v>  Move
   <Esc> Exit        <F6> Apply
```

Figure 211. System Identification

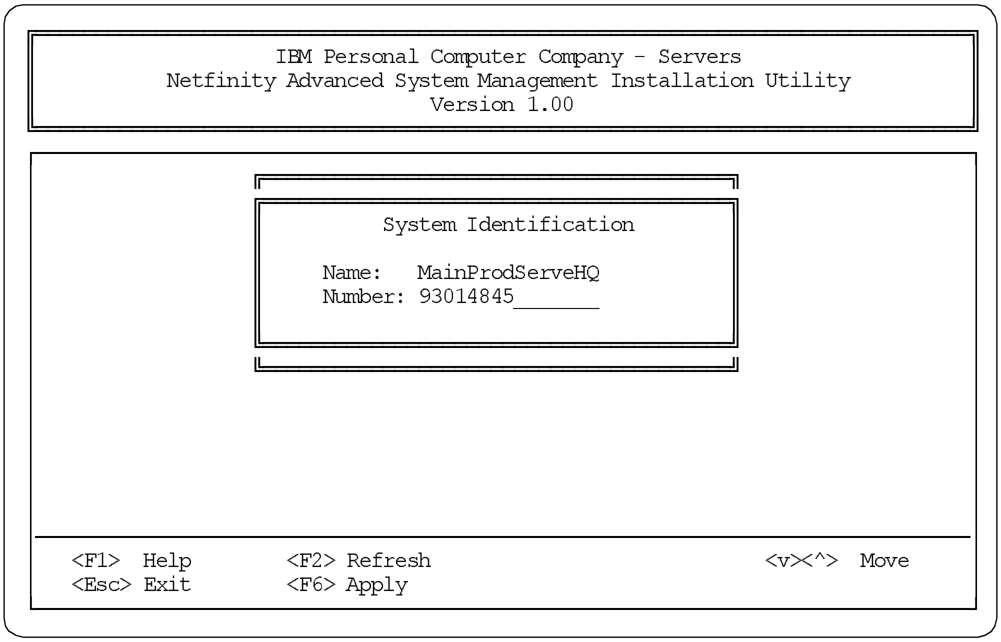
4. Enter your system name and system number. The number can be a phone number, a department number or some other form of identification.
5. Press F6 to save the changes.
6. Exit the program and reboot the server.

The setup for the Netfinity 5000 is complete.

7.10.1.2 Configure Your Netfinity 7000 M10

Perform the following steps:

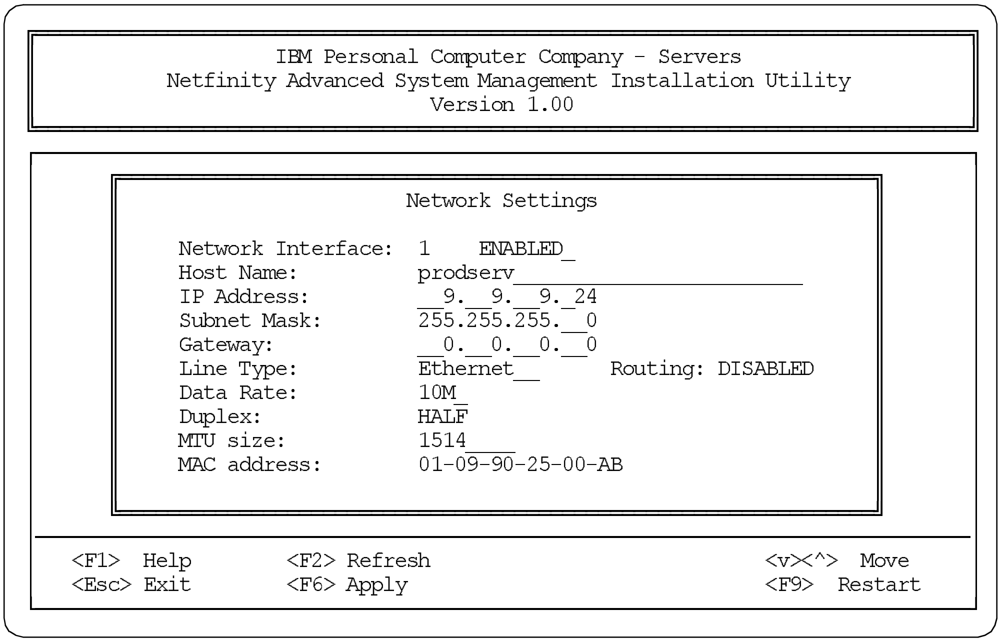
1. Boot your server with the Advanced System Management Installation Utility diskette.
2. Select Configuration Settings and press Enter.
3. Select System Identification and press Enter.
4. Type in a name and number for the server as you did for the Netfinity 5000, as shown in Figure 212:



```
                 IBM Personal Computer Company - Servers
         Netfinity Advanced System Management Installation Utility
                              Version 1.00

                          System Identification

                      Name:   MainProdServeHQ
                      Number: 93014845________

   <F1>  Help       <F2> Refresh                         <v><^>  Move
   <Esc> Exit       <F6> Apply
```

Figure 212. System Identification

5. Press F6 to save the changes and exit the window.
6. Highlight **Network Settings** and press Enter. Figure 213 appears:



```
              IBM Personal Computer Company - Servers
     Netfinity Advanced System Management Installation Utility
                           Version 1.00

                         Network Settings

       Network Interface:  1    ENABLED_
       Host Name:          prodserv________________________
       IP Address:         __9.__9.__9._24
       Subnet Mask:        255.255.255.__0
       Gateway:            __0.__0.__0.__0
       Line Type:          Ethernet__      Routing: DISABLED
       Data Rate:          10M_
       Duplex:             HALF
       MTU size:           1514____
       MAC address:        01-09-90-25-00-AB

   <F1>  Help       <F2> Refresh                        <v><^>  Move
   <Esc> Exit       <F6> Apply                          <F9>  Restart
```

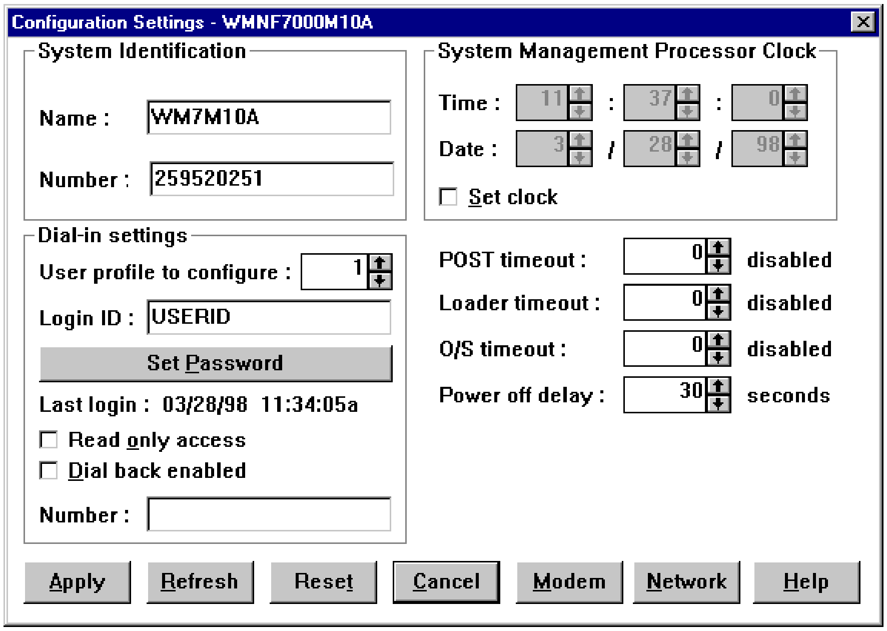
Figure 213. ASM PCI Adapter Network Settings

7. Set each of the fields in the window to configure the ASM PCI adapter into your network. See 3.3.4.2, “Configuration Settings” on page 77 for details of the options.
8. Press F6 to save the changes.
9. Exit the program and restart the server.

7.10.1.3 Password Consideration

After you finished the steps above your system is ready to be used in an TCP/IP-RS-485 environment. However, no changes have been made to the user ID and password. As mentioned earlier, the default user ID is USERID (uppercase) and the default password is PASSW0RD (with a zero). If you want to create additional users you need to use Netfinity Manager:

1. From Netfinity Manager, open the Advanced System Management window and double-click **Configuration Settings**. Figure 214 appears:



Configuration Settings - WMNF7000M10A

System Identification

Name : WM7M10A

Number : 259520251

System Management Processor Clock

Time : 11 : 37 : 0

Date : 3 / 28 / 98

□ Set clock

Dial-in settings

User profile to configure : 1

Login ID : USERID

Last login : 03/28/98 11:34:05a

□ Read only access

□ Dial back enabled

Number :

POST timeout : 0 disabled

Loader timeout : 0 disabled

O/S timeout : 0 disabled

Power off delay : 30 seconds

Figure 214. Configuration Setting in Netfinity Manager

2. Use the **User profile to configure** spin buttons change to the next profile number. Enter a new name for Login ID and click **Set Password**. Enter and confirm the new password.
3. After you have created the password click **Apply**. It is important not to forget to click **Apply**. If you close the window before doing so, all changes will be lost.

Note: You may want to consider replacing User profile 1 rather than adding an additional user profile. This will improve security.

7.10.2 Running the Scenario

We are now back in the present. You are at the branch office. You get the call that printing appears to be down and decide that rebooting the print server is the best course of action. The servers are in a locked room and there's no one there who can access them.

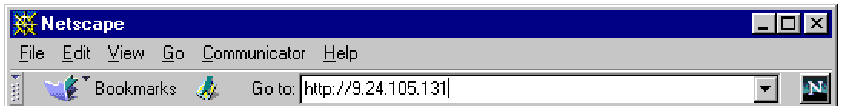
You remembered you read about an almost identical scenario in an IBM Redbook and how the guys in the book came through with the solution.

Because there is no direct access to the print server from the branch office, you need to connect somehow to that server. Fortunately, you had decided to set up an RS-485 interconnect network. You know you can access an ASM PCI adapter via TCP/IP and connect from it to your print server and you know you can use a Web browser.

7.10.2.1 Connect to the Server

To connect to the server, you do the following:

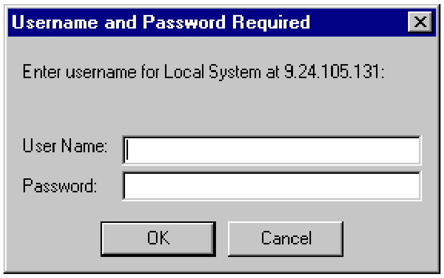
1. Fire up your Web browser and point it to the IP address of the ASM PCI adapter installed in the Netfinity 7000 M10 as shown in Figure 215:



Go to: http://9.24.105.131

Figure 215. Enter the ASM PCI adapter IP Address

2. After a connection is established you are prompted for a user ID and password as shown in Figure 216:


Username and Password Required

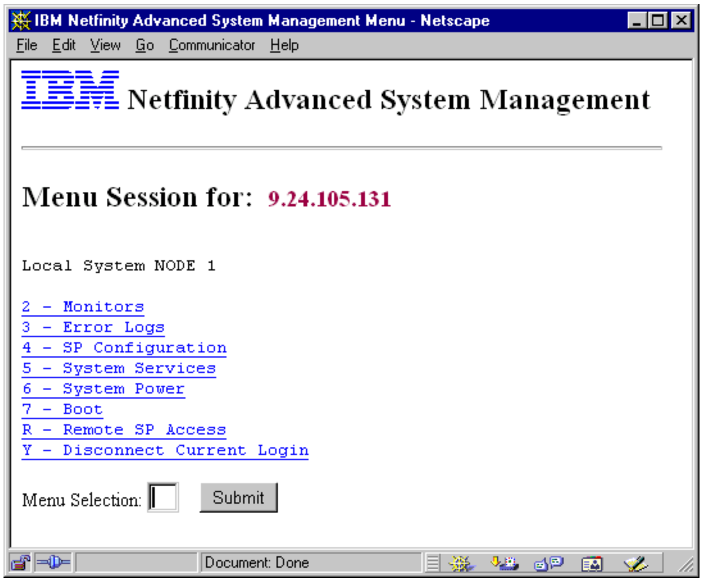
Enter username for Local System at 9.24.105.131:

User Name:

Password:

Figure 216. Enter your User ID and Password

3. After you have logged in you see the main menu as shown in Figure 217:


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help

IBM Netfinity Advanced System Management

Menu Session for: 9.24.105.131

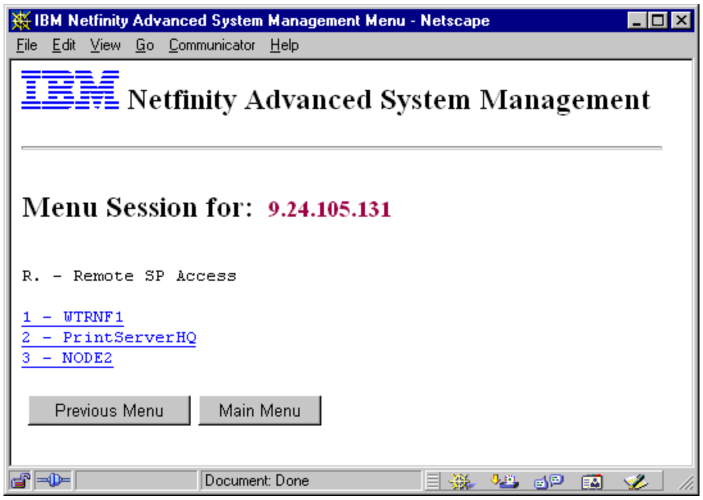
```
Local System NODE 1

2 - Monitors
3 - Error Logs
4 - SP Configuration
5 - System Services
6 - System Power
7 - Boot
R - Remote SP Access
Y - Disconnect Current Login
```

Menu Selection:

Figure 217. Main Menu Selection

4. You need to connect to a remote service processor. Therefore, click **R-Remote SP Access**.

5. Figure 218 appears, giving you a selection of all ASM devices on your RS-485 network:


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help
Previous Menu
Main Menu
Document: Done

IBM Netfinity Advanced System Management

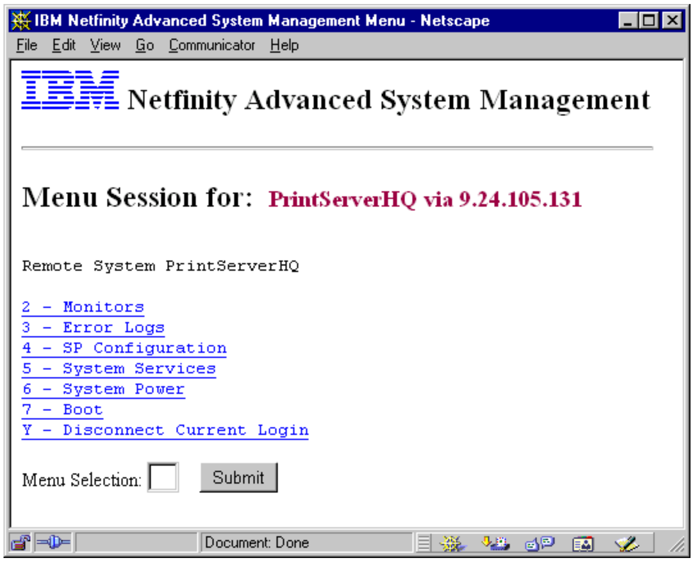
Menu Session for: 9.24.105.131

R. - Remote SP Access

1 - WTRNF1
2 - PrintServerHQ
3 - NODE2

Figure 218. Accessible Devices on Your RS-485 Network

6. You click your print server, **2-PrintServerHQ**.
7. You are again prompted for a user ID and password, but this time for the ASM processor on the Netfinity 5000 PrintServerHQ. After you identified yourself, a menu Web page appears as in Figure 219:


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help
Submit
Document: Done

IBM Netfinity Advanced System Management

Menu Session for: PrintServerHQ via 9.24.105.131

Remote System PrintServerHQ

2 - Monitors
3 - Error Logs
4 - SP Configuration
5 - System Services
6 - System Power
7 - Boot
Y - Disconnect Current Login

Menu Selection: □

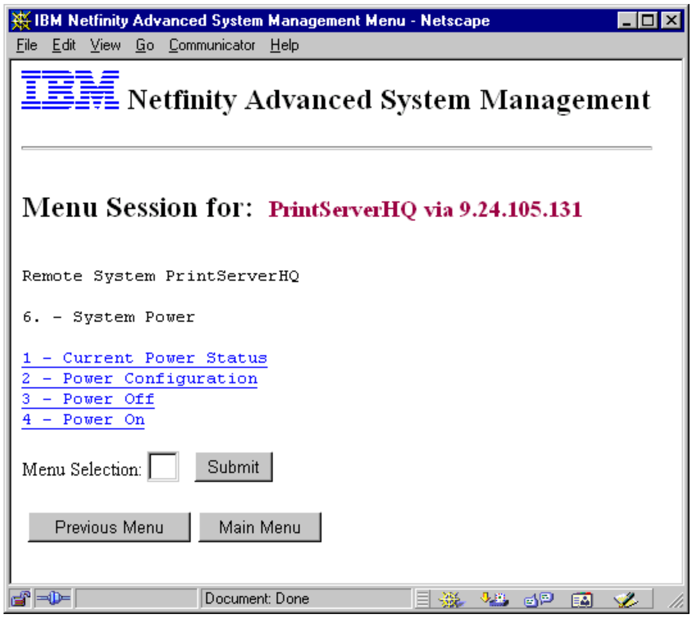
Figure 219. Now Connected to the Print Server

As you can see from the “Menu Session for:” field, you’ve now connected to the print server via the ASM PCI adapter in the Netfinity 7000 M10.

7.10.2.2 Check Server Status

The next step is to check the status of the PrintServerHQ server. You want to know if the server is still powered on. You click **6-System Power** from Figure 219.

Figure 220 appears showing the sub menu for system power:


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help
IBM Netfinity Advanced System Management

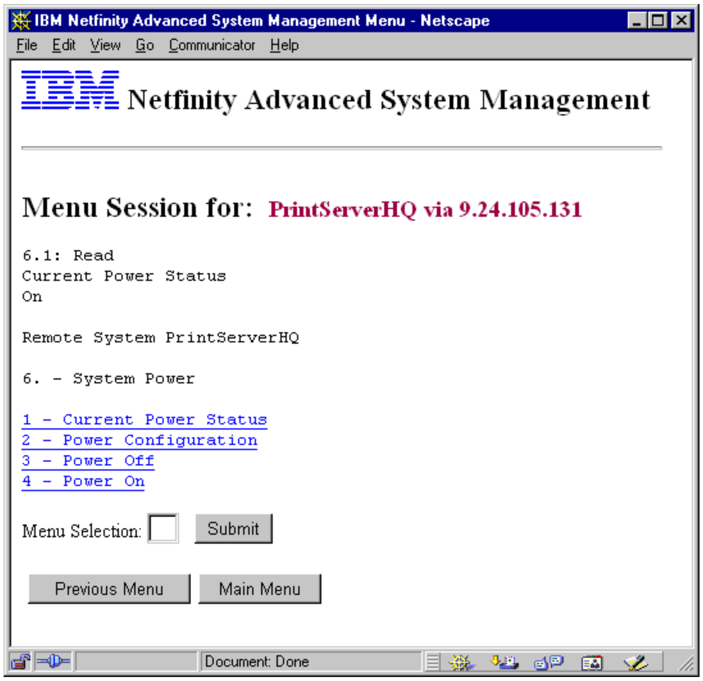
Menu Session for: PrintServerHQ via 9.24.105.131

```
Remote System PrintServerHQ

6. - System Power

1 - Current Power Status
2 - Power Configuration
3 - Power Off
4 - Power On
```

Menu Selection:
Submit
Previous Menu
Main Menu
Document: Done

Figure 220. System Power Sub Menu

You want to know the current status of the server and click **1-Current Power Status** then click **2-Read**. Figure 221 appears showing the current power status and returns you to the System Power menu:


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help
IBM Netfinity Advanced System Management

Menu Session for: PrintServerHQ via 9.24.105.131

```
6.1: Read
Current Power Status
On

Remote System PrintServerHQ

6. - System Power

1 - Current Power Status
2 - Power Configuration
3 - Power Off
4 - Power On
```

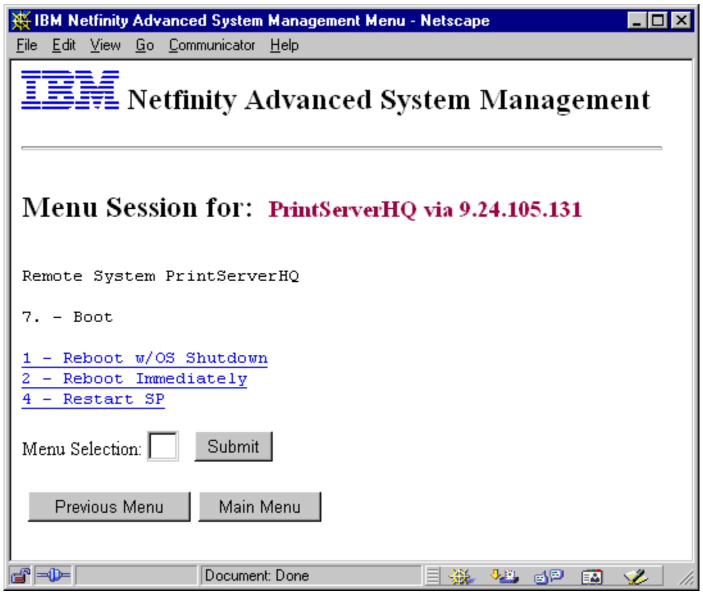
Menu Selection:
Submit
Previous Menu
Main Menu
Document: Done

Figure 221. Current System Power Status

7.10.2.3 Reboot the Server

You know now that your server is powered on. Now you initiate a reboot with a clean operating system shutdown:

1. Click **Main Menu** which brings the main function menu for the print server.
2. Click **7-Boot**. Figure 222 appears:


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help
IBM Netfinity Advanced System Management

Menu Session for: PrintServerHQ via 9.24.105.131

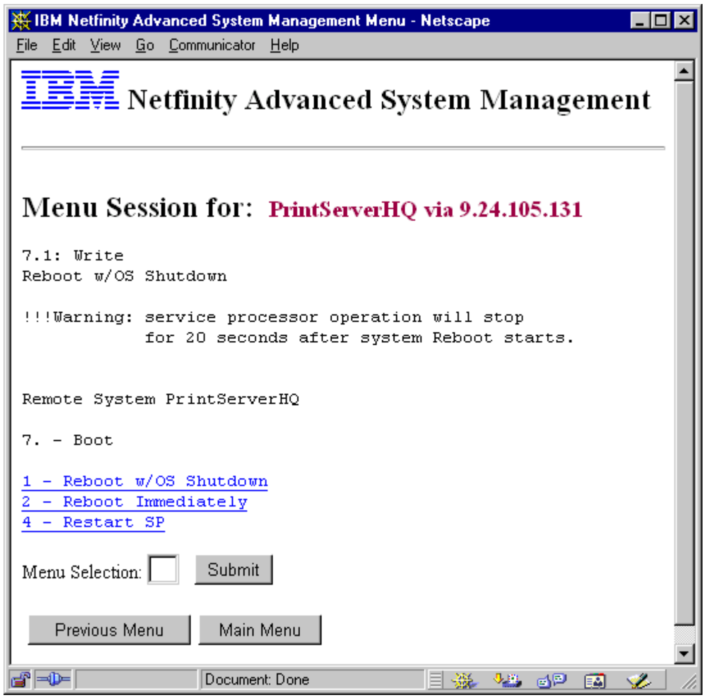
```
Remote System PrintServerHQ

7. - Boot

1 - Reboot w/OS Shutdown
2 - Reboot Immediately
4 - Restart SP
```

Menu Selection:
Submit
Previous Menu
Main Menu
Document: Done

Figure 222. Remote Boot

3. Click **1-Reboot w/OS Shutdown** then click **0-Write** to initiate the reboot.

You are returned to the previous menu with a warning about the ASM processor as shown in Figure 223. The warning says the print server's ASM processor will not be available for approximately 20 seconds.


IBM Netfinity Advanced System Management Menu - Netscape
File Edit View Go Communicator Help
IBM Netfinity Advanced System Management

Menu Session for: PrintServerHQ via 9.24.105.131

```
7.1: Write
Reboot w/OS Shutdown

!!!Warning: service processor operation will stop
            for 20 seconds after system Reboot starts.


Remote System PrintServerHQ

7. - Boot

1 - Reboot w/OS Shutdown
2 - Reboot Immediately
4 - Restart SP
```

Menu Selection:
Submit
Previous Menu
Main Menu
Document: Done

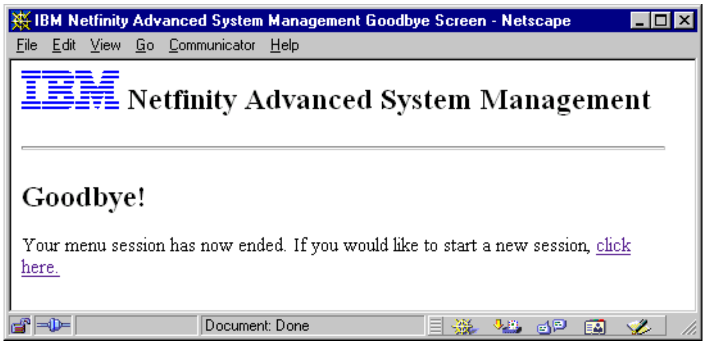
Figure 223. Reboot in Progress

Now you want to see whether the restart was successful. Repeat the steps in 7.10.2.2, “Check Server Status” on page 256.

7.10.2.4 Terminate the Session

Once you have finished working on the print server, you should disconnect the browser. Return to the main menu by clicking the **Main Menu** button, then click **Y-Disconnect Current Login**.

The browser will then disconnect from the print server and return to the production server. You should then click **Y-Disconnect Current Login** again to log out completely. You should then see Figure 224:


IBM Netfinity Advanced System Management Goodbye Screen - Netscape
File Edit View Go Communicator Help
IBM Netfinity Advanced System Management
Document: Done

Goodbye!

Your menu session has now ended. If you would like to start a new session, click here.

Figure 224. Exit from the ASM PCI Adapter

7.10.3 Summary

The following steps are necessary to enable the reboot of a remote server without using Netfinity Manager:

1. Configure all systems.
2. Connect all systems through LAN and RS-485.
3. Create new user IDs.
4. Use a Web browser to connect through TCP/IP to an RS-485 network.
5. Check the server status.
6. Reboot the server.
7. Check the success of the operation.

7.11 Example 11: Using Telnet to View Remote POST

This example will show you how to set up your Advanced System Management PCI Adapter to use in a Telnet session to watch the POST on a remote server. Most of the configuration steps are discussed in 7.10, “Example 10: Reboot a Server through a Web Browser Interface” on page 250.

In 7.10, “Example 10: Reboot a Server through a Web Browser Interface” on page 250 we ended with the reboot of your print server. This time it is your main production server that is in trouble. You are still in your local branch. You receive a phone call from your proxy telling you the server has a blue screen of death and nothing works.

The plan is as follows:

1. Telnet into the ASM PCI adapter installed in the server.
2. Restart the server.
3. Watch the server’s POST messages.

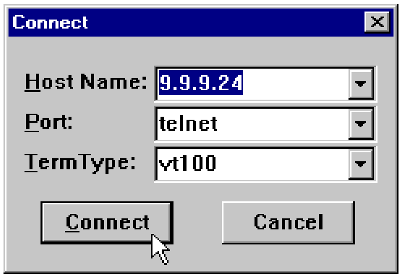
7.11.1 Connect to and Restart the Server

All configuration steps necessary have been done in the previous example. You remember reading in the redbook about Remote POST Control via Telnet and you’ve always wanted to try it.

1. Open a Telnet session on the secretary’s workstation:

   ```
   telnet
   ```

2. After the Telnet window opens, you click **Connect** from the menu bar. The connection window opens (Figure 225) and you enter ProdServHQ’s IP address in Host Name. Use the defaults for the other fields.

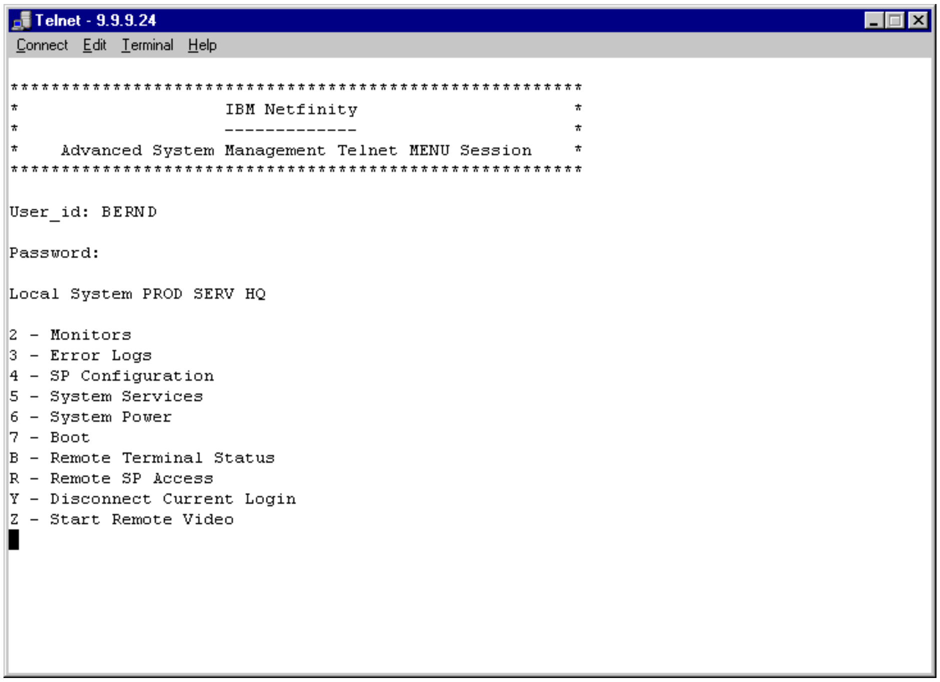


Host Name: 9.9.9.24
Port: telnet
TermType: vt100

Figure 225. Connection Window

3. Click **Connect.** Next you will be presented with your Netfinity 7000 M10 ASM PCI adapter login screen where you enter your user ID and password.

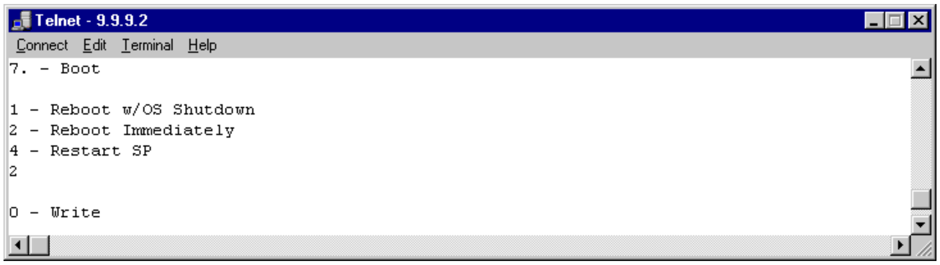
   The options in the Telnet session are the same as those in the Web browser except that Start Remote Video is now available.



```
*********************************************************
*                    IBM Netfinity                      *
*                    -------------                      *
*    Advanced System Management Telnet MENU Session     *
*********************************************************

User_id: BERND

Password:

Local System PROD SERV HQ

2 - Monitors
3 - Error Logs
4 - SP Configuration
5 - System Services
6 - System Power
7 - Boot
B - Remote Terminal Status
R - Remote SP Access
Y - Disconnect Current Login
Z - Start Remote Video
```

Figure 226. Telnet Window

4. Press 7 to access the boot menu as shown in Figure 227.



```
7. - Boot

1 - Reboot w/OS Shutdown
2 - Reboot Immediately
4 - Restart SP
2

0 - Write
```

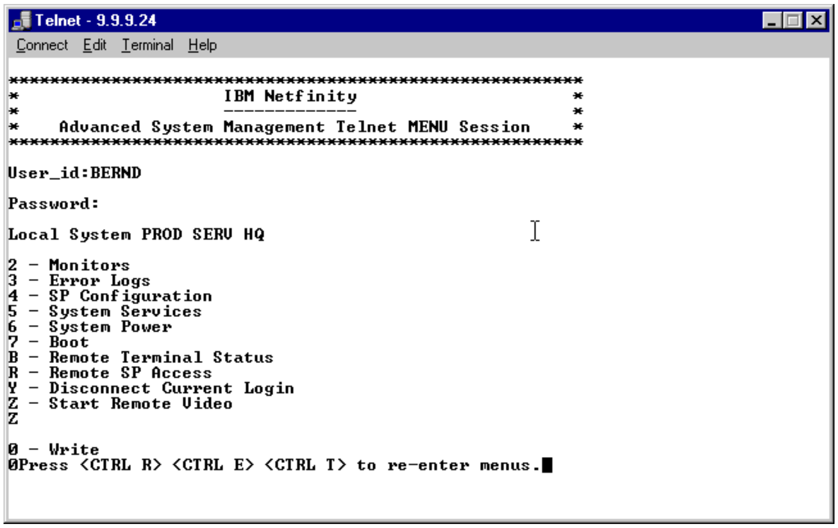
Figure 227. Boot Sub Menu

5. The server has already crashed so press 2 to reboot the server immediately. Press 0 to send the command to the ASM PCI adapter.
6. The reboot sequence is started and you are back in the 7-Boot sub menu. Now you press the Escape key in order to go back to the main menu.

It’s time to start the remote video sequence.

7.11.2 Start the POST Console

At the main menu, press Z to start the remote POST function. The Telnet session will look like Figure 228:

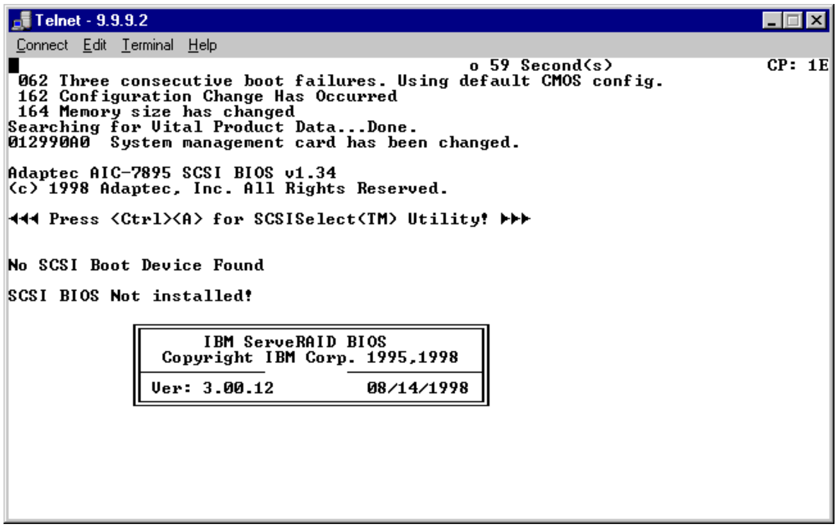


```
********************************************************
*                    IBM Netfinity                     *
*                    -------------                     *
*    Advanced System Management Telnet MENU Session    *
********************************************************

User_id:BERND

Password:

Local System PROD SERV HQ

2 - Monitors
3 - Error Logs
4 - SP Configuration
5 - System Services
6 - System Power
7 - Boot
B - Remote Terminal Status
R - Remote SP Access
Y - Disconnect Current Login
Z - Start Remote Video
Z

0 - Write
0Press <CTRL R> <CTRL E> <CTRL T> to re-enter menus.
```

Figure 228. Wait for Remote Video

As soon as the POST sequence starts, the screen clears and you see the standard POST messages that you would on the server monitor, except for the IBM logo. Now you have full control over the server's setup and configuration utility, diagnostics, Adaptec and ServeRAID ROM-based configuration utilities.

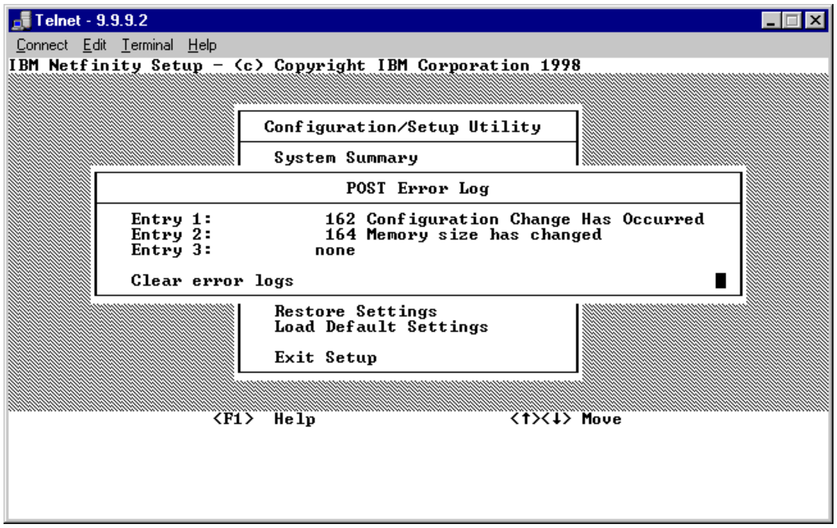
As you see from the POST messages, your server has developed a fault (Figure 229):



```
                                             o 59 Second(s)               CP: 1E
 062 Three consecutive boot failures. Using default CMOS config.
 162 Configuration Change Has Occurred
 164 Memory size has changed
Searching for Vital Product Data...Done.
012990A0  System management card has been changed.

Adaptec AIC-7895 SCSI BIOS v1.34
(c) 1998 Adaptec, Inc. All Rights Reserved.

◄◄◄ Press <Ctrl><A> for SCSISelect(TM) Utility! ►►►


No SCSI Boot Device Found

SCSI BIOS Not installed!

             ╔═══════════════════════════════════╗
             ║         IBM ServeRAID BIOS        ║
             ║ Copyright IBM Corp. 1995,1998     ║
             ╟───────────────────────────────────╢
             ║ Ver: 3.00.12           08/14/1998 ║
             ╚═══════════════════════════════════╝
```

Figure 229. ProdServHQ Error Message during POST

The error causes the server to boot into the server configuration utility. Here you check the POST and system error log to find out what has really happened. First you check the POST error log as shown in Figure 230.



```
IBM Netfinity Setup - (c) Copyright IBM Corporation 1998

                    Configuration/Setup Utility

                       System Summary
                              POST Error Log

          Entry 1:           162 Configuration Change Has Occurred
          Entry 2:           164 Memory size has changed
          Entry 3:          none

          Clear error logs

                       Restore Settings
                       Load Default Settings

                       Exit Setup

                 <F1>  Help                  <↑><↓> Move
```

Figure 230. POST Error Log

Next you check the system error log for entries. (You could have used option 3 from the main menu in Figure 228).

Your server problem turns out to be a memory fault. The server has automatically disabled the faulty memory module and the server is now back in business. After you reboot the server again no further error message is displayed. The POST session finishes when the operating system starts.

You return to the main menu by holding down the Crtl key and pressing R E T. From the main menu, press Y and your session will be terminated.

Note: You could have used a terminal session if you had a modem or null modem connected to the ASM PCI adapter’s serial port. All of the above applies to a terminal session too.

7.11.3 Summary

The Telnet facility provides a rather powerful tool for remote troubleshooting. In summary, we have done the following:

1. Configured the adapter during installation time
2. Assigned a name and configured network settings
3. Used Netfinity Manager to create a user ID and a password
4. Connected to the ASM PCI adapter using Telnet
5. Rebooted the server
6. Launched Remote Video
7. Entered the server configuration and setup utility
8. Checked error logs
9. Rebooted the server

Appendix A. Advanced System Management Alerts

Table 45 lists all the alerts generated by the ASM PCI adapter and ASM processor.

Note: This list is a work in progress. It may not list all alerts generated by the ASM hardware. Future updates are planned that will include recommended actions for each alert. Check `http://www.pc.ibm.com/support` for the latest information.

Table 45. Alerts Issued by the ASM Devices

Message	Alert Type	Description
"X" V Bus Fault	Critical	The indicated voltage bus was outside of the recommended range.
"X" V Fault	Critical	The indicated voltage subsystem was outside of the recommended range.
"X" V PCI Fault	Critical	The indicated PCI voltage was beyond the recommended range.
12V "X" Bus Fault	Critical	The indicated 12v bus was beyond the recommended range.
"X" V Planar Fault	Critical	The indicated voltage on the planar was beyond the recommended range.
240V Fault	Critical	Wall input power was beyond the recommended range.
5V "X" Bus Fault	Critical	The indicated voltage subsystem was beyond the recommended range.
5V Continuous ASM Fault	Warning	Continuous power was beyond the recommended range.
5V Fault	Critical	A fault condition was detected on the 5v subsystem.
Advanced System Management PCI Card’s Continuous 5V over recommended value.	Warning	Advanced System Management PCI Card’s Continuous 5V outside recommended values.
Advanced System Management PCI Card’s Continuous 5V under recommended value.	Warning	Advanced System Management PCI Card’s Continuous 5V outside recommended values.
Application Fail	Critical	Netfinity Manager sent a message that one of it’s applications failed.
Application Posted Alert to SP	Critical	Netfinity Manager sent an alert message to the service processor.
Application Warning	Critical	A Netfinity application sent a warning message to the service processor.
BIOS ROM switched to alternate Boot page.	Critical	BIOS ROM switched to alternate Boot page.
BIOS ROM switched to default Boot page.	Critical	BIOS ROM switched to default Boot page.
CD-ROM drive cable is not plugged in.	Critical	CD-ROM drive cable is not plugged in.
CPU "X" Fault	Critical	The indicated CPU had an internal condition.
CPU "X" Invalid Configuration.	Critical	System CPUs configured in slots incorrectly.

Message	Alert Type	Description
CPU "X" Over Temperature	Critical	The indicated CPU had an over temperature condition.
CPU removal detected	Critical	A CPU assembly was removed.
Cable: C2 Security Not Present	Critical	Security cable was not detected.
Cable: Control Panel Not Present	Critical	The cable for the control panel was not detected.
Cable: Diag Panel Not Present	Information	The cable for the diagnostic panel was not detected.
Cable: LED Panel Not Present	Critical	The cable for the LED panel was not detected.
Cable: Power Supply Not Present	Information	The cable for a power supply was not detected.
Cable: Service Processor Not Present	Critical	The cable for the service processor was not present.
DASD "X" Over Temperature	Critical	The indicated Direct Access Storage Device bay was over temperature.
DASD backplane Failure	Warning	The direct access storage device backplane had a failure.
DASD failure	Critical	There was a direct access storage device failure.
DASD over recommended temperature.	Warning	The direct access storage device bay had an over temperature condition.
DASD under recommended temperature.	Warning	The direct access storage device bay had an under temperature condition.
External SCSI cable is not plugged in.	Critical	External SCSI cable is not plugged in.
Failure reading an I2C device, possible bus failure.	Critical	Failure reading an I2C device, possible bus failure.
Fan "X" Failure	Critical	The indicated fan had a failure.
Fan "X" Fault	Critical	The indicated fan was beyond the recommended range.
Fan "X" Outside Recommended Speed.	Critical	The indicated fan’s speed was outside of recommended values.
Fan "X" Present	Information	The indicated fan is present.
Floppy drive cable is not plugged in.	Critical	The floppy drive cable is not plugged in.
Front Panel is not plugged in.	Critical	The front panel is not plugged in.
Hard Drive "X" Fault	Critical	The indicated hard drive had an error.
Hard Drive "X" removal detected.	Critical	The indicated hard drive has been removed.
Host BIST Fail	Information	The Host’s built in self test failed.
Hot plug card is not plugged in.	Critical	Did not detect the indicated hot plugable card.
Internal Error CPU "X" Fault	Critical	The indicated CPU had an internal error.
Internal SCSI cable is not plugged in.	Critical	The internal SCSI cable is not detected.
Loader Watchdog Triggered	Critical	The operating system’s loader did not complete within the allotted time.

Message	Alert Type	Description
Memory Card Not Responding	Critical	The indicated memory card’s I2C subsystem is not responding.
Memory card "X" I2C not responding.	Critical	The indicated memory card’s I2C subsystem is not responding.
Multiple fan failures	Critical	Simultaneous fan failures have been detected.
OS Watchdog Triggered	Critical	The operating system did not respond within an allotted time.
Over Temperature	Critical	An over temperature condition occurred.
PERR on PCI bus "X"	Critical	A parity error occurred on the indicated PCI bus.
PFA Alert, see preceding error in system error log.	Critical	Predictive failure analysis alert. Check the preceding entry in the system error log for more specific information.
PLANAR Over Temperature	Critical	An over temperature condition was detected on the Planar.
POST Watchdog Triggered	Critical	The power on self test did not complete within an allotted time.
Parity Error PCI Bus "X".	Critical	A parity error was reported on the indicated PCI bus.
Planar voltage over/under 3.3V	Critical	The 3.3V for the planar was outside of specifications.
Post Fail	Critical	Power on self test sent a message indicating a failure condition existed.
Post Warn	Critical	Power on self test sent a message indicating a warning condition existed.
Power Good Fault	Critical	The power good signal was not detected.
Power Supply "X" 12V Fault	Critical	The indicated 12V power supply had an error.
Power Supply "X" 3.3V Fault	Critical	The indicated 3.3V power supply had an error.
Power Supply "X" 5V Fault	Critical	The indicated 5V power supply had an error.
Power Supply "X" Current Fault	Critical	Excessive current demand on the indicated power supply.
Power Supply "X" DC Good Fault	Critical	The power good signal was not detected for the indicated power supply.
Power Supply "X" Early Power Off Warning	Critical	The indicated power supply had a condition which caused it to shut off.
Power Supply "X" Fan Fault	Critical	Fan fault in the indicated power supply.
Power Supply "X" Fault	Critical	The indicated power supply had a fault.
Power Supply "X" Temperature Fault	Critical	The indicated power supply had an over temperature condition.
Power supply upgrade present	Information	Supplemental power has been detected.
Primary Processor Bus Fault	Warning	The primary processor has experienced a bus fault.
Processor "X" BIST Fail	Critical	The built in self test for the indicated processor failed.

Message	Alert Type	Description
Processor Or VRM Failed	Critical	Processor or VRM failed.
Processor VTT Power Fault.	Critical	Processor VTT Power Fault.
Redundant Power Failure	Critical	Redundant power is no longer available.
Redundant Power Supply Event	Critical	The redundant power supply posted an event.
Remote Login Successful	Information	Service processor user login from a remote location has completed successfully.
SBC memory error has occurred.	Critical	A single bit correctable type memory has occurred.
SERR on PCI bus "X"	Critical	System error on the indicated PCI bus.
SPI to I2C translator has had a fault.	Critical	The SPI translator is reporting an error.
Secondary Processor Bus Fault	Warning	The secondary PCI bus had an error.
Security: Intrusion Detect Enabled	Critical	The intrusion detection subsystem has been activated.
Security: System Intrusion Detected	Critical	There has been an intrusion into the system.
Single fan failure	Critical	A fan has failed.
System Boot Failed	Critical	The system’s initialization firmware failed.
System Complex Powered Down	Information	The system and it’s related equipment powered off.
System Complex Powered Up	Information	The system and it’s related equipment powered on.
System Error PCI Bus	Critical	A system error was detected on a PCI bus.
System Error PCI Bus "X"	Critical	A system error was detected on the indicated PCI bus.
System IO board I2C not responding.	Critical	Failure reading an I2C device, possible partitioned I2C bus.
System Intrusion Detected	Critical	There has been an intrusion into the system.
System Memory Error	Critical	Host memory had an error.
System Power Exceeded Recommended Redundant Value	Information	The system is not operating in power redundancy mode.
System Power Good Fault	Critical	The System Power Good indicator is at a fault condition.
System Powered Off	Information	The system was powered off.
System Status Display Fail	Critical	Communication to the operator panel failed
System ambient temperature is too high.	Critical	Room temperature is over recommended limit.
System board is over recommended temperature.	Warning	System board is over recommended temperature.
System board is under recommended temperature.	Warning	System board is under recommended temperature.
System could not find processor and VRMs in matching slot.	Critical	Voltage regulator module/processor pair mismatch.
System cutoff temperature exceed	Warning	System is over temperature.

Message	Alert Type	Description
System cutoff voltage exceed	Warning	A voltage supply limit has been exceeded.
System drive array I2C not responding.	Critical	Failure reading an I2C device, possible partitioned I2C bus.
System error log full	Critical	The error log’s message retention capacity has been exceeded.
System front panel controller not responding.	Critical	System front panel controller not responding.
System is over recommended voltage on VRM "X".	Warning	System is over recommended voltage on VRM "X".
System is under recommended voltage on VRM "X".	Warning	System is under recommended voltage on VRM "X".
System log 75% full	Warning	The system log’s retention capacity is 75% utilized.
System over recommended 5V Fault.	Warning	The 5v supply tolerance has been exceeded.
System over recommended 5V PCI.	Warning	The 5v for PCI is too high.
System over recommended ambient temperature.	Warning	Room temperature is over recommended limit.
System over recommended temperature	Warning	System over recommended temperature
System over recommended voltage for "X" V.	Warning	The "X" volt supply has exceeded it’s nominal operating range.
System over recommended voltage on "X" (I/O Planar).	Warning	The indicated voltage for the I/O planar has exceeded it’s nominal operating range.
System over recommended voltage on "X" V Regulator.	Warning	System over recommended voltage on the indicated voltage regulator.
System over recommended voltage on "X" V Supply.	Warning	System over recommended voltage on the indicated supply.
System over recommended voltage on "X" v (I/O Planar).	Warning	System over recommended voltage on the indicated voltage (I/O Planar).
System over recommended voltage on +5V Standby (I/O Planar).	Warning	System over recommended voltage on +5V Standby (I/O Planar).
System over recommended voltage on A/D Reference.	Warning	System over recommended voltage on A/D Reference.
System over recommended voltage on External SCSI Terminator Power (I/O Planar).	Warning	System over recommended voltage on External SCSI Terminator Power (I/O Planar).
System over recommended voltage on Internal SCSI Terminator Power (I/O Planar).	Warning	System over recommended voltage on Internal SCSI Terminator Power (I/O Planar).
System over recommended voltage on PB64 GTL (I/O Planar).	Warning	System over recommended voltage on PB64 GTL (I/O Planar).
System over recommended voltage on PB64"X".	Warning	System over recommended voltage on the indicated PB64.
System over recommended voltage on Primary Processor bus.	Warning	System over recommended voltage on Primary Processor bus.

Message	Alert Type	Description
System over recommended voltage on Processor IO bus.	Warning	System over recommended voltage on Processor IO bus.
System over recommended voltage on Secondary Processor bus.	Warning	System over recommended voltage on Secondary Processor bus.
System over recommended voltage on VRM +3.3 (I/O Planar).	Warning	System over recommended voltage on the indicated supply (I/O Planar).
System over recommended voltage on VRM "X".	Warning	System over recommended voltage on the indicated supply (I/O Planar).
System over temperature for CPU "X".	Warning	The indicated CPU reporting an over temperature condition.
System over/under recommended voltage	Warning	System over/under recommended voltage
System physical security compromised	Critical	System physical security compromised
System power controller not responding.	Critical	Communication with the power controller could not be established.
System power failure	Critical	System power failure
System shutoff due CPU "X" temperature under min value.	Critical	The indicated CPU has detected a temperature below the minimum acceptable value.
System shutoff due to +12V Supply over voltage.	Critical	System shutoff due to the indicated supply over voltage.
System shutoff due to +12V Supply under voltage.	Critical	System shutoff due to the indicated supply under voltage.
System shutoff due to "X"v "Y" (I/O Planar) over voltage.	Critical	The system has shutoff due to an over voltage condition for the indicated supply (I/O planar).
System shutoff due to "X"v "Y" (I/O Planar) under voltage.	Critical	The system has shutoff due to an under voltage condition for the indicated supply (I/O planar).
System shutoff due to +12v over voltage.	Warning	System shutoff due to an over voltage condition of the indicated supply.
System shutoff due to +12v under voltage.	Warning	System shutoff due to an under voltage condition of the indicated supply.
System shutoff due to "X" V Regulator over voltage.	Critical	System shutoff due to the indicated regulator over voltage.
System shutoff due to "X" V Regulator under voltage.	Critical	System shutoff due to the indicated regulator under voltage.
System shutoff due to "X" V Supply over voltage.	Critical	System shutoff due to the indicated supply over voltage.
System shutoff due to "X" V Supply under voltage.	Critical	System shutoff due to the indicated supply under voltage.
System shutoff due to "X" v (I/O Planar) over voltage.	Critical	System shutoff due to the indicated supply over voltage (I/O Planar).
System shutoff due to "X"v (I/O Planar) under voltage.	Critical	System shutoff due to the indicated supply under voltage (I/O Planar).

Message	Alert Type	Description
System shutoff due to "X"v over voltage.	Critical	System shutoff due to the indicated supply over voltage.
System shutoff due to "X"v under voltage.	Critical	System shutoff due to the indicated supply under voltage.
System shutoff due to +5V Standby (I/O Planar) over voltage.	Critical	System shutoff due to +5V Standby (I/O Planar) over voltage.
System shutoff due to +5V Standby (I/O Planar) under voltage.	Critical	System shutoff due to +5V Standby (I/O Planar) under voltage.
System shutoff due to +5V Supply over voltage.	Critical	System shutoff due to +5V Supply over voltage.
System shutoff due to +5V Supply under voltage.	Critical	System shutoff due to +5V Supply under voltage.
System shutoff due to "X" over voltage.	Warning	System shutoff due to the indicated voltage was beyond the recommended range.
System shutoff due to "X" under voltage.	Warning	System shutoff due to the indicated voltage was beyond the recommended range.
System shutoff due to "X" (I/O Planar) over voltage.	Critical	System shutoff due to an over voltage condition for the indicated voltage (I/O Planar).
System shutoff due to "X" (I/O Planar) under voltage.	Critical	System shutoff due to an under voltage condition for the indicated voltage (I/O Planar).
System shutoff due to "X" over voltage.	Warning	System shutoff due to an over voltage condition for the indicated voltage.
System shutoff due to "X" under voltage.	Warning	System shutoff due to an under voltage condition for the indicated voltage.
System shutoff due to 5V Fault Over max value.	Warning	System shutoff due to 5V Fault Over max value.
System shutoff due to 5V Fault under min value.	Warning	System shutoff due to 5V Fault under min value.
System shutoff due to 5V PCI over max value.	Warning	System shutoff due to 5V PCI over max value.
System shutoff due to 5V PCI under min value.	Warning	System shutoff due to 5V PCI under min value.
System shutoff due to A/D Reference over voltage.	Critical	System shutoff due to A/D Reference over voltage.
System shutoff due to A/D Reference under voltage.	Critical	System shutoff due to A/D Reference under voltage.
System shutoff due to Advanced System Management PCI Card’s Continuous 5V under minimum value.	Warning	System shutoff due to Advanced System Management PCI Card’s Continuous 5V under minimum value
System shutoff due to Advanced System Management PCI Card’s Continuous 5V over max allowed.	Warning	System shutoff due to Advanced System Management PCI Card’s Continuous 5V over max allowed.
System shutoff due to CPU "X" over temperature.	Critical	System shutoff due to the indicated CPU over temperature.
System shutoff due to CPU "X" under temperature.	Critical	System shutoff due to the indicated CPU under temperature.

Message	Alert Type	Description
System shutoff due to DASD temperature.	Critical	The direct access storage device area reported a temperature outside the recommended operating range.
System shutoff due to External SCSI Terminator Power (I/O Planar) over voltage.	Critical	System shutoff due to External SCSI Terminator Power (I/O Planar) over voltage.
System shutoff due to External SCSI Terminator Power (I/O Planar) under voltage.	Critical	System shutoff due to External SCSI Terminator Power (I/O Planar) under voltage.
System shutoff due to Internal SCSI Terminator Power (I/O Planar) over voltage.	Critical	System shutoff due to Internal SCSI Terminator Power (I/O Planar) over voltage.
System shutoff due to Internal SCSI Terminator Power (I/O Planar) under voltage.	Critical	System shutoff due to Internal SCSI Terminator Power (I/O Planar) under voltage.
System shutoff due to PB64 GTL (I/O Planar) over voltage.	Critical	System shutoff due to PB64 GTL (I/O Planar) over voltage.
System shutoff due to PB64 GTL (I/O Planar) under voltage.	Critical	System shutoff due to PB64 GTL (I/O Planar) under voltage.
System shutoff due to PB64"X" over voltage.	Critical	System shutoff due to the indicated PB64 over voltage.
System shutoff due to PB64"X" under voltage.	Critical	System shutoff due to the indicated PB64 under voltage.
System shutoff due to Primary Processor bus GTL+ over voltage.	Critical	System shutoff due to Primary Processor bus GTL+ over voltage.
System shutoff due to Primary Processor bus GTL+ under voltage.	Critical	System shutoff due to Primary Processor bus GTL+ under voltage.
System shutoff due to Processor IO bus over voltage.	Critical	System shutoff due to Processor IO bus over voltage.
System shutoff due to Processor IO bus under voltage.	Critical	System shutoff due to Processor IO bus under voltage.
System shutoff due to Secondary Processor bus GTL+ over voltage.	Critical	System shutoff due to Secondary Processor bus GTL+ over voltage.
System shutoff due to Secondary Processor bus GTL+ under voltage.	Critical	System shutoff due to Secondary Processor bus GTL+ under voltage.
System shutoff due to VRM "X" (I/O Planar) over voltage.	Critical	System shutoff due to the indicated VRM over voltage (I/O Planar).
System shutoff due to VRM "X" (I/O Planar) under voltage.	Critical	System shutoff due to the indicated VRM under voltage (I/O Planar).
System shutoff due to VRM "X" over voltage.	Warning	System shutoff due to the indicated VRM having an over voltage condition.
System shutoff due to VRM "X" under voltage.	Warning	System shutoff due to the indicated VRM having an under voltage condition.
System shutoff due to board over temperature.	Critical	System shutoff due to board over temperature.
System shutoff due to high ambient temperature.	Critical	System shutoff due to high ambient temperature.

Message	Alert Type	Description
System shutoff due to system board under temperature.	Critical	System shutoff due to system board under temperature.
System under recommended 5V Fault.	Warning	The 5 bus was under recommended tolerances.
System under recommended 5V PCI.	Warning	PCI +5 volts was under recommended tolerances.
System under recommended CPU "X" temperature.	Warning	System reported an under temperature condition for the indicated CPU.
System under recommended voltage for "X" v.	Warning	The indicated voltage supply is under nominal value.
System under recommended voltage on "X" (I/O Planar).	Warning	The indicated voltage supply is under nominal value (I/O planar).
System under recommended voltage on "X" V Regulator.	Warning	System under recommended voltage on the indicated regulator.
System under recommended voltage on "X" v.	Critical	The indicated voltage supply is under nominal value.
System under recommended voltage on A/D Reference.	Warning	System under recommended voltage on A/D Reference.
System under recommended voltage on External SCSI Terminator Power (I/O Planar).	Warning	System under recommended voltage on External SCSI Terminator Power (I/O Planar).
System under recommended voltage on Internal SCSI Terminator Power (I/O Planar).	Warning	System under recommended voltage on Internal SCSI Terminator Power (I/O Planar).
System under recommended voltage on PB64"X".	Warning	System under recommended voltage on the indicated PB64.
System under recommended voltage on Primary Processor bus.	Warning	System under recommended voltage on Primary Processor bus.
System under recommended voltage on Processor IO bus.	Warning	System under recommended voltage on Processor IO bus.
System under recommended voltage on Secondary Processor bus.	Warning	System under recommended voltage on Secondary Processor bus.
System under recommended voltage on VRM "X" (I/O Planar).	Warning	System under recommended voltage on the indicated VRM (I/O Planar).
System under recommended voltage on VRM "X"	Warning	System under recommended voltage on the indicated VRM.
Upgrade Power Supply Fan Fault	Critical	The upgrade power supply’s fan had a fault condition.
Upgrade Power Supply Fault	Critical	The upgrade power supply had a fault condition.
VFD BIST Complete	Critical	The operator display completed the built in self test.
VFD On/Off Switch Cable Not Installed	Information	The front panel cable supplying the operator display was not detected.
VRM "X" Fault	Critical	The indicated voltage regulator module was not within the recommended range.
VRM "X" Power Good Fault	Critical	The Power Good indicator for the indicated VRM signaled a fault condition.
Wall power failure to power supply "X".	Critical	Wall input power was beyond the recommended range.

Appendix B. Special Notices

This publication is intended to help customers, business partners and IBMers successfully implement a server management environment using IBM Netfinity Manager and the Advanced System Management processor and adapters on Netfinity servers. The information in this publication is not intended as the specification of any programming interfaces that are provided by Netfinity Manager and the Advanced System Management processor and adapters. See the PUBLICATIONS section of the applicable IBM Programming Announcement 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, North Castle Drive, Armonk, NY 10504-1785 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:

FFST
FFST/2
IBM
Micro Channel

NetBAY3
Netfinity
Netfinity Manager
OS/2
PowerPC 403
Predictive Failure Analysis
RETAIN
ServeRAID
ThinkPad

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries. (For a complete list of Intel trademarks see www.intel.com/dradmarx.htm)

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

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related Publications

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

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 279.

- *Implementing Netfinity Disk Subsystems: ServeRAID SCSI, Fibre Channel and SSA*, SG24-2098
- *Netfinity Performance Tuning with Windows NT 4.0*, SG24-5287
- *Integrating LAN Management Tools with Tivoli LAN Access*, SG24-2118
- *Universal Management Agent: Functions and Integration*, SG24-5294
- *NetFinity V5.0 Command Line and LMU Support*, SG24-4925
- *NetFinity V5.0 Database Support*, SG24-4808
- *Using LCCM Functions with Servers and Workstations*, SG24-5292

C.2 Redbooks on CD-ROMs

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at `http://www.redbooks.ibm.com/` for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr Format)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037

C.3 Other Publications

These publications are also relevant as further information sources:

- *Advanced System Management PCI Adapter Software User’s Guide*, 10L9285 available from `http://www.pc.ibm.com/support`
- *Advanced System Management PCI Adapter, Installation Instructions*, 10L9284 available from `http://www.pc.ibm.com/support`
- *Netfinity Advanced System Management Interconnect Cable Option*, 24L7782 available from http:/`/www.pc.ibm.com/support`
- *Netfinity Manager User’s Guide*, 10L9271 available from `http://www.pc.ibm.com/support` and with your server on ServerGuide

- *Netfinity Manager Command Reference*, 10L9270 available from `http://www.pc.ibm.com/support` and with your server on ServerGuide

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** `http://www.redbooks.ibm.com/`

  Search for, view, download, or order hardcopy/CD-ROM redbooks from the redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this redbooks site.

  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.

- **E-mail Orders**

  Send orders by e-mail including information from the redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at `http://w3.itso.ibm.com/` and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access `MyNews` at `http://w3.ibm.com/` for redbook, residency, and workshop announcements.

IBM Redbook Fax 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 Corporation
API	application programming interface
APPC	advanced program-to-program communication
ASCII	American National Standard Code for Information Interchange
ASM	Advanced System Management
ASMA	Advanced Systems Management Adapter
ATA	AT Attachment
BIOS	basic input/output system
BIST	boot initial system test
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
DASD	direct access storage device
DC	direct current
DIMM	dual inline memory module
DMI	Desktop Management Interface
DNS	domain name server
DOS	disk operating system
DTR	data terminal ready
ECC	error checking and correction
ECC-P	error checking and correction - parity
EDO	extended data output
EEPROM	electrically erasable programmable read only memory
EMEA	Europe/Middle East/Africa
EOS	ECC on SIMM
FVT	final verification test
GB	gigabyte
GUI	graphical user interface
HDD	hard disk drive
HEX	hexadecimal
HP	Hewlett Packard
HTML	Hypertext Markup Language
I/O	input/output
IBM	International Business Machines Corporation
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
MAC	medium access control
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
MSCS	Microsoft Cluster Server
MTU	maximum transmission unit
NC	normally closed
NFM	Netfinity Manager
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
PCI	peripheral component interconnect
PCMCIA	Personal Computer Memory Card International Association
PDF	portable document format
PFA	predictive failure analysis
POST	power-on self-test
PPP	point-to-point protocol
PS	PostScript
PSE	Professional Server Expert
RAID	redundant array of independent disks
RAM	random access memory
RETAIN	Remote Technical Assistance Information Network
RISC	reduced instruction set computer
ROM	read-only memory
RTS	ready to send
RWC	remote workstation control
SAF-TE	SCSI accessed fault-tolerant enclosures
SCF	service configuration file
SCO	Santa Cruz Operation Inc.
SCSI	small computer system interface
SCU	system configuration utility
SDRAM	static dynamic random access memory
SLT	slot
SMART	self-monitoring and reporting technology
SMI	system management interrupt
SMP	symmetric multiprocessing
SMS	System Management Server
SN	serial number
SNA	systems network architecture
SNMP	simple network management protocol
SP	service processor
SRAM	static random access memory
SSA	serial storage architecture
SSL	secure sockets layer
TAP	telocator alphanumeric protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TME	Tivoli Management Environment
UART	uniform asynchronous receiver/transmitter
UDP	user datagram protocol
UPS	uninterruptible power supply
URL	universal resource locator
UTP	unshielded twisted pair
VAC	volts alternating current
VDC	volts direct current
VIM	vendor independent messaging
VPD	vital product data
VRM	voltage regulator module
WAN	wide area network

Index

ITSO Redbook Evaluation

Netfinity Server Management
SG24-5208-01

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

Which of the following best describes you?
_ Customer _ Business Partner _ Solution Developer _ IBM employee
_ None of the above

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!)

____

____

____

____

____

SG24-5208-01

Printed in the U.S.A.

Netfinity Server Management

SG24-5208-01