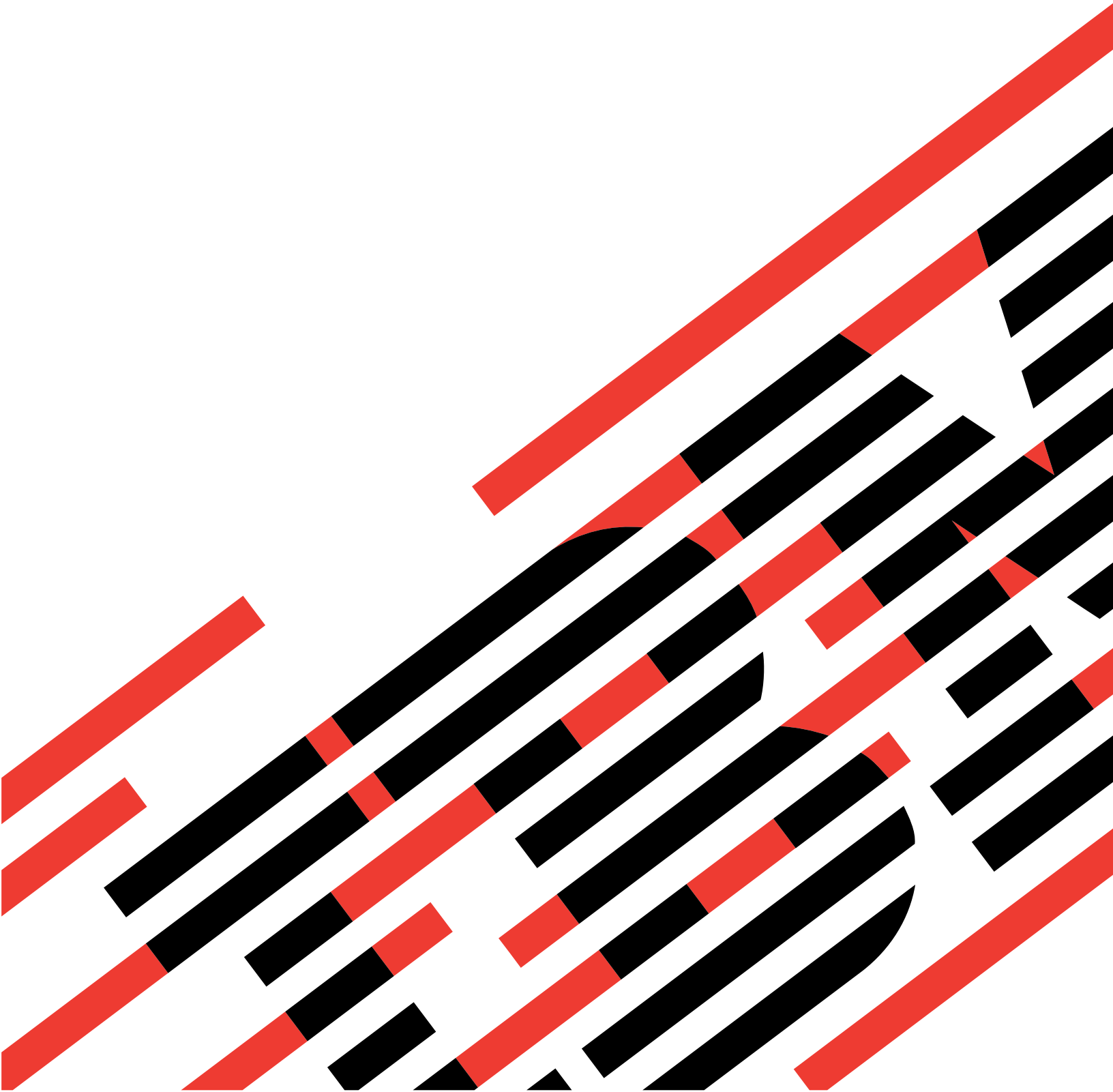
IBM

eserver

pSeries 655

User's Guide

SA38-0617-00



IBM

@server

pSeries 655

User's Guide

SA38-0617-00

First Edition (November 2002)

Before using this information and the product it supports, read the information in “Safety Notices” on page ix, Appendix A, “Environmental Notices”, on page 115, and Appendix B, “Notices”, on page 117.

A reader’s comment form is provided at the back of this publication. If the form has been removed, address comments to Information Development, Department H6DS-905-6C006, 11501 Burnet Road, Austin, Texas 78758-3493. To send comments electronically, use this commercial internet address: aix6kpub@austin.ibm.com. Any information that you supply may be used without incurring any obligation to you.

Contents

Safety Notices

A *danger* notice indicates the presence of a hazard that has the potential of causing death or serious personal injury. *Danger* notices appear on the following pages:

- ix

A *caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury. *Caution* notices appear on the following pages:

- ix
- x

For a translation of the safety notices contained in this book, see the *System Unit Safety Information*, order number SA23-2652.

Electrical Safety

Observe the following safety instructions any time you are connecting or disconnecting devices attached to the system.

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

Use one hand, when possible, to connect or disconnect signal cables to prevent a possible shock from touching two surfaces with different electrical potentials.

During an electrical storm, do not connect cables for display stations, printers, telephones, or station protectors for communications lines.
D06

CAUTION:
This product is equipped with a four-wire (three-phase and ground) power cable for the user's safety. Use this power cable with a properly grounded electrical outlet to avoid electrical shock.
C27

DANGER

To prevent electrical shock hazard, disconnect all power cables from the electrical outlet before relocating the system.
D01

Laser Safety Information

CAUTION:
This product may contain a CD-ROM, DVD-ROM, or laser module on a PCI card, which are class 1 laser products.
C30

Laser Compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with the IEC 825 (first edition 1984) as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
All IBM laser modules are designed so that there is never any human access to laser radiation above a class 1 level during normal operation, user maintenance, or prescribed service conditions. Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. Only trained service personnel should perform the inspection or repair of optical fiber cable assemblies and receptacles.
C25, C26

Data Integrity and Verification

IBM computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check the IBM support websites for updated information and fixes applicable to the system and related software.

About This Book

This book provides information on how to use the server, use diagnostics, use service aids, and verify server operation. This book also provides information to help you solve some of the simpler problems that might occur.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

Highlighting

The following highlighting conventions are used in this book:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
Italics	Identifies parameters whose actual names or values are to be supplied by the user.
`Monospace`	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

Accessing Information

Documentation for the IBM @server pSeries is available online. Visit the IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base.

- To access the pSeries publications, click **Hardware documentation**.
- To view information about the accessibility features of @server pSeries hardware and the AIX operating system, click **AIX and pSeries accessibility**.

References to AIX Operating System

This document may contain references to the AIX operating system. If you are using another operating system, consult the appropriate documentation for that operating system.

This document may describe hardware features and functions. While the hardware supports them, the realization of these features and functions depends upon support from the operating system. AIX provides this support. If you are using another operating system, consult the appropriate documentation for that operating system regarding support for those features and functions.

Related Publications

The following publications provide related information:

- The *System Unit Safety Information*, order number SA23-2652, contains translations of safety information used throughout this book.
- The *Site and Hardware Planning Information*, order number SA38-0508, contains information to help you plan your installation.
- The @server *pSeries 655 Service Guide*, order number SA38-0618, contains reference information, maintenance analysis procedures (MAPs), error codes, removal and replacement procedures, and a parts catalog.
- The @server *pSeries 655 Installation Guide*, order number SA38-0616, contains information on how to set up and cable the server, install additional processors and subsystems, and verify server operation.

- The *IBM Hardware Management Console for pSeries Installation and Operations Guide*, order number SA38-0590, provides information to system administrators on how to install and use a Hardware Management Console (HMC) to manage a system.
- The *IBM Hardware Management Console for pSeries Maintenance Guide*, order number SA38-0603, provides information on how to service a Hardware Management Console (HMC).
- The *RS/6000 and @server Diagnostic Information for Multiple Bus Systems*, order number SA38-0509, contains diagnostic information, service request numbers (SRNs), and failing function codes (FFCs).
- The *RS/6000 and @server Adapters, Devices and Cable Information for Multiple Bus Systems*, order number SA38-0516, contains information about adapters, devices, and cables for your server. This manual is intended to supplement the service information found in the *RS/6000 and @server Diagnostic Information for Multiple Bus Systems*.
- The *PCI Adapter Placement Reference*, order number SA38-0538, contains information regarding slot restrictions for adapters that can be used in this system.
- The *AIX System Management Guide: Operating System and Devices* describes various operating system procedures for managing this system.

  Documentation for the AIX operating system is available from the IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base. Select **AIX documentation**. The *AIX Documentation* CD contains the base set of publications for the operating system, including system-management and end-user documentation.

Trademarks

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

- AIX
- @server
- IBM
- pSeries
- RS/6000

Other company, product, and service names may be trademarks or service marks of others.

Chapter 1. Reference Materials

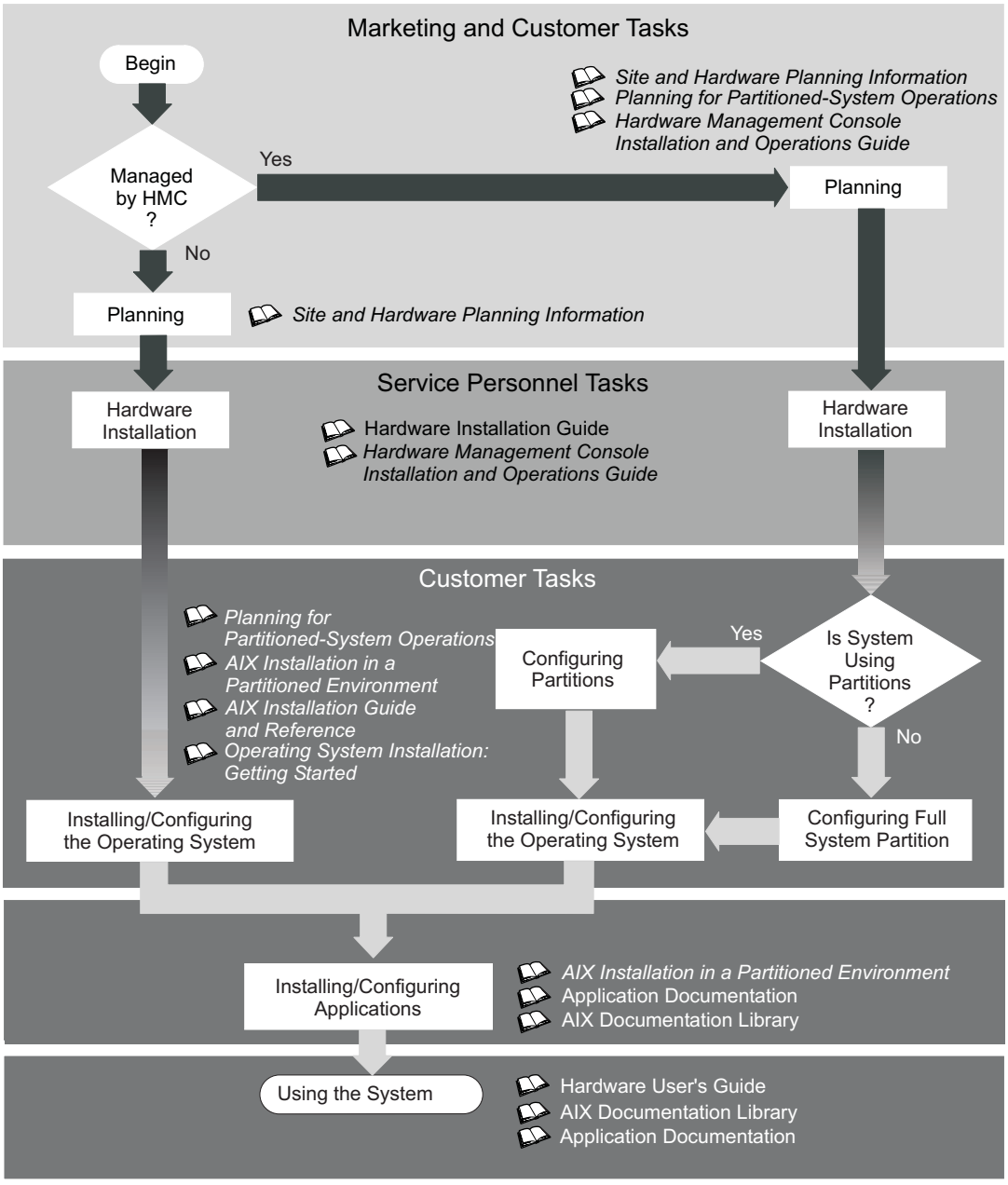
Note: This document may contain references to the AIX operating system. If you are using another operating system, consult the appropriate documentation for that operating system.

This document may describe hardware features and functions. While the hardware supports them, the realization of these features and functions depends upon support from the operating system. AIX provides this support. If you are using another operating system, consult the appropriate documentation for that operating system regarding support for those features and functions.

This chapter helps you get started with installing and configuring the @server pSeries environment. The following information is included in the chapter:

- @server pSeries Roadmap
- Documentation Overview - Brief description of the printed and softcopy documentation shipped including targeted audience

The following @server pSeries Roadmap helps you locate marketing, service, and customer task information. The roadmap guides you through the tasks and the publications that document those tasks.



The publications listed in this section are available online. To access the online books, visit our IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base.

Documentation Overview

This section provides descriptions and target audience information for the @server pSeries and AIX 5L documentation libraries. Some of the documentation may only be available in printed form or in softcopy form. Based on the documentation content, the books are divided into the following categories: **Planning**, **Installing and Configuring**, and **Using the System**.

Table 1. Planning

Documentation Title	Description	Audience	Type
Site and Hardware Planning Information	Contains information to help plan for site preparation tasks, such as floor-planning, electrical needs, air conditioning, and other site-planning considerations.	Marketing, system administrators	softcopy
Planning for Partitioned-System Operations	Describes planning considerations for partitioned systems, including information on dynamic partitioning and Capacity Upgrade on Demand.	System administrators	printed and softcopy
Hardware Management Console for pSeries Installation and Operations Guide	Provides information on how to install, configure, and use a Hardware Management Console (HMC). Logical partition (LPAR) tasks, such as configuring and managing partitions on multiple host servers, are included.	System administrators	printed and softcopy

Table 2. Installing and Configuring

Documentation Title	Description	Audience	Type
Hardware Installation Guide	Provides information on how to install system hardware, cable the system, and verify operations.	Service personnel	printed and softcopy
Planning for Partitioned-System Operations	Describes planning considerations for partitioned systems, including information on dynamic partitioning and Capacity Upgrade on Demand.	System administrators	printed and softcopy
Hardware Management Console for pSeries Installation and Operations Guide	Provides information on how to install, configure, and use a Hardware Management Console (HMC). Logical partition (LPAR) tasks, such as configuring and managing partitions on multiple host servers, are included.	System administrators	printed and softcopy
AIX Installation in a Partitioned Environment	Provides information on how to install the AIX operating system in an LPAR environment.	System administrators	printed and softcopy
AIX Operating System Installation: Getting Started	Provides information on how to install and configure the AIX operating system on a standalone system using a CD-ROM device.	System administrators	printed and softcopy
AIX 5L Installation Guide and Reference	Provides information on installing the AIX 5L operating system on standalone systems, as well as on client systems using the Network Installation Management (NIM) interface.	System administrators	printed and softcopy
PCI Adapter Placement Reference	Outlines system-specific PCI adapter slot placement and adapter support configurations.	Service personnel	printed
AIX 5L Release Notes	Provides late-breaking information for a specific AIX release.	System administrators	printed and softcopy
AIX 5L Documentation CD	AIX documentation library (system management guides, user guides, application programmer guides, commands and files references, AIX man pages, and so on).	System administrators	softcopy

Table 3. Using the System

Documentation Title	Description	Audience	Type
Hardware Management Console for pSeries Installation and Operations Guide	Provides information on how to install, configure, and use a Hardware Management Console (HMC). Logical partition (LPAR) tasks, such as configuring and managing partitions on multiple host servers, are included.	System administrators	printed and softcopy
Hardware User's Guide	Provides using, problem determination, and service processor information.	System administrators	printed and softcopy
Diagnostic Information for Multiple Bus Systems	Combines operating instructions for hardware diagnostic programs with common MAPs and SRNs (Service Request Numbers).	Service personnel	printed and softcopy
PCI Adapter Placement Reference	Outlines system-specific PCI adapter slot placement and adapter support configurations.	Service personnel	printed
Hardware Management Console for pSeries Maintenance Guide	Contains MAPs, removal and replacement, error code, and parts information to help diagnose and repair the system.	Service personnel	printed and softcopy
Adapters, Devices, and Cable Information for Multiple Bus Systems	Provides information about adapters, devices, and cables that are attached to or used within the system.	System administrators	printed and softcopy
System Unit Safety Information	Contains the English version of safety notices, as well as translations of those safety notices into other languages.	System administrators, service personnel	printed and softcopy
AIX 5L Documentation CD	AIX documentation library (system management guides, user guides, application programmer guides, commands and files references, AIX man pages, and so on).	System administrators	softcopy

Chapter 2. Introducing the pSeries 655

The pSeries 655 is a shared multiprocessor server.

The processor subsystem can be configured (or partitioned) as multiple separate systems. This configuration is known as a logically partitioned system. The processor subsystem is described in “Processor Subsystem” on page 6.

Other options for a rack configuration include the 7040 Model 61D I/O Subsystem and 7040 Model W42 Integrated Battery Feature (IBF) for the power subsystem.

The following components comprise configurations of the pSeries 655 system:

- **Bulk Power Assembly** (BPA). The BPA is the main power control unit for the pSeries 655 system. This redundant bulk power assembly distributes power at 350 V to each drawer where conversion is made to the required chip level. The BPA contains the following components:
  - Bulk Power Regulator (BPR)
  - Bulk Power Controller (BPC)
  - Bulk Power Distributor (BPD)
  - Bulk Power Jumper (BPJ) - optional
- **Processor Subsystem**. The processor subsystem is a 4 EIA-unit-high drawer. The processor subsystem contains:
  - One 4-way processor module at 1.3 GHz or one 8-way processor module at 1.1 GHz
  - Four L3 cache modules
  - Two externalized RIO ports
  - One pair of internal RIO ports servicing 3 PCI-X slots, two 10/100 Ethernet adapters, a dual SCSI adapter, and a service processor card
  - Fan assembly
  - Two 3.5-inch SCSI DASD bays
  - Four memory cards

  The processor subsystem contains the Distributed Converter Assembly (DCA) used in the conversion of 350 V bulk power to the supply voltages required by the various internal components.

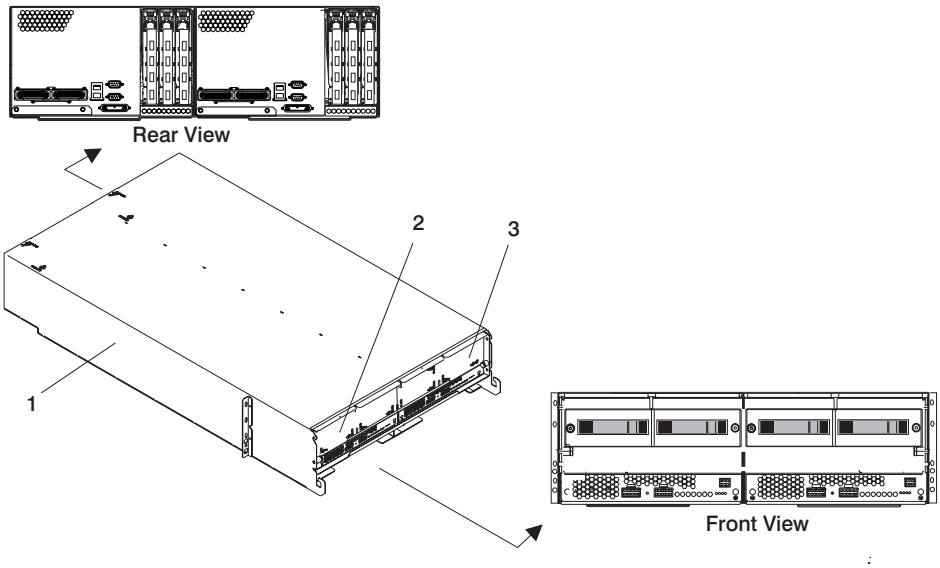
  The minimum memory required to operate this system is 4 GB, and the maximum amount of memory is 32 GB.
- **Integrated Battery Feature** (IBF). The IBF is a 2 EIA-unit-high drawer that can be added to your system. The IBF is optional and provides backup electric power in case of a power outage. You can install up to six IBFs in the rack configuration. The total number of IBFs that can be installed depends upon the number of processor subsystems and I/O subsystems installed in the rack.
- **I/O Subsystem**. Each I/O subsystem is a 4 EIA-unit-high subsystem containing up to 2 I/O boards, up to 16 disk drives, 4 DASD backplanes, a midplane card, 4 cooling fans and 2 power supplies (which are independent of the bulk power assembly). A rack can have up to 5 I/O subsystems with each drawer having 20 PCI card slots, and more than 500 GB of storage.

  Note: If your system configuration contains IBFs, the rack drawer space may be limited for I/O subsystems.
- **Hardware Management Console** (HMC). The HMC consists of a display, independent processor, keyboard, and mouse. One HMC is standard for all systems. An additional HMC is optional. Two HMCs can attach to one processor subsystem, or two HMCs can jointly manage up to 16 processor subsystems in up to 4 racks with the use of 8-port asynchronous adapters and 128-port asynchronous adapters.

For more information on the use of logical partitioned systems, see the “Partitioned System Overview”.

Processor Subsystem

The pSeries 655 Model 651 (processor subsystem) is a processor node installed in a frame-mounted cage. The equipment rack holds a maximum of 16 processor subsystems.



1 Frame Cage (shown with two processor subsystems and front cover removed)
2 First pSeries 655 Processor Subsystem
3 Second pSeries 655 Processor Subsystem

The Hardware Management Console for pSeries (HMC) is used to manage the resources in the system. The system can be configured as a full system partition, which means that all resources of the system are used as a single system.

The system can also be configured into multiple (or logical) partitioned systems. With a logically partitioned system, system resources can be divided into a number of systems each running in its own partition.

Numerous configurations of pSeries 655 systems can be managed from one Hardware Management Console. A second Hardware Management Console can be used for redundancy.

Partitioned System Overview

Partitioning enables users to configure a single computer into several independent systems. Each of these systems, called *logical partitions*, is capable of running applications in its own independent environment. This independent environment contains its own operating system, its own set of system processors, its own set of system memory, and its own I/O adapters.

The HMC allows you to perform many hardware management tasks for your managed system, including configuring logical partitions. You can choose to operate your managed system as a single server (called *full system partitions*), or you can choose to run multiple partitions.

Partition Profiles

A profile defines a configuration setup for a managed system or partition. The HMC allows you to create multiple profiles for each managed system or partition. You can then use the profiles you created to start a managed system or partition in a particular configuration.

A partition does not actually own any resources until it is activated; resource specifications are stored within partition profiles. The same partition can operate using different resources at different times, depending on the profile you activate.

When you activate a partition, you enable the system to create a partition using the set of resources in a profile created for that partition. For example, a logical partition profile might indicate to the managed system that its partition requires 3 processors, 2 gigabytes of memory, and I/O slots 6, 11, and 12 when activated.

You can have more than one profile for a partition. However, you can only activate a partition with one profile at a time.

When you create a partition profile, the HMC shows you all the resources available on your system. The HMC does not, however, verify if another partition profile is currently using a portion of these resources. For example, the HMC might show eight processors on your system, but does not notify you that other partitions are using six of them. You can create two partition profiles, each using a majority of system resources. If you attempt to activate both of these partitions at the same time, the second partition in the activation list fails.

System Profiles

Using the HMC, you can create and activate often-used collections of predefined partition profiles. A collection of predefined partition profiles is called a *system profile*. The system profile is an ordered list of partitions and the profile that is to be activated for each partition. The first profile in the list is activated first, followed by the second profile in the list, followed by the third, and so on.

The system profile helps you change the managed systems from one complete set of partition configurations to another. For example, a customer may want to switch from using 8 partitions to using only four, every day. To do this, the system administrator deactivates the 8 partitions and activates a different system profile, one specifying four partitions.

When you create a group of affinity partitions, the HMC automatically creates a system profile that includes all of the affinity partitions that you created.

Types of Partitions

The HMC allows you to use two types of partitions: logical partitions and the full system partition.

Logical Partitions

Logical partitions are user-defined system resource divisions. Users determine the number of processors, memory, and I/O that a logical partition can have when active.

Full System Partition

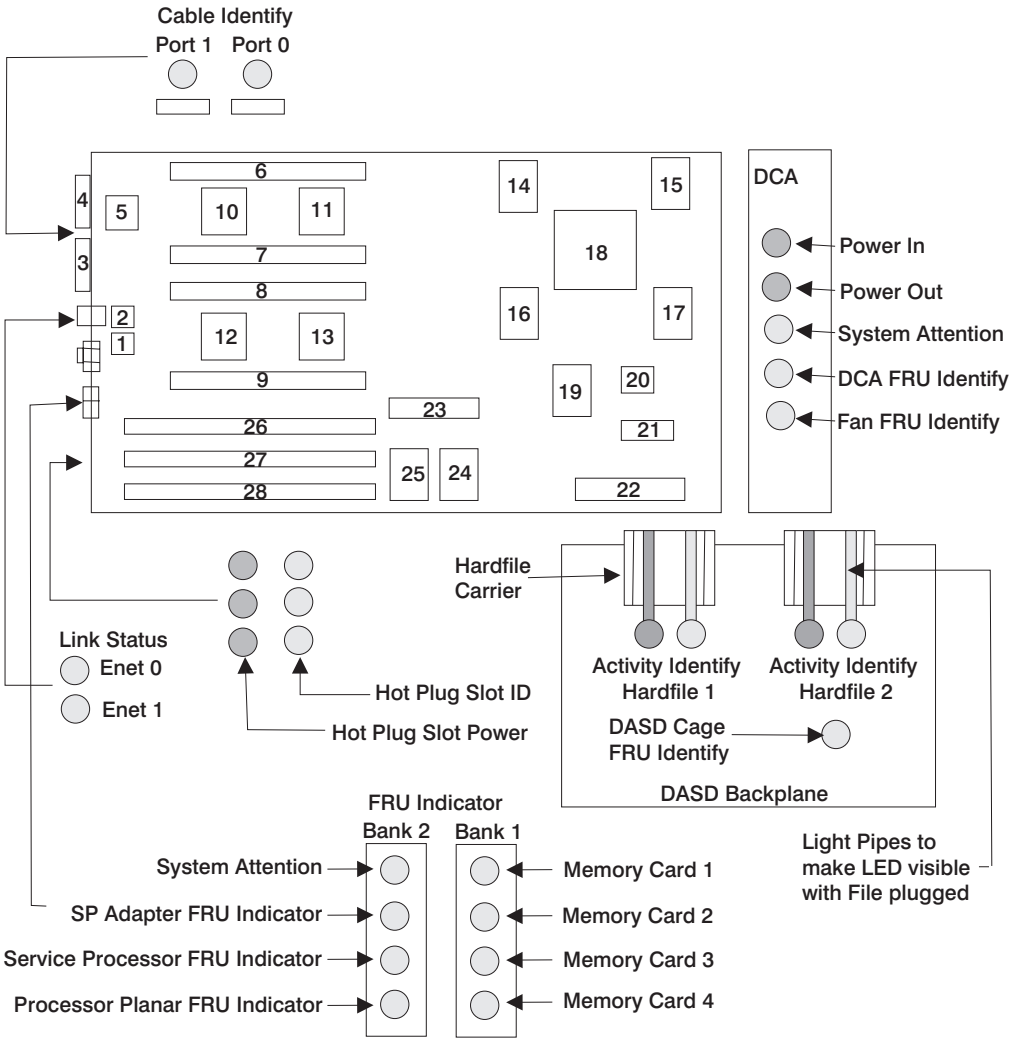
A special partition called the full system partition assigns all of your managed system's resources to one large partition. The full system partition is similar to the traditional, non-partitioned method of operating a system. Because all resources are assigned to this partition, no other partitions can be started when the full system partition is running. Likewise, the full system partition cannot be started while other partitions are running.

The HMC allows you to easily switch from the full system partition to logical partitions. The actual setup of the operating system in a partition may require some careful planning to ensure no conflicts exist between the two environments.

For more detail on partitions, see the *IBM Hardware Management Console for pSeries Installation and Operations Guide*.

System Attention LEDs

On the processor subsystem, there are two system attention LEDs, one on the DCA and the other on the back of the system. For the specific locations of these LEDs, refer to the following illustration.



1 Ethernet Port 1
2 Ethernet Port 0
3 RIO Port 0 (A0)
4 RIO Port 1 (A1)
5 RIO Adapter
6 Memory Card Slot 1
7 Memory Card Slot 2
8 Memory Card Slot 3
9 Memory Card Slot 4
10 Memory Controller 0
11 Memory Controller 1
12 Memory Controller 3
13 Memory Controller 2
14 L3 Cache Module 0
15 L3 Cache Module 1
16 L3 Cache Module 3
17 L3 Cache Module 2
18 MCM Module (processor)
19 RIO/PCI-X Bridge
20 SCSI Controller
21 DASD Ribbon Cable Connector
22 Service Processor/VPD Card Connector
23 SP Adapter Connector
24 PCI-X Bridge (PH2)
25 PCI-X Bridge (PH0)
26 PCI Adapter Slot 1
27 PCI Adapter Slot 2
28 PCI Adapter Slot 3

The two LEDs are tied together, so they will always be in the same state, either both on or both off. They are referred to as the system attention LED. The system attention LED is turned on when an entry is made in the service processor error log that gets transmitted to the system-level error logs (the AIX error log and the service action event log in service focal point). When the attention light comes on, these error logs should be examined to see if user intervention is required.

If a hardware problem is indicated, call service support.

Disturbance or System Attention LED

The system attention LED lights on solid when an event occurs that either needs customer intervention or IBM service. The system attention LED is turned on when an entry is made in the service processor error log. The error entry is transmitted to the following:

- System-level error logs
- AIX error log
- As an entry in the service action event log in the Service Focal Point application. For example, the loss of surveillance from the HMC to a logical partition.

HMC Attached System Error Interrogation

On systems attached to an HMC, when the system attention LED turns on, you should refer to the Service Action Event Log in the Service Focal Point application on the HMC and check the open service events using the procedure described in Working with Serviceable Events in the *IBM Hardware Management Console for pSeries Installation and Operations Guide*.

Note: For information on Service Focal Point settings, refer to Setting Up Surveillance and Enabling Surveillance Notifications in the *IBM Hardware Management Console for pSeries Installation and Operations Guide*.

Events requiring customer intervention are marked as Call Home Candidate? NO. For all of these events, examine the description in the serviceable event error details. If actions are listed in the description, perform those actions. If the error indicates a loss of surveillance between the HMC and a partition, check the status of the partition, the network, and the cabling between the HMC and the partition. If the surveillance error persists, call service support.

Whether a user intervention error or an IBM serviceable error is detected, the system attention light can be reset by following the procedures in “Resetting the System Attention LED”. The preferred method to reset the attention indicator is by following the HMC Attached Systems procedures. Either the HMC Attached Systems procedures or the alternate procedures will reset the attention indicator.

Resetting the System Attention LED

The system attention LED can be turned off by using either of the HMC-Attached Systems or alternate methods.

Resetting the System Attention LED on HMC-Attached Systems

To reset the system attention LED on HMC-attached systems, do the following:

1. On the HMC interface, click **Service Applications**.
2. Double-click **Service Focal Point**.
3. In the Contents area of the screen, select **Hardware Service Functions**. The LED Management window opens.
4. In the LED Management window, select one or more managed systems from the table.
5. Select **Deactivate LED**. The associated system attention LED is turned off.

For more information about the virtual operator panel on the HMC, see the *IBM Hardware Management Console for pSeries Installation and Operations Guide*.

Alternate Method of Resetting the System Attention LED Using the AIX Command Line

As a user with root authority, enter `diag` on the AIX command line, and do the following:

1. Select **Task Selection**.
2. On the Task Selection Menu, select **Identify and Attention Indicators**.
3. When the list of LEDs displays, use the cursor to highlight **Set System Attention Indicator to Normal**.
4. Press Enter, and then press F7 to commit. This action turns off the LED

Alternate Method of Resetting the System Attention LED Using the Service Processor

If the system is powered off, access the service processor menus. From the service processor main menu, do the following:

1. Select the **System Information Menu**.
2. Select **LED Control Menu**.
3. Select **Clear System Attention Indicator**. This action turns off the LED.

Chapter 3. Using the Hardware Management Console for pSeries

This chapter discusses the Hardware Management Console for pSeries (HMC), system power control, and the power-on self-test that occurs after powering on the system.

Hardware Management Console (HMC) Overview and Setup

The HMC uses its connection to the processor subsystem to perform various functions. The main functions of the HMC include:

- Creating and maintaining a multiple-partition environment
- Detecting, reporting, and storing changes in hardware conditions
- Acting as a service focal point for service representatives to determine an appropriate service strategy

Note: The HMC is shipped with the @server pSeries 655 and is the main interface for configuring and managing resources on this system through the HMC virtual terminal window. *Virtual terminal window* refers to the operating system session on a particular window. You can have up to 16 virtual terminal windows.

All the tasks you need to maintain the interface, the underlying operating system, and the HMC application code are available by using the HMC's management applications.

For more information on the HMC, refer to the *IBM Hardware Management Console for pSeries Installation and Operations Guide*.

System Power-On Methods

The HMC is used to power on the managed system. The managed system will reboot in the same mode in which it was previously booted. (If the managed system was previously booted in partitioned system mode, all partitions will automatically start and run.)

Powering On the Processor Subsystem Using the HMC

To power on the processor subsystem using the HMC, do the following:

1. Log in to the HMC with your user ID and password. Refer to the *IBM Hardware Management Console for pSeries Installation and Operations Guide* for more information on HMC user IDs and passwords.
2. To select your preferred partition environment, click on the **Partition Management** icon under the HMC hostname. The Contents area now lists the processor subsystem as available as a managed system. If you have only one processor subsystem, the Contents area lists the processor subsystem as **System A**.
3. Select the appropriate managed system.
4. To power on the managed system, select the desired system in the Contents area. Next, on the menu, choose **Selected**.
5. Select **Power On**.

Powering Off the Processor Subsystem Using the HMC

Attention: Shut down the partitions before powering off the processor subsystem.

To power off the processor subsystem using the HMC, do the following:

1. To select your preferred partition environment, click on the **Partition Management** icon under the HMC hostname. The Contents area now lists the processor subsystem as available as a managed system. If you have only one processor subsystem, the Contents area lists the processor subsystem as **System A**.
2. Select the appropriate managed system.
3. To power off the managed system, select the desired system in the Contents area. Next, on the menu, choose **Selected**.
4. Select **Power Off**.
5. A screen displays to verify that you want to power off. Select **Yes**.

Note: Only logic power will be removed; 350 V dc power will still be present within the system.

Graphics Console Support

The pSeries 655 Model 651 Processor Subsystem supports graphics consoles. Graphics console support requires the following adapters:

- Graphics adapter with a graphics display attached
- Universal Serial Bus (USB) adapter with a keyboard and mouse attached

Only one graphics console is supported per system partition. If the system is running partitions, up to eight partitions can have graphics consoles.

The graphics console is functional only when AIX is running. For any installation or service processor functions, you must use the HMC.

Understanding the Power-On Self-Test (POST)

After power is turned on and before the operating system is loaded, the partition does a power-on self-test (POST). This test performs checks to ensure that the hardware is functioning correctly before the operating system is loaded. During the POST, a POST screen displays, and POST indicators appear on the virtual terminal window. The next section describes the POST indicators and functions that can be accessed during the POST.

POST Indicators

POST indicators indicate tests that are being performed as the partition is preparing to load the operating system. The POST indicators are words that display on the virtual terminal window. Each time that the firmware starts another different step in the POST, a POST indicator word appears on the console. Each word is an indicator of the tests that are being performed.

The POST screen displays the following words:

Memory
: Memory test

Keyboard
: Initialize the keyboard and mouse. The time period for pressing a key to access the System Management Services, or to initiate a service mode boot, is now open. See “POST Keys” on page 13 for more information.

Network
: Self-test on network adapters

SCSI
: Adapters are being initialized

Speaker

A speaker is not implemented on this system

POST Keys

The POST keys, if pressed *after* the **keyboard** POST indicator displays and *before* the last (speaker) POST indicator displays, cause the system to start services or to initiate service mode boots used for configuring the system and diagnosing problems. The keys are described below:

Note: The program function keys (F1-F12) on a keyboard attached to the HMC or USB card are not used and will be ignored. After the **keyboard** POST indicator displays, you must use the numeric number keys to enter input.

1 Key

The numeric 1 key, when pressed during POST, starts the System Management Services (SMS) interface.

5 Key

The numeric 5 key, when pressed during POST, initiates a system boot in service mode using the default service mode boot list.

6 Key

The numeric 6 key works like the numeric 5 key, except that the firmware uses the customized service mode bootlist.

8 Key

This option is used by service personnel. To enter the open firmware command line, press the numeric 8 key *after* the word **keyboard** displays and *before* the last word **speaker** displays during startup. After you press the 8 key, the remaining POST indicators display until initialization completes.

When initialization and POST are complete, the open firmware command line (an `0K` prompt) displays.

Note: This option should only be used by service personnel to obtain additional debug information.

To exit from the open firmware command prompt, type `reset-all` or power off the system and reboot.

Chapter 4. Using the Service Processor

Note: The information in this chapter regarding the configuring of serial ports does not apply to the serial ports, or modems attached to those serial ports, on the Hardware Management Console (HMC).

The service processor runs on its own power boundary and continually monitors hardware attributes and the environmental conditions within the system. The service processor is controlled by firmware and does not require the operating system to be operational to perform its tasks.

The service processor menus allow you to configure service processor options, as well as enable and disable functions.

Service processor menus are available using an HMC virtual terminal window when `0K` is displayed on the virtual operator panel or when the service processor has detected a server problem (such as a surveillance failure).

Service Processor Menus

The service processor menus are divided into the following groups:

- General user menu - the user must know the general-access password.
- Privileged user menus - the user must know the privileged-access password.

If the server is powered off, the service processor menus can be accessed on the HMC.

Accessing the Service Processor Menus

Service processor menus are accessed by opening a virtual terminal window on the HMC. After `0K` displays in the virtual operator panel on the HMC, press any key on the keyboard to signal the service processor.

When you gain access, the service processor prompts you for a password (if one is set), and when verified, displays the service processor menus.

The service processor menu prompt, represented by `0>` on the HMC, indicates the serial port to which the terminal is connected.

Saving and Restoring Service Processor Settings

All the settings that you make (except language) from the service processor menus can be backed up either for recovering from a fault that may corrupt these settings, or for replicating these settings to other servers that include a service processor.

The service aid, Save or Restore Hardware Management Policies, can be used to save your settings after initial setup or whenever the settings must be changed for system operation purposes.

It is strongly recommended that you use this service aid for backing up service processor settings to protect the usefulness of the service processor and the availability of the server. Refer to ″Save or Restore Hardware Management Policies,″ in the ″Introduction to Tasks and Service Aids″ section of the *RS/6000 and @server Diagnostic Information for Multiple Bus Systems*.

It is strongly recommended that you use this service aid for backing up service processor settings to protect the usefulness of the service processor and the availability of the server. Refer to “Save or Restore Hardware Management Policies,” in “Introduction to Tasks and Service Aids” for information about this service aid.

Menu Inactivity

The service processor exits menu mode after ten minutes of inactivity and displays a message indicating that it has done so. Pressing any key on the virtual terminal window causes the main menu to display.

General User Menu

The menu options presented to the general user are a subset of the options available to the privileged user. The user must know the general-access password, if one is set, to access this menu.

```
       GENERAL USER MENU

 1. Power-on System

 2. Power-off System

 3. Read VPD Image from Last System Boot

 4. Read Progress Indicators from Last System Boot

 5. Read Service Processor Error Logs

 6. Read System POST Errors

99. Exit from Menus

 0>
```

- **Power-on System**

  Allows the user to start the system using the current virtual operator panel on the HMC.
- **Power-off System**

  This option is not available on this system.
- **Read VPD Image from Last System Boot**

  Displays manufacturer vital product data, such as serial numbers and part numbers, that were stored from the system boot prior to the one in progress now, for the entire system.
- **Read Progress Indicators from Last System Boot**

  Displays a number of the boot progress indicators, which may include service processor checkpoints, IPL checkpoints, or AIX configuration codes, from the previous system boot. This information can be useful in diagnosing system faults.

  Note: If you are running one or more logical partitions, enter the partition ID (0-15) to display progress indicators for that partition since the last system boot. If your system is running in Full System Partition mode, this option automatically displays details from partition zero.

  The progress indicator codes are listed from top (latest) to bottom (oldest).

  This information is not stored in nonvolatile storage. If the system is powered off using the HMC, this information is retained. If the ac power is disconnected from the system, this information will be lost. For an example, refer to “LCD Progress Indicator Log” on page 42.
- **Read Service Processor Error Logs**

  Displays the service processor error logs. For an example, refer to “Service Processor Error Logs” on page 40.
- **Read System POST Errors**

  Displays additional error log information (this option is only for service personnel).
- **Exit from Menus**

  Selecting this option will exit the service processor menus. You can re-enter the menus by pressing any key on the console.

Privileged User Menus

The following menus are available to privileged users only. The user must know the privileged-access password, if one is set, to access these menus.

Main Menu

A listing at the top of the main menu contains the following:

- Your system's current firmware version
- The firmware copyright notice
- The system name given to your server during setup

You need the firmware version for reference when you either update or repair the functions of your service processor.

The system name, an optional field, is the name that your server reports in problem messages. This name helps your support team (for example, your system administrator, network administrator, or service representative) to more quickly identify the location, configuration, and history of your server. Set the system name, from the main menu, using option 6.

Note: The information under the Service Processor Firmware heading in the following Main Menu illustration is example information only.

```
        Service Processor Firmware
        VERSION: RH011007
        Copyright 2001 IBM Corporation
             SYSTEM NAME


        MAIN MENU

  1. Service Processor Setup Menu

  2. System Power Control Menu

  3. System Information Menu

  4. Language Selection Menu

  5. Call-In/Call-Out Setup Menu
         Not Supported

  6. Set System Name

 99. Exit from Menus

 0>
```

- **Service Processor Setup Menu**
  See "Service Processor Setup Menu" on page 18 for more information.
- **System Power Control Menu**
  See "System Power Control Menu" on page 22 for more information.
- **System Information Menu**
  See "System Information Menu" on page 25 for more information.
- **Language Selection Menu**
  See "Language Selection Menu" on page 32 for more information.
- **Call-In/Call-Out Setup Menu**
  This function is not available on this system.
- **Set System Name**

Allows setting of the system name.

- **Reset all L3 Cache Module Records**

  Clears L3 Gard records after a repair action.

  Note: This is a hidden menu option for use only by a service representative.
  Allows setting of the system name.

Service Processor Setup Menu

The following Service Processor Setup Menu is accessed from the Main Menu:

```
       SERVICE PROCESSOR SETUP MENU

 1. Change Privileged Access Password

 2. Change General Access Password

 3. Enable/Disable Console Mirroring:
        Not Supported

 4. Start Talk Mode
        Not Supported

 5. OS Surveillance Setup Menu

 6. Reset Service Processor

 7. Reprogram Flash EPROM Menu
        Not Supported

 8. Serial Port Snoop Setup Menu
      Not Supported

 9. Scan Log Dump Setup Menu:
 Currently As Needed

98. Return to Previous Menu

99. Exit from Menus

0>
```

Note: Unless otherwise stated in menu responses, settings become effective when a menu is exited using option 98 or 99.

Passwords

Passwords can be any combination of up to eight alphanumeric characters. You can enter longer passwords, but the entries are truncated to include only the first eight characters. The privileged access password can be set from service processor menus or from System Management Services (SMS) utilities (see Chapter 5, “Using System Management Services”, on page 47). The general access password can be set only from service processor menus.

For security purposes, the service processor counts the number of attempts to enter passwords. The results of not recognizing a password within this error threshold are different, depending on whether the attempts are being made locally (at the server) or remotely (through a modem). The error threshold is three attempts.

If the error threshold is reached by someone entering passwords at the server, the service processor commands the server to resume the initial program load (IPL). This action is taken based on the assumption that the server is in an adequately secure location with only authorized users having access. Such users must still successfully enter a login password to access the operating system.

If the error threshold is reached by someone entering passwords remotely, the service processor commands the server to power off to prevent potential security attacks on the server by unauthorized remote users. The following table lists what you can access with the privileged-access password and the general-access password.

Privileged Access Password	General Access Password	Resulting Menu
None	None	Service processor MAIN MENU displays.
Set	None	Users with the password see the service processor MAIN MENU. Users without password cannot log in.
Set	Set	Users see menus associated with the entered password.

- **Change Privileged-Access Password**

  Set or change the privileged-access password. It provides the user with the capability to access all service processor functions. This password is usually used by the system administrator or root user.
- **Change General-Access Password**

  Set or change the general-access password. It provides limited access to service processor menus, and is usually available to all users who are allowed to power on the server, especially remotely.

  Note: The general-access password can only be set or changed after the privileged access password is set.
- **Enable/Disable Console Mirroring**

  This function is not available on this system.
- **Start Talk Mode**

  This function is not available on this system.
- **OS Surveillance Setup Menu**

  Note: This option is disabled in partitioned systems.

  This menu can be used to set up operating system (OS) surveillance.

```
       OS Surveillance Setup Menu

 1. Surveillance:
      Currently Enabled

 2. Surveillance Time Interval:
      2 minutes

 3. Surveillance Delay:
      2 minutes


98. Return to Previous Menu

0>
```

– **Surveillance**

  Can be set to Enabled or Disabled.

– **Surveillance Time Interval**

  Can be set to any number from 2 through 255.

– **Surveillance Delay**

  Can be set to any number from 0 through 255.

Refer to “Service Processor System Monitoring - Surveillance” on page 39 for more information about surveillance.

- **Reset Service Processor**

  If this option is selected, entering `Y` causes the service processor to reboot.
- **Reprogram Flash EPROM Menu**

  This function is not available on this system.
- **Serial Port Snoop Setup Menu**

  This function is not available on this system.
- **Scan Log Dump Policy**

  A scan dump is the collection of chip data that the service processor gathers after a system malfunction, such as a checkstop or hang. The scan dump data may contain chip scan rings, chip trace arrays, and SCOM contents.

  The scan dump data are stored in the system control store. The size of the scan dump area is approximately 4 MB.

  During the scan log dump, A8xx (in the range A810 to A8FF) displays in the operator panel value on the HMC. The xx characters will change as the scan log dump progresses. If the xx characters do not change after five minutes, the service processor is hung and must be reset.

  When the scan log dump is complete, depending on how the reboot policy is set, the system will either:

  – Go to the standby state (and the service processor menus will be available), indicated by OK or STBY in the virtual operator panel on the HMC.

  OR

  – Attempt to reboot.

```
Scan Log Dump Setup Menu

      1.  Scan Log Dump Policy:
            Currently As Needed

      2.  Scan Log Dump Content:
            Currently As Requested

      3.  Immediate Dump

     98.  Return to Previous Menu
```

```
    Select from the following options:
    (As Needed=2, Always=3)

    Enter New Option:

0>
```

The scan log dump policy can be set to the following:

2 = As Needed
The processor run-time diagnostics record the dump data based on the error type. This is the default value.

3 = Always
Selecting this option allows the service processor to record a scan log dump for all error types.

The scan log dump policy can also be set from the Tasks menu in the AIX service aids.

Option 2 displays the following screens:

```
               Scan Log Dump Setup Menu

      1.  Scan Log Dump Policy:
            Currently As Needed

      2.  Scan Log Dump Content:
            Currently As Requested

      3.  Immediate Dump

     98.  Return to Previous Menu
```

```
    Select from the following options:
    (As Requested=1, Optimum=2, Complete=3, Minimum=4)

    Enter New Option:
0>
```

The scan log dump content can be set to the following:

1 = As Requested
The processor run-time diagnostics will select the contents of the dump file based on the type of error that occurs. This is the default.

2 = Optimum
The dump will include the smallest amount of information to diagnose a hardware error.

3 = Complete
The dump will include as much information as possible to allow the complete analysis of hardware and software errors.

4 = Minimum

The dump will include the smallest amount of information possible (a minimum number of hardware scan log rings).

The complete dump will take the longest time to finish; it may take as long as 1.5 hours on a fully configured system.

The scan log dump content can also be set from the Tasks menu in the AIX diagnostic service aids.

If a valid dump file already exists, the dump control code will stop because the contents of the prior dump must be protected.

Option 3, **Immediate Dump**, can only be used when the system is in the standby state with power on. It is used to dump the system data after a checkstop or machine check occurs when the system firmware is running, or when the operating system is booting or running.

System Power Control Menu

This menu is used to set power control options. Other menus that control boot options are available from this menu.

```
       SYSTEM POWER CONTROL MENU

 1. Enable/Disable Unattended Start Mode:
       Currently Enabled

 2. Ring Indicate Power-On Menu

 3. Reboot/Restart Policy Setup Menu

 4. Power-On System

 5. Power-Off System

 6. Enable/Disable Fast System Boot
       Currently Fast Boot

 7. Boot Mode Menu

98. Return to Previous Menu

99. Exit from Menus

0>
```

- **Enable/Disable Unattended Start Mode**

  Use this option to instruct the service processor to restore the power state of the server after a temporary power failure. Unattended start mode can also be set through the SMS menus. This option is intended to be used on servers that require automatic power-on after a power failure.
- **Ring Indicate Power-On Menu**

  This function is not available on this system.
- **Reboot/Restart Policy Setup Menu**

  The following menu controls the Reboot/Restart Policy:

```
       Reboot/Restart Policy Setup Menu

 1. Number of reboot attempts:
      Currently 1

 2. Use OS-Defined restart policy?
      Currently No

 3. Enable supplemental restart policy?
      Currently Yes

 4. Call-Out before restart:
      Currently Disabled

98. Return to Previous Menu

0>
```

Reboot is the process of bringing up the system hardware; for example, from a system reset or power on. *Restart* is activating the operating system after the system hardware is reinitialized. Restart must follow a successful reboot.

- **Number of reboot attempts** - If the server fails to successfully complete the boot process, it attempts to reboot the number of times specified. Entry values equal to or greater than 0 are valid. Only successive failed reboot/restart attempts are counted.
- **Use OS-Defined restart policy** - In a full system partition, this allows the service processor to react in the same way that the operating system does to major system faults by reading the setting of the operating system parameter **Automatically Restart/Reboot After a System Crash**. This parameter might already be defined, depending on the operating system or its version or level. If the operating system automatic restart setting is defined, it can be set to respond to a major fault by restarting or by not restarting. See your operating system documentation for details on setting up operating system automatic restarts. The default value is No.

  On a partitioned system, this setting is ignored.
- **Enable supplemental restart policy** - The default setting is Yes. When set to Yes in a full system partition, the service processor restarts the system when the system loses control as detected by service processor surveillance, and either:

  The **Use OS-Defined restart policy** is set to No.

  OR

  The **Use OS-Defined restart policy** is set to Yes, and the operating system has no automatic restart policy.

  If set to Yes in a partitioned system, the service processor restarts the system when the system loses control and it is detected by service processor surveillance.
- **Call-Out before restart (Enabled/Disabled)** - If a restart is necessary due to a system fault, and you are running a full system partition, you can enable the service processor to call out and report the event. This option can be valuable if the number of these events becomes excessive, which might signal a bigger problem.

  This setting is ignored on a partitioned system.

- **Power-On System**

  Allows immediate power-on of the system.
- **Power-Off System**

  This option is not available on this system.
- **Enable/Disable Fast System Boot**

  Allows the user to select the IPL type, mode, and speed of the system boot.

  Attention: Selecting the fast IPL results in several diagnostic tests being skipped and a shorter memory test being run.

- **Boot Mode Menu**

  The Boot Mode Menu allows you to select a boot mode.

```
       Boot Mode Menu

 1. Boot to SMS Menu:
      Currently Disabled

 2. Service Mode Boot from Saved List:
      Currently Disabled

 3. Service Mode Boot from Default List:
      Currently Disabled

 4. Boot to Open Firmware Prompt:
      Currently Disabled

98. Return to Previous Menu

 0>
```

  To select a boot mode, select a number and press Enter. The item corresponding to the selected number toggles between Disabled to Enabled. If a boot mode is Enabled, the boot mode selected is performed, and the Disabled/Enabled selection is reset to Disabled. The following describes each boot mode:

  – **Boot to SMS Menu**

    When this selection is enabled, the system boots to the SMS Menu.

  – **Service Mode Boot from Saved List**

    This selection causes the system to perform a service mode boot using the service mode boot list saved in NVRAM. If the system boots AIX from the disk drive and AIX diagnostics are loaded on the disk drive, AIX boots to the diagnostics menu.

    Using this option to boot the system is the preferred way to run online diagnostics.

  – **Service Mode Boot from Default List**

    This selection is similar to *Service Mode Boot from Saved List*, except the system boots using the default boot list that is stored in the system firmware. This is normally used to try to boot customer diagnostics from the CD-ROM drive or NIM server.

    Using this option to boot the system is the preferred way to run standalone diagnostics from CD-ROM.

  – **Boot to Open Firmware**

    This option should only be used by service personnel to obtain additional debug information. When this selection is enabled, the system boots to the open firmware prompt.

System Information Menu

This menu provides access to system configuration information, error logs, system resources, and processor configuration.

```
        SYSTEM INFORMATION MENU

  1. Read VPD Image from Last System Boot

  2. Read Progress Indicators from Last System Boot

  3. Read Service Processor Error Logs

  4. Read System POST Errors

  5. Read NVRAM

  6. Read Service Processor Configuration

  7. Processor Configuration/Deconfiguration Menu

  8. Memory Configuration/Deconfiguration Menu

  9. Power Control Network Utilities Menu

 10. LED Control Menu

 11. MCM/L3 Interposer Plug Count Menu

 12. Performance Mode Setup Menu

 13. L3 Mode Menu

 98. Return to Previous Menu

 99. Exit from Menus

 0>
```

- **Read VPD Image from Last System Boot**

  Displays manufacturer's vital product data (VPD), such as serial numbers, part numbers, and so on, that was stored from the system boot prior to the one in progress now. VPD from all devices in the system is displayed.
- **Read Progress Indicators from Last System Boot**

  Displays a number of the boot progress indicators, which may include Service Processor checkpoints, IPL checkpoints, or AIX configuration codes, from the previous system boot. This information can be useful in diagnosing system faults.

  The progress indicator codes are listed from top (latest) to bottom (oldest).

  This information is not stored in nonvolatile storage. If the system is powered off using the HMC, this information is retained. If the ac power is disconnected from the system, this information will be lost. For an example, refer to "LCD Progress Indicator Log" on page 42.
- **Read Service Processor Error Logs**

  Displays error conditions detected by the service processor. Refer to "Service Processor Error Logs" on page 40 for an example of this error log.
- **Read System POST Errors**

  This option should only be used by service personnel to obtain additional debug information.
- **Read NVRAM**

  Displays Non Volatile Random Access Memory (NVRAM) content.
- **Read Service Processor Configuration**

  Displays current service processor configuration.
- **Processor Configuration/Deconfiguration Menu**

Enable/Disable CPU Repeat Gard

CPU repeat gard will automatically deconfigure a CPU during a system boot if a processor has failed BIST (power-on self-test), caused a machine check or check stop, or has reached a threshold of recoverable errors. The processor will remain deconfigured until repeat gard is disabled or the processor is replaced.

The default is enabled.

For more information, see “Configuring and Deconfiguring Processors or Memory” on page 39.

Enable/Disable Processor Hot Sparing

This function is not available on this system.

This menu allows the user to change the system processor configuration. If it is necessary to take one of the processors offline, use this menu to deconfigure a processor, and then reconfigure the processor at a later time. An example of this menu follows:

```
        PROCESSOR CONFIGURATION/DECONFIGURATION MENU

77. Enable/Disable CPU Repeat Gard: Currently Enabled
78. Enable/Disable Processor Hot Sparing (if available): Currently Enabled

 1.  0   3.0  (00)  Configured by system     2.  1   3.1  (00)  Deconfigured by system
 3.  2   3.2  (00)  Configured by system     4.  3   3.3  (00)  Configured by system



98. Return to Previous Menu

0>
```

Note: This table is built from vital product data collected during the last boot sequence. The first time the system is powered on, or after the system’s nonvolatile RAM (NVRAM) has been erased, this table may be empty. The table is rebuilt during the next boot into AIX.

The fields of the previous table represent the following:

Column 1

(1.) Menu selection index.

Column 2

(0) Logical processor device number assigned by AIX. You can display these logical device numbers by issuing the following command on the AIX command line:

```
lsdev -C | grep proc
```

Column 3

(3.0) Processor address list used by the service processor.

Column 4

(00) Error status of the processors.

The error status of each processor is indicated by AB, where B indicates the number of errors and A indicates the type of error according to the following:

1. Bring-up failure
2. Run-time non-recoverable failure
3. Run-time recoverable failure
4. Group integrity failure
5. Non-repeat-gardable error. The resource may be reconfigured on the next boot.

A status of 00 indicates that the CPU has not had any errors logged against it by the service processor.

To enable or disable CPU repeat gard, use menu option 77. CPU repeat gard is enabled by default.

If CPU repeat gard is disabled, processors that are in the ″deconfigured by system″ state will be reconfigured. These reconfigured processors are then tested during the boot process, and if they pass, they remain online. If they fail the boot testing, they are deconfigured even though CPU repeat gard is disabled.

The failure history of each CPU is retained. If a processor with a history of failures is brought back online by disabling repeat gard, it remains online if it passes testing during the boot process. However, if repeat gard is enabled, the processor is taken offline again because of its history of failures.

Note: The processor numbering scheme used by the service processor is different from the numbering scheme used by AIX. Consult the AIX documentation before configuring or deconfiguring a processor to ensure that the correct processor is selected.

Note: The number of processors available to AIX can be determined by issuing the following command on the AIX command line: `bindprocessor -q`

- **Memory Configuration/Deconfiguration Menu**

  Enable/Disable Memory Repeat

  Memory repeat gard will automatically deconfigure a memory riser card during a system boot if a memory card has failed BIST (power-on self-test), caused a machine check or checkstop, or has reached a threshold of recoverable errors. The memory will remain deconfigured until repeat gard is disabled or the memory card is replaced.

  For more information, see “Configuring and Deconfiguring Processors or Memory” on page 39.

  Runtime Recoverable Error Repeat Gard

  The runtime recoverable error repeat gard flag controls the deallocation of the memory if a recoverable error occurs during runtime. If a recoverable memory error occurs, and runtime recoverable error repeat gard is disabled, the system will continue running with no change in the memory configuration. If a recoverable memory error occurs, and runtime recoverable error repeat gard is enabled, the memory card on which the error occurred will be garded out (taken offline).

  The default is disabled.

These menus allow the user to change the system memory configuration. If it is necessary to take one of the memory cards offline, this menu allows you to deconfigure a memory card, and then reconfigure the card at a later time.

When this option is selected, a menu displays. The following is an example of this menu:

```
        MEMORY CONFIGURATION/DECONFIGURATION MENU

77. Enable/Disable Memory Repeat Gard: Currently Enabled

78. Runtime Recoverable Error Repeat Gard: Currently Disabled

 1. Memory card

98. Return to Previous Menu
```

After you select the memory card option by entering 1, a menu displays, allowing the selection of a memory card. The following is an example of this menu.

```
       MEMORY CONFIGURATION/DECONFIGURATION MENU


 1. 16.16(00, -)  Configured by system   2. 16.17(00, -) Configured by system
 3. 16.18(00, -)  Configured by system   4. 16.19(00, 1) Partially deconfigured by system




98. Return to Previous Menu
```

Note: This table is built from vital product data collected during the last boot sequence. The first time the system is powered on, or after the system's nonvolatile RAM (NVRAM) has been erased, this table may be empty. The table is rebuilt during the next boot into AIX.

The fields in the previous table represent the following:

Column 1

1. Menu selection index/card number

Column 2

xx.xx : Card address used by service processor

Column 3

(00.-) Error/deconfiguration status

The error status of the each memory card is indicated by AB, where B indicates the number of errors and A indicates the type of error according to the following table:

1. Bring-up failure
2. Run-time non-recoverable failure
3. Run-time recoverable failure
4. Group integrity failure
5. Non-repeat-gardable error. The resource may be reconfigured on the next boot.

An error status of (00, -) (for example, 11.16(00, -)) indicates that the memory card has not had any errors logged against it by the service processor, and it is fully configured.

The field after the error status will be a ″-″, ″0″, or ″1″. The dash indicates that the memory card is fully configured. A zero or a one indicates that memory repeat gard has deconfigured half of the memory card. If this occurs, the status of the card in the menu is shown as ″Partially deconfigured by system.″

To change the memory configuration, select the number of the memory card. The memory card state will change from `configured` to `deconfigured` or from `deconfigured` to `configured`.

This menu only allows the deconfiguration of an entire card; it does not allow the manual deconfiguration of half a card. If half a card has been configured by the system (″Partially deconfigured″), it can be manually reconfigured using this menu.

In the previous example menu, each line shows two cards and indicates whether they are configured.

To enable or disable Memory Repeat Gard, use menu option 77 of the Memory Configuration/Deconfiguration menu.

To enable or disable runtime recoverable error repeat gard, use option 78 of the Memory Configuration/Deconfiguration menu.

The failure history of each card is retained. If a card with a history of failures is brought back online by disabling Repeat Gard, it remains online if it passes testing during the boot process. However, if Repeat Gard is enabled, the card is taken offline again because of its history of failures.

- **Power Control Network Utilities Menu**

```
        POWER CONTROL NETWORK UTILITIES MENU

  1. Lamp Test for all Operator Panels

  2. Display I/O Type

  3. Change I/O Type

 98. Return to Previous Menu

 0>
```

  - **Lamp Test for All Operator Panels**

    This option is not available on this system.

  - **Display I/O Type**

    This option is not available on this system.

  - **Change I/O Type**

    Use this option to change the I/O type of the service processor after a service action or configuration change if the I/O type is incorrect. If this option is chosen, you will be asked to make the following entries:

    1. For the I/O drawer address, type `1`.
    2. For the I/O type, type `A5`.

    If either value is not valid, a failure message displays on the console. Press Enter to return to the Power Control Network Utilities Menu.

- **LED Control Menu**

  This menu displays the state of the I/O subsystem disturbance/system attention LED. Use this menu to toggle the attention/fault LEDs between identify (blinking) and off. Option 1 is only available when the system is in the error state (the processor subsystem is powered on and the service processor menus are available). Option 1 is not available when the system is in standby. An example of this menu follows:

```
       LED Control Menu


   1. Set/Reset Identify LED state

   2. Clear System Attention Indicator


98. Return to Previous Menu

 0 >
```

  If option 1 is selected, a list of location codes of the I/O subsystems is shown. The screen will be similar to the following:

```
      LED Control Manu

    1. U1.9-P1
    2. U1.9-P2
    3. U1.5-P1
    4. U1.5-P2



Enter number corresponding to the location code, or
press Return to continue, or 'x" to return to the menu.

0>4
```

If one of the devices is selected using the index number, the present state of its LED will be displayed, and you will be given the option to toggle it as shown in these example screens. The final state of the LED will then be displayed whether it was changed or not.

```
     U1.5–P2 is currently in the OFF state

     Select from the following (1=IDENTIFY ON, 2=IDENTIFY OFF)

0>2
```

```
     Please wait ...

     U1.5-P2 is currently in the OFF state
     (Press Return to continue)
```

Option 2 is not available on this system.

- **Interposer Plug Count Menu**

  Attention: Do not power on the system when in this menu. Fully exit from this menu before powering on the system.

  This menu tracks the number of times that the MCM and L3 cache modules have been plugged into the system backplane.

  If the MCM or L3 cache module is reseated or replugged, the plug count for that module must be incremented by 1. If the plug count exceeds the limit of 10 (reaches 11 or greater), a 450x yyyy or 4B2x yyyy error with a detail value of CFF0 that calls out an MCM or L3 cache module will be posted in the service processor error log. The FRU should be replaced during a deferred service call.

  If the MCM or L3 cache module is replaced, or installed during an MES upgrade, the plug count must be set using the interposer plug count menu. If the plug count information is not included with the new or replacement module, enter the default value of 8 (7 for the manufacturing process and 1 for the installation of the module that was just done). If the plug count is not entered, a B1xx 4699 error code, with a detailed value of E10B or E10C, will be posted in the service processor error log.

  If the service processor card is replaced, the plug counts are retained. However, the plug count menu must be accessed and option 50, **Commit the values and write to the VPD**, must be executed, so that the plug counts are revalidated. If the counts are not revalidated, a B1xx 4699 error code, with a detail value of E10B or E10C, will be posted in the service processor error log.

  A screen similar to the following will be displayed.

```
          MCM/L3 Interposer Plug Count Menu

     1. L3_0:7                          2. L3_1:9


                    3. MCM_0:8

     4. L3_3:7                          5. L3_2:7

50. Commit the values and write to the VPD

98. Return to the Previous Menu
```

The MCM modules and L3 cache modules are shown in the same way that they are plugged into the processor subsystem planar; the layout shown in the menu represents the physical location as seen from the front of the subsystem.

The format of the menu entries shown above is the menu index number, followed by L3_xx, followed by the plug count after the colon. The following tables correlates the information shown above with the physical location codes.

Menu Index Number	Physical Location Code
1. L3_0	U1.x-P1-C1
2. L3_1	U1.x-P1-C3
3. MCM_0	U1.x-P1-C2
4. L3_3	U1.x-P1-C4
5. L3_2	U1.x-P1-C5

Enter a menu index number to change the plug count for a particular module. For example, to change the plug count of the L3 cache module that is physically in the upper-left corner (U1.9-P1-C1), type `1`, then enter the new plug count.

When all of the new plug counts have been entered, select 50, **Commit the values and write to the VPD**. This action will store the new values in NVRAM.

Performance Mode Setup Menu

If certain types of processor cards are installed in the system, this menu will remain ″not applicable.″ For other types of processor cards, this menu will be active after the first boot as noted below.

Note: The first time the system is booted after NVRAM is cleared, `Not Applicable` displays under Performance Mode Setup Menu on the screen. This may also occur if the service processor is replaced, or the processor MCM module is upgraded.

If option 12 is selected when `Not Applicable` is on the screen, the system responds with `Not Applicable` and redisplays the system information menu. The setup menu can be displayed after the performance mode is set, which happens the first time that the system is booted.

The default performance mode is set by the firmware during IPL. The default mode provides the best performance for the hardware configuration of the system. The performance mode is system wide; it cannot be set on a per-partition basis. The default setting can be overwritten using the performance mode setup menu. The performance mode setup menu will be similar to the following:

```
       Default Performance Mode:   Standard Operation

 1. Current Performance Mode:

       Standard Operation


98. Return to Previous Menu

 0>
```

Selecting option 1 displays the three possible performance mode:

```
 Select from the following options:


 1. Large Commercial System optimization

 2. Standard Operation

 3. Turbo Database Mode


 0>
```

If you want to override the default setting, a brief description of each performance mode follows:

- Large Commercial System Optimization is the setting for systems that do not fall under the other two selections, **Standard Operation** and **Turbo Database Mode**.
- Standard Operation optimizes the system for high-memory bandwidth applications where minimal sharing of data occurs, and the likelihood of significant hardware data prefetching exists. This is the default performance mode on this system.
- Turbo Database Mode optimizes system operation for environments where there is a large amount of data-sharing among processes running concurrently on the system.

L3 Mode Menu

This menu is not supported on this system.

Language Selection Menu

The service processor menus and messages are available in various languages. This menu allows selecting languages in which the service processor and system firmware menus and messages are displayed.

```
       LANGUAGE SELECTION MENU

 1. English

 2. Francais

 3. Deutsch

 4. Italiano

 5. Espanol

98. Return to Previous Menu

99. Exit from Menus

 0>
```

Note: Your virtual terminal window must support the ISO-8859 character set to correctly display languages other than English.

Call-In/Call-Out Setup Menu

This menu is not supported on this system.

Service Processor Parameters in Service Mode (Full System Partition)

When the system is in service mode, the following service processor parameters are suspended:

- Unattended Start Mode
- Reboot/Restart Policy
- Surveillance

When service mode is exited, the service processor parameters revert to the customer settings.

Service Processor Reboot/Restart Recovery

Reboot describes bringing the system hardware back up; for example, from a system reset or power-on. The boot process ends when control passes to the operating system process.

Restart describes activating the operating system after the system hardware is reinitialized. Restart must follow a successful reboot.

Boot (IPL) Speed

When the server enters reboot recovery, slow IPL is automatically started, which gives the POST an opportunity to locate and report any problems that might otherwise be unreported.

Failure During Boot Process

During the boot process, either initially after system power-on or upon reboot after a system failure, the service processor monitors the boot progress. If progress stops, the service processor can reinitiate the boot process (reboot) if enabled to do so. The service processor can re-attempt this process according to the number of retries selected in the Reboot/Restart Policy Setup Menu.

Failure During Normal System Operation

When the boot process completes and control transfers to the operating system (OS), the service processor can monitor operating system activity (see the Set Surveillance Parameters option in the SERVICE PROCESSOR SETUP MENU). If OS activity stops due to a hardware- or software-induced failure, the service processor can initiate a reboot/restart process based on the settings in the Service Processor Reboot/Restart Policy Setup Menu and the OS automatic restart settings (see the operating system documentation).

If you are using the AIX operating system, the menu item under SMIT for setting the restart policy is **Automatically Reboot After Crash**. The default is false. When the setting is true, and if the service processor parameter ″Use OS-Defined Restart Policy″ is yes (the default), the service processor takes over for AIX to reboot/restart after a hardware or surveillance failure.

Service Processor Reboot/Restart Policy Controls

The operating system's automatic restart policy (see operating system documentation) indicates the operating system response to a system crash. The service processor can be instructed to refer to that policy by the Use OS-Defined Restart Policy setup menu.

If the operating system has no automatic restart policy, or if it is disabled, then the service processor-restart policy can be controlled from the service processor menus. Use the Enable Supplemental Restart Policy selection.

Use OS-Defined restart policy - The default setting is no. If set to yes on a full system partition, this causes the service processor to refer to the OS Automatic Restart Policy setting and take action (the same action the operating system would take if it could have responded to the problem causing the restart).

When this setting is no, or if the operating system did not set a policy, the service processor refers to enable supplemental restart policy for its action.

This setting is ignored on a partitioned system.

Enable supplemental restart policy - The default setting is Yes. When set to yes on a full system partition, the service processor restarts the server when the operating system loses control and either:

- The **Use OS-Defined restart policy** is set to No.

OR

- The **Use OS-Defined restart policy** is set to Yes and the operating system has no automatic restart policy.

  If set to Yes on a partitioned system, the service processor restarts the system when the system loses control and it is detected by service processor surveillance.

The following table describes the relationship among the operating system and service processor restart controls in a full system partition.

OS Automatic reboot/restart after crash setting	Service processor to use OS-Defined restart policy?	Service Processor Enable supplemental restart policy?	System response
None	No[1]	No	
None	No[1]	Yes[1]	Restarts
None	Yes	No	
None	Yes	Yes[1]	Restarts
False[2]	No[1]	No	
False[2]	No[1]	Yes[1]	Restarts
False[2]	Yes	No	
False[2]	Yes	Yes[1]	
True	No[1]	No	
True	No[1]	Yes[1]	Restarts
True	Yes	No	Restarts
True	Yes	Yes[1]	Restarts

[1] Service processor default
[2] AIX default

In a partitioned system, the service processor's supplemental restart policy is the only setting that is used, as shown in the following table:

Service Processor enable supplemental restart policy	System Response
No	
Yes (default)	Restarts

Processor Subsystem Firmware Updates

This section provides information and instructions for updating the system firmware. This procedure will normally be performed by a service representative.

To check the availability of firmware and microcode updates, go to http://techsupport.services.ibm.com/server/mdownload2.

If you cannot download from the Web, do the following:

- If the system is running, but access to the Web is not available, see "Processor Subsystem Firmware Update Using a Locally Available Image".

To check the level of firmware that is currently on the system, see "Determining the Level of Firmware on the Processor Subsystem".

General Information on Processor Subsystem Firmware Updates

Firmware on the processor subsystem includes:

1. System firmware. System firmware includes:
   a. System power control network programming
   b. Service processor programming
   c. IPL programming
   d. Run-time abstraction services
2. Frame (Power Subsystem) firmware
3. Integrated SCSI controller microcode
4. Integrated Ethernet microcode

To obtain the firmware and microcode updates, and complete procedures for performing the updates, go to http://techsupport.services.ibm.com/server/mdownload2.

Determining the Level of Firmware on the Processor Subsystem

Note: This information may be superseded by the information that is available on the Web site listed below. Always check the Web site for the latest images and instructions for checking the firmware level. The Web address is http://techsupport.services.ibm.com/server/mdownload2.

The firmware level is denoted by XXYYMMDD, where XX = model designation, YY = year, MM = month, and DD = day of the release.

The firmware level can be determined by either of the following methods:

- On the AIX command line, by typing:

  ```
  lscfg -vp|grep -p Platform
  ```

  A line that begins with `ROM level (alterable)..` displays the firmware level that is currently on the system.
- Looking at the top of the Service Processor Main Menu.

Processor Subsystem Firmware Update Using a Locally Available Image

To update the system firmware using a locally available image, perform the following steps:

1. Log in as root user.

2. If the **/tmp/fwupdate** directory does not exist, create it by issuing the following command:

   ```
   mkdir /tmp/fwupdate
   ```

3. The firmware update file must be downloaded or copied into the **/tmp/fwupdate** directory on the system. This can be done by using the **ftp** command to get the image from an ftp server or a NIM server, or NFS-mounting the directory on the host system. If a control workstation (CWS) is attached to the system, the **ftp** command can be used to transfer the update file to the target system from the control workstation.

   The firmware updated file can also be transferred to the target system by backing up the image onto diskettes from another server and restoring it into the **/tmp/fwupdate** directory.

   After the firmware update file has been downloaded or copied into the **/tmp/fwupdate** directory, verify its existence by entering the following command:

   ```
   ls /tmp/fwupdate/RJ*.img
   ```

   The update file will have the format RJyymmdd.img. The RJ indicates that this is an update image for your system: yy is the year, mm is the month, and dd is the day of the update file.

4. After the update file has been written to the **/tmp/fwupdate** directory, enter the following commands:

   ```
   cd /usr/lpp/diagnostics/bin

   ./update_flash -f /tmp/fwupdate/RJyymmdd.img
   ```

   Attention: Do not overlook the periods (.) in the commands shown above. AIX commands are case-sensitive. Type them exactly as shown.

You will be asked for confirmation to proceed with the firmware update and the required reboot. If you confirm, the system will apply the new firmware, reboot, and return to the AIX prompt. This may take up to ten minutes depending on the configuration of the system.

Attention: On some systems, the message `Wait for rebooting before stopping` may display on the system console. Do not turn off the system until the system has fully rebooted to the AIX login prompt. If a shutdown is necessary at that time, log in as root user and issue the **shutdown** command.

While the update is in progress, you will see `Rebooting...` on the display for several minutes.

The firmware update is complete.

Updating System Firmware from the AIX Service Aids

Attention: This method is not recommended for partitioned systems, but if the device resources are allocated properly, the firmware update can be done using the AIX service aid.

Note: This service aid is supported only in online diagnostics.

If the firmware on a partitioned system is being updated:

- One partition running AIX must have service authority.
- All other partitions except the one with service authority must be shut down.
- The partition with service authority must own the device from which the firmware update image will be read.
- The partition with service authority must have a hard disk.

If the required devices are not in the partition with service authority, the customer or system administrator must reassign the appropriate resources to it. This requires rebooting the partition with service authority.

If the firmware on a full system partition is being updated, no special steps are required to perform the firmware update using the service aid.

Note: Because the system always reboots itself during this type of firmware update process, the update process can take from 20 to 60 minutes.

Updating System Firmware from the AIX Command Line

This task is normally performed by a service representative. Refer to the detailed instructions that are provided on CORE with the latest image.

Note: The update process can take up to 60 minutes, and the system reboots itself during the update process.

Frame (Power Subsystem) Firmware Update

The frame code (which includes the power subsystem) is updated using a task on the HMC. This task is normally performed by a service representative. A code update (also called *corrective service*) may be available at `http://techsupport.services.ibm.com/server/mdownload2`

This task downloads a corrective service for the frame onto the HMC.

Note: Because the HMC is a closed system, you cannot install additional applications on your HMC. All of the tasks you need to maintain the managed system, the underlying operating system, and the HMC application code are available by using the HMC's management applications.

To download corrective service on the HMC, do the following:

1. From the HMC interface, in the Navigation area (left side of the panel), open the Software Maintenance folder.
2. In the Contents area (right side of the panel), double-click the **Frame** icon. The Frame application opens in the Contents area.
3. In the Contents area, click **Receive Corrective Service** task.
4. Select one of the following by clicking on the circle to the left.
   - **Upload corrective service from diskette.** If you select this option, make sure the proper diskette is in the HMC diskette drive.
   - **Download the corrective service file from a remote system.** If you select this option, complete the Remote Site (hostname), Patch file (filename or remote system), User ID (for remote system), and password (for remote system).
5. Click **OK** to copy the corrective service to this HMC.

Integrated SCSI Controller Microcode Update

The SCSI controller is located on the system planar and may require microcode updates. The SCSI controller microcode is updated using a task in AIX. A code update may be available at `http://techsupport.services.ibm.com/server/mdownload2`

The updated microcode and procedures for performing the update are available at the Web site.

Integrated Ethernet Microcode Update

The Ethernet microcode may require microcode updates. The Ethernet microcode is updated using a task in AIX. A code update may be available at `http://techsupport.services.ibm.com/server/mdownload2`

The updated microcode code and procedures for performing the update are available at the Web site.

Installing Corrective Service on the Frame

This task allows you to update the level of code on the frame after you have downloaded a corrective service. This procedure should be run after any of the following components are replaced:

- Bulk Power Regulator (BPR)
- Bulk Power Controller (BPC)
- Distributed Converter Assembly (DCA)

Notes:

1. To install a corrective service on a frame, you must be a member of either the system administrator role or the service representative role. Refer to the *IBM Hardware Management Console for pSeries Installation and Operations Guide* for information on these roles.
2. *Do not* power off any of the components in the frame at any time during this installation procedure. Interruptions can leave the power subsystem, or one of the other components in the frame, in an unrecoverable state.

To install a corrective service, do the following:

1. If you have not installed the corrective fix from ftp or diskette onto this HMC, perform steps to receive frame corrective service on the HMC (as described in “Frame (Power Subsystem) Firmware Update” on page 37). Then go to Step 4.
2. From the HMC interface, in the Navigation area (left side of the panel), open the Software Maintenance folder.
3. In the Contents area (right side of the panel), double-click the **Frame** icon. The Frame application opens in the Contents area.
4. In the Contents area, click **Install Corrective Service**. The Install Corrective Service window opens.
5. Select the **Corrective Service Version**, and select the frame where the service will be applied.

   Note: Unless you are directed otherwise, select the highest version number for the most recent fix.
6. Click **Install**. The installation may take up to an hour, depending on the number of parts in the frame that require an update. When installation is complete, a window opens to indicate installation status.

   Note: If you have replaced a single frame part and are using this procedure to update it, this process normally takes only two to five minutes.
7. If the installation fails, click **Reason for Failure**.
   a. If you are able to correct the problems(s), click **Cancel** and go to Step 6.
   b. If you are given an SRC, perform the steps to service the SRC, then return to this procedure.
   c. Otherwise, contact the next level of support.
8. After the corrective service has been applied successfully, click **Cancel** to return.

Configuring and Deconfiguring Processors or Memory

All failures that crash the system with a machine check or check stop, even if intermittent, are reported as a diagnostic callout for service repair. To prevent the recurrence of intermittent problems and improve the availability of the system until a scheduled maintenance window, processors and memory cards with a failure history are marked ″bad″ to prevent their being configured on subsequent boots.

A processor or memory card is marked ″bad″ under the following circumstances:

- A processor or memory card fails built-in self-test (BIST) or power-on self-test (POST) testing during boot (as determined by the service processor).
- A processor or memory card causes a machine check or check stop during runtime, and the failure can be isolated specifically to that processor or memory card (as determined by the processor runtime diagnostics in the service processor).
- A processor or memory card reaches a threshold of recovered failures that results in a predictive callout (as determined by the processor run-time diagnostics in the service processor).

During boot time, the service processor does not configure processors or memory cards that are marked “bad.”

If a processor or memory card is deconfigured, the processor or memory card remains offline for subsequent reboots until it is replaced or repeat gard is disabled. The repeat gard function also provides the user with the option of manually deconfiguring a processor or memory card, or re-enabling a previously deconfigured processor or memory card. For information about configuring or deconfiguring a processor, see the Processor Configuration/Deconfiguration Menu on page 25. For information on configuring or deconfiguring a memory card, see the Memory Configuration/Deconfiguration Menu on page 27. Both of these menus are submenus under the System Information Menu. You can enable or disable CPU Repeat Gard or Memory Repeat Gard using the Processor Configuration/Deconfiguration Menu.

Run-Time CPU Deconfiguration (CPU Gard)

L1 instruction cache recoverable errors, L1 data cache correctable errors, and L2 cache correctable errors are monitored by the processor runtime diagnostics (PRD) code running in the service processor. When a predefined error threshold is met, an error log with warning severity and threshold exceeded status is returned to AIX. At the same time, PRD marks the CPU for deconfiguration at the next boot. AIX will attempt to migrate all resources associated with that processor to another processor and then stop the defective processor.

Service Processor System Monitoring - Surveillance

Surveillance is a function in which the service processor monitors the system, and the system monitors the service processor. This monitoring is accomplished by periodic samplings called *heartbeats*.

Surveillance is available during the following phases:

- System firmware bringup (automatic)
- Operating system runtime (optional)

System Firmware Surveillance

System firmware surveillance is automatically enabled during system power-on. It cannot be disabled by the user, and the surveillance interval and surveillance delay cannot be changed by the user.

If the service processor detects no heartbeats during system IPL (for a set period of time), it cycles the system power to attempt a reboot. The maximum number of retries is set from the service processor menus. If the fail condition persists, the service processor leaves the machine powered on, logs an error, and displays menus to the user. If Call-out is enabled, the service processor calls to report the failure and displays the operating-system surveillance failure code on the operator panel on the HMC.

Operating System Surveillance

Note: This function is not available on a partitioned system.

Operating system surveillance provides the service processor with a means to detect hang conditions, as well as hardware or software failures, while the operating system is running. It also provides the operating system with a means to detect a service processor failure caused by the lack of a return heartbeat.

Operating system surveillance is not enabled by default, allowing you to run operating systems that do not support this service processor option.

You can also use service processor menus and AIX service aids to enable or disable operating system surveillance.

For operating system surveillance to work correctly, you must set these parameters:

- Surveillance enable/disable
- Surveillance interval

  The maximum time the service processor should wait for a heartbeat from the operating system before timeout.
- Surveillance delay

  The length of time to wait from the time the operating system is started to when the first heartbeat is expected.

Surveillance does not take effect until the next time the operating system is started after the parameters have been set.

If desired, you can initiate surveillance mode immediately from service aids. In addition to the three options above, a fourth option allows you to select immediate surveillance, and rebooting of the system is not necessarily required.

If operating system surveillance is enabled (and system firmware has passed control to the operating system), and the service processor does not detect any heartbeats from the operating system, the service processor assumes the system is hung and takes action according to the reboot/restart policy settings. See “Service Processor Reboot/Restart Recovery” on page 33.

If surveillance is selected from the service processor menus which are only available at bootup, then surveillance is enabled by default as soon as the system boots. From service aids, the selection is optional.

Service Processor Error Logs

The service processor error logs, an example of which follows, contain error conditions detected by the service processor.

```
                          Error Log

1. 11/30/99    19:41:56 Service Processor Firmware Failure
   B1004999

   Enter error number for more details.
   Press Return to continue, or 'x' to return to menu.
     Press "C" to clear error log, any other key to continue. >
```

Note: The time stamp in this error log is coordinated universal time (UTC), which is also referred to as Greenwich mean time (GMT). Operating system error logs have additional information available and can time stamp with local time.

Entering an error number provides nine words of system reference code (SRC) data; an example menu follows.

```
Detail:    6005

SRC
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
word11:B1004999      word12:0110005D      word13:00000000
word14:00000000      word15:00001111      word16:00000 000
word17:B1004AAA      word18:0114005D      word19:A4F1E909

B1004999

   Press Return to continue, or 'x' to return to menu.
```

If Return is pressed, the contents of NVRAM will be dumped 320 bytes at a time, starting at address 0000.

LCD Progress Indicator Log

The following is an example of the LCD progress indicator log. It shows the types of entries that can appear in the log, and is for example purposes only.

The progress indicator codes are listed from top (latest) to bottom (oldest).

```
                        LCD Progress Indicator Log
          B0FF
          0539..17
          0538..17
          0539..17
          0538..17
          0539..17
          0581
          0538..17
          0539..12
          0538..12
          0539..
          0821..01-K1-00
          0539..
          0728..01-R1-00-00
          0539..
          0664..40-60-00-1,0
          0539..
          0777..U0.1-P2-I1/E1
          0539..
          0742..U0.1-P2-I2/E1
          0539..
          0776..U0.1-P2-I3/T1
          E139
          E1FB
          E139
          E183
Press Return to continue, or 'x' to return to menu. >
          EAA1..U0.1-P1-I4
          E172..U0.1-P1
          E172..U0.1-P1-I4
          E172..U0.1-P1
          94BB
          9109
          9380
          9108
          9107
          9106
          9105
          9118
          9104
          9103
          9102
          90FD
```

Resetting the Service Processor

If required, the system is restarted by resetting the service processor. If the system is powered up, resetting the service processor will cause the system to shut down. When the service processor is reset, it goes through its power-up sequence, including self-tests. Successful completion of the reset sequence is indicated by OK on the HMC display.

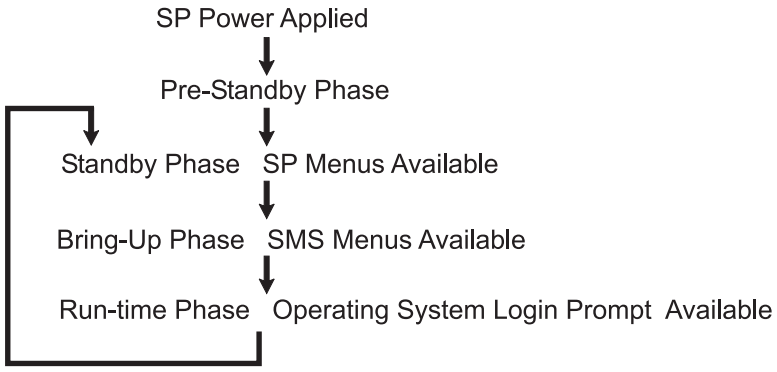
Before resetting the service processor, if the managed system is powered up and running, shut down all partitions, or the full system partition. This action causes the system to shutdown and the system power is turned off.

To reset the service processor when the managed system is powered off, perform either of the following:

- If the service processor is responding to input from the HMC, select **Service Processor Setup Menu** from the main menu, then select **Reset Service Processor**. This can only be done by a privileged user.
- Remove, then reapply, power using the HMC.

Service Processor Operational Phases

This section provides a high-level flow of the phases of the service processor.



Pre-Standby Phase

This phase is entered when the server is connected to a power source. The server may or may not be fully powered on. This phase is exited when the power-on self-tests (POSTs) and configuration tasks are completed.

The pre-standby phase components are:

- Service Processor Initialization - Service processor performs any necessary hardware and software initialization.
- Service Processor POST - Service processor conducts Power-on self-tests on its various work and code areas.
- Service Processor Unattended Start Mode Checks - To assist fault recovery. If unattended start mode is set, the service processor automatically reboots the server. The service processor does not wait for user input or power-on command, but moves through the phase and into the bring-up phase. Access the SMS menus or the service processor menus to reset the unattended start mode.

Standby Phase

The standby phase can be reached in either of the following ways:

- With the server off and power connected (the normal path), recognized by `0K` in the virtual operator panel.

  OR

- With the server on after an operating system fault, recognized by an 8-digit code in the virtual operator panel.

In the standby phase, the service processor takes care of some automatic duties and is available for menus operation. The service processor remains in the standby phase until a power-on request is detected.

The standby phase components are as follows:

- Menus

  The service processor menus are password-protected. Before you can access them, you need either the general user-password or privileged-user password.

  On HMC-managed systems, service processor menus are available on the HMC graphical user interface.

Bring-Up Phase

The bring-up phase components are as follows:

- Retry Request Check

  The service processor checks to see if the previous boot attempt failed. If the specified number of failures are detected, the service processor displays an error code.

- Dial Out

  This function is handled by the Service Agent code running on the HMC. The service processor issues an error report with the last reported IPL status indicated and any other available error information.

- Update Operator Panel (on the HMC)

  The service processor displays operator panel data on the HMC virtual terminal window if a remote connection is active.

- Environmental Monitoring

  The service processor provides expanded error recording and reporting.

- System Firmware Surveillance (Heartbeat Monitoring)

  The service processor monitors and times the interval between system firmware heartbeats.

- Responding to System Processor Commands

  The service processor responds to any command issued by the system processor.

Runtime Phase

This phase includes the tasks that the service processor performs during steady-state execution of the operating system.

- Environmental Monitoring

  The service processor monitors voltages, temperatures, and fan speeds (on some servers).

- Responding to System Processor Commands

  The service processor responds to any command issued by the system processor.

- Run-Time Surveillance

  If the device driver is installed and surveillance enabled, the service processor monitors the system heartbeat. If the heartbeat times out, the service processor places an outgoing call. This is different from the bring-up phase scenario, where the specified number of reboot attempts are made before placing an outgoing call.

- HMC surveillance

  On an HMC-managed system, the service processor monitors the communication link between the managed system and the HMC. If the service processor detects that this communication link has been broken, it will post an error to the operating system running on the managed system.

Clearing L3 Gard Records

Attention: The following menu should be accessed only by a customer engineer after an L3 cache module is replaced.

To reset clear the L3 module Gard records, perform the following steps:

1. At the service processor main menu, enter the access code 85712. A screen similar to the following is displayed.

```
        **** IBM Authorized USE ONLY ****


   This menu is for IBM authorized use only.
   If you have not been authoriz3ed to use this
   menu, plase sicontinue use immediately.

   Please press 'x' and return, for main menu
   or press any other key(s) and return, to continue

   0>
```

2. Press Enter. The following text is displayed at the bottom of the screen:

```
    Reset all L3 records
============================

    Want to clear all L3 records (y/n)?:

    Enter y.

   0>
```

3. Enter **y** to clear the records. A `Task Completed` message is displayed.

   Note: If ″n″ is entered, the ″(Press Return to Continue)″ message is displayed and the L3 Gard records are not cleared.

   This step ends the procedure for clearing the L3 Gard records.

Chapter 5. Using System Management Services

Use the system management services menus to view information about your system or partition, and to perform tasks such as setting a password, changing the boot list, and setting the network parameters.

To start the text-based System Management Services, press the number **1** key on the terminal or in the virtual operator panel on the HMC after the word **keyboard** appears and before the word **speaker** appears. After the text-based System Management Services starts, the following screen displays.

```
Main Menu

 1   Select Language
 2   Change Password Options NOT availabe in LPAR mode
 3   View Error Log
 4   Setup Remote IPL (Initial Program Load)
 5   Change SCSI Settings
 6   Select Console NOT availabe in LPAR mode
 7   Select Boot Options


-------------------------------------------------------------------------------
Navigation keys:

                                                  X = eXit System Management Services
-------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

On all menus except the Main Menu, there are several navigation keys:

M Return to the main menu.

ESC Return to the previous menu.

X Exit the System Management Services and start the operating system.

If X is entered, you are asked to confirm your choice to exit the SMS menus and start the operating system.

When there is more than one page of information to display, there are two additional navigation keys:

N Display the next page of the list.

P Display the next page of the list.

Note: The lowercase navigation key has the same effect as the uppercase key that is shown on the screen. For example, ″m″ or ″M″ takes you back to the main menu.

On each menu screen, you are given the option of choosing a menu item and pressing enter (if applicable), or selecting a navigation key.

Select Language

Note: Your virtual terminal must support the ISO-8859 character set to properly display languages other than English.

This option allows you to change the language used by the text-based System Management Services menus.

```
 SELECT LANGUAGE

  1.  English
  2.  Francais
  3.  Deutsch
  4.  Italiano
  5.  Espanol









--------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
--------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Change Password Options

Note: This option is not available when the system is booted in LPAR mode.

The Change Password Options menu enables you to select from password utilities.

```
Password Utilities

 1 Set Privileged-Access Password
 2 Remove Privileged-Access Password



--------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
--------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Set Privileged-Access Password

The priviledged-access password protects against the unauthorized starting of the system programs.

Attention: If the priviledged-access password has been enabled, you are asked for the priviledged-access password at startup every time you boot your system.

If you previously had set a priviledged-access password and want to remove it, select **Remove Privileged-Access Password**.

View Error Log

Use this option to view or clear your system's error log. A menu similar to the following displays when you select this option.

```
 Error Log

          Date       Time       Error Code      Location
 Entry 1. 01/04/96   12:13:22   25A80011        00-00
 Entry 2. no error logged

1. Clear error log



-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Note: The time stamp in this error log is coordinated universal time (UTC), which is also referred to as Greenwich mean time (GMT). Operating system error logs have more information available and can time stamp with your local time.

Setup Remote IPL (Initial Program Load)

This option allows you to enable and set up the remote startup capability of your system unit. You must first specify the network parameters.

```
Network Parameters

 1. IP Parameters
 2. Adapter Parameters
 3. Ping Test



-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Selecting the IP (Internet Protocol) Parameters option displays the following menu.

```
IP Parameters

 1. Client IP Address    [000.000.000.000]
 2. Server IP Address    [000.000.000.000]
 3. Gateway IP Address   [000.000.000.000]
 4. Subnet Mask          [255.255.255.000]




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

To change IP parameters, type the number of the parameters for which you want to change the value.

Attention: If the client system and the server are on the same subnet, set the gateway IP address to [0.0.0.0].

Selecting the **Adapter Parameters** option allows you to view an adapter's hardware address, as well as configure network adapters that require setup. A menu similar to the following displays.

```
 Device                                Slot              Hardware Address

 1. 10/100 Ethernet Adapter         4:U1.9-P1-I3/E1         000629aca72d
 2. 10/100 Ethernet Adapter         Integrated:U1.9-P1/E1   0020357A0530
 3. High Speed Token-Ring Adapter   1:U1.9-P1-I2/T1         000629be04e1
 4. Gigabit Ethernet PCI Adapter    3:U1.9-P1-I3/E1         0004ac7c9ec7




--------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
--------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Entering adapter parameters on these screens will automatically update the parameters on the ping test screen.

Selecting an adapter on this menu displays configuration menus for that adapter:

```
10/100 Ethernet TP PCI Adapter


1. Data Rate           [Auto]
2. Full Duplex         [Yes]







--------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
--------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Selecting the **Data Rate** option allows you the change the data rate used by the Ethernet adapter:

```
Data Rate

  1. 10 Mbps
  2. 100 Mbps
  3. Auto




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Selecting the **Full Duplex** option allows you to change how the Ethernet adapter communicates with the network:

```
Full Duplex

  1. Yes
  2. No
  3. Auto




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Select **Ping**, from the Network Parameters Menu, to test a connection to a remote system unit. After selecting the **Ping** option, you must choose which adapter communicates with the remote system.

```
 Adapter Parameters

 Device                                Slot              Hardware Address

 1. 10/100 Ethernet Adapter         4:U1.9-P1-I3/E1         000629aca72d
 2. 10/100 Ethernet Adapter         Integrated:U1.9-P1/E1   0020357A0530
 3. High Speed Token-Ring Adapter   1:U1.9-P1-I2/T1         000629be04e1
 4. Gigabit Ethernet PCI Adapter    3:U1.9-P1-I3/E1         0004ac7c9ec7




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

After selecting an adapter, you will be asked to set the parameters for the adapter; a menu similar to the following will be displayed:

```
Adapter Parameters
10/100 Ethernet Adapter
  1. Data Rate     [Auto]
  2. Full Duplex    [Auto]
  3. Continue with Ping




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

After choosing which adapter to use to ping the remote system, and setting its parameters, you must provide the addresses needed to communicate with the remote system.

```
Ping Test

 1. Client IP Address    [129.132.4.20]
 2. Server IP Address    [129.132.4.10]
 3. Gateway IP Address   [129.132.4.30]
 4. Subnet Mask          [255.255.255.0]
 5. Execute Ping Test




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

If changes to the adapter parameters must be made on this screen, entering those changes will not automatically update the adapter parameters screen. You must go back to the adapter parameters menu to make changes.

Notes:

1. After the ping test is initiated, it may take up to 60 seconds to return a result.
2. If the ping test passes or fails, the firmware will stop and wait for a key to be pressed before continuing.

Change SCSI Settings

This option allow you to view and change the addresses of the SCSI controllers attached to your system.

```
SCSI Utilities

  1. Hardware Spin Up Delay
  2. Change SCSI Id




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Select Console

Note: This function is not available on a partitioned system.

The Select Console Utility allows the user to select which console the user would like to use to display the SMS menus. This selection is only for the SMS menus and does not affect the display used by the operating system.

Follow the instructions that display on the screen. The firmware will automatically return to the SMS main menu.

Select Boot Options

Use this menu to view and set various options regarding the installation devices and boot devices.

```
  1. Select Install or Boot a Device
  2. Select Boot Devices
  3. Multiboot Startup




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Option 1

Select Install or Boot a Device, allows you to select a device to boot from or install the operating system from. This selection is for the current boot only.

Option 2

Select Boot Devices, allows you to set the boot list.

Option 3

Multiboot Startup, toggles the multiboot startup flag, which controls whether the multiboot menu is invoked automatically on startup.

If option 1 is selected, the following menu displays:

```
 Select Device Type
1.  Diskette
2.  Tape
3.  CD/DVD
4.  IDE
5.  Hard Drive
6.  Network
7.  None
8.  List All Devices




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

If a device is selected that does not reside in the system, a menu with the following message displays:

```
        .-----------------------------------------------------.
        | THE SELECTED DEVICES WERE NOT DETECTED IN THE SYSTEM !  |
        | Press any key to continue.                          |
        `-----------------------------------------------------'
```

If hard drive is selected, the following menu displays:

```
 Select Hard Drive Type
1.  SCSI
2.  SSA
3.  SAN
4.  None
5.  List All Devices




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

If List All Devices is selected, a menu similar to the following displays, depending on the devices that are installed in the system:

```
 Select Device
Device  Current  Device
Number  Position  Name
 1.        1      SCSI 18200 MB Harddisk (loc=U1.9-P1/Z1-A8,0)
 2.        -      SCSI 18200 MB Harddisk (loc=U1.9-P1/Z2-A9,0)
 3.        -      SCSI 18200 MB Harddisk (loc=U1.9-P1/Z2-Aa,0)
 4.   None
 5.  List all devices



--------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
--------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

The appropriate device can then be selected for this boot or installation.

When a device is selected for installing the operating system, or to boot from, the Select Task menu allows you to get more information about the device, or to boot from that device in normal mode or service mode. The following is an example of this menu.

```
 Select Task

SCSI 18200 MB Harddisk (loc=U1.9-P1/Z1-A8,0)

 1.  Information
 2.  Normal Mode Boot
 3.  Service Mode Boot



--------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
--------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

If either Normal Mode Boot or Service Mode Boot is selected, the next screen will ask, ″Are you sure?″. If you answer yes, the device will be booted in the appropriate mode. If you answer no, the firmware will return to the Select Task menu.

Select Boot Devices

Select this option to view and change the customized boot list, which is the sequence of devices read at startup.

```
 Configure Boot Device Order
 1.  Select 1st Boot Device
 2.  Select 2nd Boot Device
 3.  Select 3rd Boot Device
 4.  Select 4th Boot Device
 5.  Select 5th Boot Device
 6.  Display Current Setting
 7.  Restore Default Setting



-------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                    X = eXit System Management Services
-------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

When any of the options 1-5 is selected, the Select Device Type screen displays, which will be similar to the following.

```
 Select Device Type
 1.  Diskette
 2.  Tape
 3.  CD/DVD
 4.  IDE
 5.  Hard Drive
 6.  Network
 7.  None
 8.  List All Devices


-------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                    X = eXit System Management Services
-------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

When a device type is selected, a Select Task menu displays. The following is an example of that menu for a hard disk.

```
 Select Task

SCSI 18200 MB Harddisk (loc=U1.9-P1/Z1-A8,0)

 1.  Information
 2.  Set Boot Sequence: Configure as 1st Boot Device




--------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                    X = eXit System Management Services
--------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Selecting **Information** displays a menu similar to the following for a hard disk.

```
 Device Information
    /pci@3fffdf0a000/pci@2,4/scsi@1/sd@8,0
                  :  (Integrated)     (Bootable)
DEVICE            : SCSI 18200 MB Harddisk (loc=U1.9-P1/Z1-A8,0)
NAME              : sd
DEVICE-TYPE       : block




--------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                    X = eXit System Management Services
--------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

The Set Boot Sequence option allows you to set the location of the device in the boot list.

Display Current Settings

This option displays the current setting of the customized boot list. An example of this menu, with one device in the boot list, follows.

```
 Current Boot Sequence
 1.  SCSI 18200 MB Harddisk (loc=U1.9-P1/Z1-A8,0)
 2.   None
 3.   None
 4.   None
 5.   None




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Restore Default Settings

This option restores the boot list to the default boot list. The default boot list will vary depending on the devices that are installed in the system.

```
 The default boot list is:

1.  Primary diskette drive (if installed)
2.  CD-ROM drive (if installed)
3.  Tape drive (in installed)
4.  Hard disk drive (if installed)
5.  Network adapter




-------------------------------------------------------------------------------------------------
Navigation keys:
M = return to main menu
ESC key = return to previous screen                          X = eXit System Management Services
-------------------------------------------------------------------------------------------------
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Multiboot Startup

Multiboot Startup toggles the multiboot startup flag, which controls whether the multiboot menu is invoked automatically on startup.

Exiting System Management Services

After you have finished using the system management services, type **x** (for exit) to boot your system or partition.

Chapter 6. Using the Online and Standalone Diagnostics

Running diagnostics verifies system hardware operation. The diagnostics consist of online diagnostics and standalone diagnostics.

Note: The diagnostic procedures described in this chapter must be run for each processor subsystem installed in a rack.

Attention: The AIX operating system must be installed in a partition in order to run online diagnostics on that partition. If the AIX operating system is not installed, use the standalone diagnostic procedures.

Online diagnostics, when they are installed, reside with AIX in the file system. They can be booted:

- In single user mode (referred to as *service mode*)
- To run in maintenance mode (referred to as *maintenance mode*)
- To run concurrently with other applications (referred to as *concurrent mode*)

Standalone diagnostics must be booted before they can be run. If booted, the diagnostics have no access to the AIX error log or the AIX configuration data.

Online and Standalone Diagnostics Operating Considerations

Note: When possible, run online diagnostics in service mode. Online diagnostics perform additional functions compared to standalone diagnostics. Running online diagnostics in service mode ensures that the error state of the system that has been captured in NVRAM is available for your use in analyzing the problem. The AIX error log and certain SMIT functions are only available when diagnostics are run from the disk drive.

Consider the following items before using the diagnostics:

- Standalone diagnostics can run on systems configured for either a full (or single) system partition or a multiple partitioned system. When running in a partitioned system, the device from which you are booting standalone diagnostics must be made available to the partition dedicated to running standalone diagnostics. This may require moving the device from the partition that currently contains the boot device (for example, the network adapter connected to the Network Installation Management (NIM) server that has a standalone diagnostic image) to the partition used to run standalone diagnostics. If you move devices, reboot both partitions. For more information, see “Standalone Diagnostic Operation” on page 63.
- When diagnostics are installed, the device support for some devices might not get installed. If this is the case, that device does not display in the diagnostic test list when running disk-based diagnostics.
- When running diagnostics in a partitioned system, diagnostics function only with the resources that were assigned to that partition. You must run diagnostics in the partition containing the resource that you want to test.

Identifying the Terminal Type to the Diagnostics

When you run diagnostics, you must identify which type of terminal you are using. If the terminal type is not known when the FUNCTION SELECTION menu is displayed, the diagnostics do not allow you to continue until a terminal is selected from the DEFINE TERMINAL option menu. Choose the ″vt320″ selection when running diagnostics from an HMC.

Undefined Terminal Types

If you specify an undefined terminal type from the DEFINE TERMINAL option menu, the menu prompts the user to enter a valid terminal type. The menu redisplays until either a valid type is entered or you exit the DEFINE TERMINAL option.

Resetting the Terminal

If you enter a terminal type that is valid (according to the DEFINE TERMINAL option menu) but is not the correct type for the HMC virtual terminal window being used, you may be unable to read the screen, use the function keys, or use the Enter key. Bypass these difficulties by pressing Ctrl-C to reset the terminal. The screen display that results from this reset depends on the mode in which the system is being run:

- Online Normal or Maintenance Mode - The command prompt displays.
- Standalone Mode or Online Service Mode - The terminal type is reset to `dumb`, the Diagnostic Operating Instruction panel displays, and you are required to go through the DEFINE TERMINAL process again.

Running Online Diagnostics

Consider the following when you run the online diagnostics from a server or a disk:

- The diagnostics cannot be loaded and run from a disk until the AIX operating system has been installed and configured.
- The diagnostics cannot be loaded on a system (client) from a server if that system is not set up to boot from a server over a network. When the system is set up to boot from a server, the diagnostics are run in the same manner as they are from disk.
- On full system partitions, if the diagnostics are loaded from disk or a server, you must shut down the AIX operating system before turning off the system unit to prevent possible damage to disk data. Do this in either of the following ways:
  - If the diagnostics were loaded in standalone mode, press the F3 key until `DIAGNOSTIC OPERATING INSTRUCTIONS` displays. Then press the F3 key once again to shut down the AIX operating system.
  - If the diagnostics were loaded in maintenance or concurrent mode, type the `shutdown -F` command.
- Under some conditions, the system might stop, with instructions displayed on attached displays and terminals. Follow the instructions to select a console display.

Online Diagnostics Modes of Operation

Note: When running online diagnostics on a partition in a partitioned system, diagnostics can be run only on resources that are allocated to that partition.

The online diagnostics can be run in the following modes:

- Service Mode (see “Service Mode”). Refer to “Running Online Diagnostics in Service Mode” on page 62 for instructions on how to run the diagnostics in service mode.
- Concurrent Mode (see “Concurrent Mode” on page 61). Refer to “Running the Online Diagnostics in Concurrent Mode” on page 62 for instructions on how to run the diagnostics in service mode.
- Maintenance Mode (see “Maintenance Mode” on page 61). Refer to “Running the Online Diagnostics in Maintenance Mode” on page 62 for instructions on how to run the diagnostics in service mode.

Service Mode

Service mode provides the most complete checkout of the system resources. This mode also requires that no other programs be running on the partition or system on a full system partition. All partitions or system on a full system partition resources, except the SCSI adapter and the disk drives used for paging, can be tested. However, note that the memory and processor are only tested during POST, and the results of the POST tests are reported by diagnostics.

Error-log analysis is done in service mode when you select the Problem Determination option on the DIAGNOSTIC MODE SELECTION menu.

Concurrent Mode

Use concurrent mode to run online diagnostics on some of the system resources while the system is running normal activity.

Because the system is running in normal operation, the following resources cannot be tested in concurrent mode:

- SCSI adapters connected to paging devices
- Disk drive used for paging
- Some display adapters and graphics related devices
- Memory (tested during POST)
- Processor (tested during POST)

The following levels of testing exist in concurrent mode:

- The **share-test level** tests a resource while the resource is being shared by programs running in the normal operation. This testing is mostly limited to normal commands that test for the presence of a device or adapter.
- The **sub-test level** tests a portion of a resource while the remaining part of the resource is being used in normal operation. For example, this test could test one port of a multiport device while the other ports are being used in normal operation.
- The **full-test level** requires the device not be assigned to or used by any other operation. This level of testing on a disk drive might require the use of the **varyoff** command. The diagnostics display menus to allow you to vary off the needed resource.

Error-log analysis is done in concurrent mode when you select the Problem Determination option on the DIAGNOSTIC MODE SELECTION menu.

To run the online diagnostics in concurrent mode, you must be logged in to the AIX operating system and have proper authority to issue the commands (if help is needed, see the system operator).

The **diag** command loads the diagnostic controller and displays the online diagnostic menus.

Maintenance Mode

Maintenance mode runs the online diagnostics using the customer's version of the AIX operating system. This mode requires that all activity on the partition running the AIX operating system be stopped so that the online diagnostics have most of the resources available to check. All of the system resources, except the SCSI adapters, memory, processor, and the disk drive used for paging, can be checked.

Error log analysis is done in maintenance mode when you select the **Problem Determination** option on the DIAGNOSTIC MODE SELECTION menu.

Use the **shutdown -m** command to stop all activity on the AIX operating system and put the AIX operating system into maintenance mode. The **diag** command is then used to invoke the diagnostic controller so you can run the diagnostics. After the diagnostic controller is loaded, follow the normal diagnostic instructions.

Documentation for the AIX operating system is available from the IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base. Select **AIX documentation**. The *AIX Documentation* CD contains the base set of publications for the operating system, including system-management and end-user documentation.

Running Online Diagnostics in Service Mode

To run the online diagnostics in service mode from the boot hard disk, do the following:

1. From the HMC, select the **Partition Manager**.
2. Right-click on the mouse and select **Open Terminal Window**.
3. From the Service Processor Menu on the VTERM, select Option 2 **System Power Control**.
4. Select option 6. Verify that the state changes to `currently disabled`. Disabling fast system boot automatically enables slow boot.
5. Select Option 98 to exit the system power control menu.
6. Use the HMC to power on the managed system in a full system partition by selecting the managed system in the Contents area.
7. Right-click or select the desired system in the Contents area. Next, on the menu, choose **Selected**.
8. Select **Power On**.
9. Select the **Power on Diagnostic Stored Boot list** option (refer to "Full System Management Tasks" in the *IBM Hardware Management Console for pSeries Installation and Operations Guide*, for more information on full system partitions).
10. Enter any passwords, if requested.

    Note: If you are unable to load the diagnostics to the point when the `DIAGNOSTIC OPERATING INSTRUCTIONS` display, go to "Running Standalone Diagnostics from a Network Installation Management (NIM) Server" on page 63.

Running the Online Diagnostics in Concurrent Mode

To run online diagnostics in concurrent mode, do the following:

1. Log in to the AIX operating system as root user or use CE Login.
2. Enter the **diag** command.
3. When the DIAGNOSTIC OPERATING INSTRUCTIONS display, follow the instructions to check out the desired resources.
4. When testing is complete, use the F3 key to return to the DIAGNOSTIC OPERATING INSTRUCTIONS. Press the F3 key again to return to the AIX operating system prompt. Be sure to vary on any resource that you had varied to off.
5. Press Ctrl-D to log off from root user or CE Login.

Running the Online Diagnostics in Maintenance Mode

To run the online diagnostics in maintenance mode, do the following:

1. Stop all programs running on the partition except the AIX operating system (if help is needed, see the system operator).
2. Log in to the AIX operating system as root user or use CE Login.
3. Type the `shutdown -m` command.
4. When a message indicates the system is in maintenance mode, enter the **diag** command.

   Note: It might be necessary to set *TERM* type again.
5. When DIAGNOSTIC OPERATING INSTRUCTIONS screen displays, follow the displayed instructions to check out the desired resources.
6. When testing is complete, use the F3 key to return to DIAGNOSTIC OPERATING INSTRUCTIONS. Press the F3 key again to return to the AIX operating system prompt.
7. Press Ctrl-D to log off from root user or CE Login.

Standalone Diagnostic Operation

Use standalone diagnostics to test the system when the online diagnostics are not installed and as a method of testing the disk drives that cannot be tested by the online diagnostics.

Note: No error log analysis is done by the standalone diagnostics. The standalone diagnostics:

- Are resident on a Network Installation Management (NIM) server
- Provide a method to test the system when the online diagnostics are not installed or cannot be loaded from the disk drive
- Allow testing of the disk drives and other resources that cannot be tested by the online diagnostics
- Do not have access to the AIX configuration data
- Do not have access to the AIX error log
- Do not allow for running of error log analysis

Performing Slow Boot

To fully analyze all of the available information, perform the following steps before doing a hardware repair or replacement:

1. Record the 8-character error code (and location code if present) displayed as the operator panel value displayed on the HMC or that was reported by the customer.
2. Do a slow-mode boot in service mode. This boot can be specified using the System Power Control Menu on the service processor main menu. (A fast-mode boot skips much of the built-in diagnostic testing.) A slow-mode boot may yield a new 8-character error code displayed as an operator panel value on the HMC and new errors in the service processor error log. If a new error code is reported, use this code to continue problem analysis.

Partitioned System Considerations for Standalone Diagnostics

To run standalone diagnostics on a full system partition, you must reboot the entire system. However, for a partition in a partitioned system, you can boot standalone diagnostics either in a given partition or on the entire system (which is the same procedure as a full system partition). For a partitioned system, before running standalone diagnostics on a given partition, the user must move the device from the existing location where standalone diagnostics is booted (the network adapter connected to the NIM server, in the case of NIM boot of standalone diagnostics), to the partition that will run standalone diagnostics. Devices in a partitioned system are moved on an I/O-slot basis.

Running Standalone Diagnostics from a Network Installation Management (NIM) Server

A client system connected to a network with a NIM server can boot standalone diagnostics from the NIM server if the client-specific settings on both the NIM server and client are correct.

Notes:

1. All operations to configure the NIM server require root user authority.
2. If you replace the network adapter in the client, the network adapter hardware address settings for the client must be updated on the NIM server.
3. The **Cstate** for each standalone diagnostics client on the NIM server should be kept in the *diagnostic boot has been enabled* state.
4. On the client partition, the NIM server network adapter can be put in the bootlist after the boot disk drive. This allows the system to boot in standalone diagnostics from the NIM server if there is a problem booting from the disk drive. Another option is to use the **Select Boot Options** function in the SMS menu to set up the network adapter that is connected to the NIM server for a one-time boot of standalone diagnostics.

NIM Server Configuration

Refer to the “Advanced NIM Configuration Tasks” chapter of the *AIX Installation Guide and Reference*, for information on doing the following:

- Registering a client on the NIM server
- Enabling a client to run diagnostics from the NIM server

To verify that the client system is registered on the NIM server and the diagnostic boot is enabled, run the command `lsnim -a Cstate -Z` *ClientName* from the command line on the NIM server. Refer to the following table for system responses.

Note: The *ClientName* is the name of the system on which you want to run standalone diagnostics.

System Response	Client Status
`#name:Cstate:` `ClientName:diagnostic boot has been enabled:`	The client system is registered on the NIM server and enabled to run diagnostics from the NIM server.

`#name:Cstate:`
`ClientName:ready for a NIM operation:`
 	
or
`#name:Cstate:`
`ClientName:BOS installation has been enabled:`
	The client is registered on the NIM server but not enabled to run diagnostics from the NIM server.
	Note: If the client system is registered on the NIM server but Cstate has not been set, no data will be returned.

`0042-053 lsnim: there is no NIM object named "ClientName"`	The client is not registered on the NIM server.

Client Configuration and Booting Standalone Diagnostics from the NIM Server

To run standalone diagnostics on a client from the NIM server, do the following:

1. Stop all programs including the AIX operating system (get help if needed).
2. If you are running standalone diagnostics in a full system partition, verify with the system administrator and system users that the system unit can be shut down. Stop all programs, including the AIX operating system. Refer to the AIX operating system documentation for **shutdown** command information.

   Verify with the system administrator and system users using that partition that all applications on that partition must be stopped, and that the partition will be rebooted. Stop all programs on that partition, including the operating system.
3. If you are in a full system partition, power on the system unit to run standalone diagnostics. In a partitioned system, reboot the partition to run standalone diagnostics.
4. When the keyboard indicator is displayed (the word **keyboard** on an HMC virtual terminal window), press the number 1 key on the keyboard to display the SMS menu.
5. Enter any requested passwords.
6. Select **Setup Remote IPL (Initial Program Load)**.
7. Enter the client address, server address, gateway address (if applicable), and subnet mask.
8. If the NIM server is set up to allow pinging from the client system, use the **ping** utility in the RIPL utility to verify that the client system can ping the NIM server. Under the **ping** utility, choose the network adapter that provides the attachment to the NIM server to do the ping operation. If the ping returns with an `OK` prompt, the client is prepared to boot from the NIM server. If ping returns with a `FAILED` prompt, the client cannot proceed with the NIM boot.

Note: If the ping fails, refer to the *Boot Problems* section of the *@server pSeries 655 Service Guide* and follow the steps for network boot problems.

To do a one-time boot of the network adapter attached to the NIM server network, do the following:

1. Exit to the SMS Main screen.
2. Select **Select Boot Options**.
3. Select **Install or Boot a Device**.
4. On the **Select Device Type** screen, select **Network**.
5. Set the network parameters for the adapter from which you want to boot.
6. Exit completely from SMS.

   The system starts loading packets while doing a **bootp** from the network.

Follow the instructions on the screen to select the system console.

- If `Diagnostics Operating Instructions Version x.x.x` displays, standalone diagnostics have loaded successfully.
- If the AIX login prompt displays, standalone diagnostics did not load. Check the following items:
  - The network parameters on the client may be incorrect.
  - Cstate on the NIM server may be incorrect.
  - Network problems might be preventing you from connecting to the NIM server.

Verify the settings and the status of the network. If you continue to have problems, refer to the *Boot Problems* section of the *@server pSeries 655 Service Guide* and follow the steps for network boot problems.

Chapter 7. Introduction to Tasks and Service Aids

The AIX Diagnostic Package contains programs that are called *Tasks*. Tasks can be thought of as performing a specific function on a resource; for example, running diagnostics or performing a service aid on a resource.

Note: Many of these programs work on all system model architectures. Some programs are only accessible from Online Diagnostics in Service or Concurrent mode, while others might be accessible only from Standalone Diagnostics. Still other programs might only be supported on a particular system architecture, such as CHRP (Common Hardware Reference Platform) or RSPC (PowerPC Reference Platform).

Note: If the system is running on a logically partitioned system, the following tasks may only be executed in a partition with service authority:

- Configure Reboot Policy
- Configure Remote Maintenance Policy
- Configure Ring Indicate Power-On Policy
- Update System or Service Processor Flash
- Configure Scan Dump Policy

To perform one of these tasks, use the Task Selection option from the FUNCTION SELECTION menu.

After a task is selected, a resource menu may be presented, showing all resources supported by the task.

A fast path method is also available to perform a task by using the **diag** command and the **-T** flag. By using the fast path, the user can bypass most of the introductory menus to access a particular task. The user is presented with a list of resources available to support the specified task. The fast path tasks are as follows:

- Certify - Certifies media
- Chkspares - Checks for the availability of spare sectors
- Download - Downloads microcode to an adapter or device
- Disp_mcode - Displays current level of microcode
- Format - Formats media
- Identify - Identifies the PCI RAID physical disks
- IdentifyRemove - Identifies and removes devices (Hot Plug)

To run these tasks directly from the command line, specify the resource and other task-unique flags. Use the descriptions in this chapter to understand which flags are needed for a given task.

Tasks

The following tasks are described in this chapter:

- Add Resource to Resource List
- AIX Shell Prompt
- Analyze Adapter Internal Log
- Backup and Restore Media
- Certify Media
- Change Hardware Vital Product Data
- Configure Dials and LPF Keys
- Configure ISA Adapters
- Configure Reboot Policy
- Configure Remote Maintenance Policy
- Configure Ring Indicate Power-On Policy

- Configure Scan Dump Policy
- Configure Surveillance Policy
- Create Customized Configuration Diskette
- Delete Resource from Resource List
- Disk Maintenance
- Display Configuration and Resource List
- Display Firmware Device Node Information
- Display Hardware Error Report
- Display Hardware Vital Product Data
- Display Machine Check Error Log
- Display Microcode Level
- Display or Change Bootlist
- Display or Change Diagnostic Run Time Options
- Display Previous Diagnostic Results
- Display Resource Attributes
- Display Service Hints
- Display Software Product Data
- Display System Environmental Sensors
- Display Test Patterns
- Display USB Devices
- Download Microcode
- Fibre Channel RAID Service Aids
- Flash SK-NET FDDI Firmware
- Format Media
- Gather System Information
- Generic Microcode Download
- Hot Plug Task
- Local Area Network Analyzer
- Log Repair Action
- Periodic Diagnostics
- PCI RAID Physical Disk Identify
- Process Supplemental Media
- Run Diagnostics
- Run Error Log Analysis
- Run Exercisers
- SCSI Bus Analyzer
- SCSD Tape Drive Service Aid
- Spare Sector Availability
- SSA Service Aid
- System Fault Indicator
- System Identify Indicator
- Update Disk-Based Diagnostics
- Update System or Service Processor Flash
- 7135 RAIDiant Array Service Aids
- 7318 Serial Communication Network Server

Add Resource to Resource List

Use this task to add resources back to the resource list.

Note: Only resources that were previously detected by the diagnostics and deleted from the Diagnostic Test List are listed. If no resources are available to be added, then none are listed.

AIX Shell Prompt

Note: Use this service aid in Online Service Mode only.

This service aid allows access to the AIX command line. To use this service aid, the user must know the root password (when a root password has been established).

Note: Do not use this task to install code or to change the configuration of the system. This task is intended to view files, configuration records, and data. Using this service aid to change the system configuration or install code can produce unexplained system problems after exiting the diagnostics.

Analyze Adapter Internal Log

The PCI RAID adapter has an internal log that logs information about the adapter and the disk drives attached to the adapter. Whenever data is logged in the internal log, the device driver copies the entries to the AIX system error log and clears the internal log.

The Analyze Adapter Internal Log service aid analyzes these entries in the AIX system error log. The service aid displays the errors and the associated service actions. Entries that do not require any service actions are ignored.

When running this service aid, a menu is presented to enter the start time, the end time, and the file name. The start time and end time have the following format: [*mmddHHMMyy*]. (where *mm* is the month (1-12), *dd* is the date (1-31) *HH* is the hour (00-23) *MM* is the minute (00-59), and *yy* is the last two digits of the year (00-99). The file name is the location where the user wants to store the output data.

To invoke the service aid task from the command line, type:

`diag -c -d devicename -T "adapela [-s start date -e end date]`

Flag	Description
-c	Specifies not console mode.
-d *devicename*	Specifies the device whose internal log you want to analyze (for example, `SCRAID0`)
-s *start date*	Specifies all errors after this date are analyzed.
-e *end date*	Specifies all errors before this date are analyzed.
-T	Specifies the Analyze Adapter Internal Log task

Note: To specify a file name from the command line, use the redirection operator at the end of the command to specify where the output of the command is to be sent, for example `> filename` (where `filename` is the name and location where the user wants to store the output data (for example, `/tmp/adaptlog`).

Backup and Restore Media

This service aid allows verification of backup media and devices. It presents a menu of tape and diskette devices available for testing and prompts for selecting the desired device. It then presents a menu of available backup formats and prompts for selecting the desired format. The supported formats are **tar**, **backup**, and **cpio**. After the device and format are selected, the service aid backs up a known file to the selected device, restores that file to **/tmp**, and compares the original file to the restored file. The restored file remains in **/tmp** to allow for visual comparison. All errors are reported.

Certify Media

This task allows the selection of diskette, DVD-RAM media or hard files to be certified. Normally, this is done for the following two conditions:

- To determine the condition of the drive and media.
- To verify that the media is error free after a Format Service Aid has been run on the media.

Normally, one would run certify if after running diagnostics on a drive and its media, no problem is found, but one still suspects that a problem still does exist.

Hard files can be connected either to a SCSI adapter (non-RAID) or a PCI SCSI RAID adapter. The usage and criteria for a hard file connected to a non-RAID SCSI adapter are different from those for a hard file connected to a PCI SCSI RAID adapter.

Certify may be used in the following ways:

- Certify Diskette

  This selection enables you to verify the data written on a diskette. When you select this service aid, a menu asks you to select the type of diskette being verified. The program then reads all of the ID and data fields on the diskette one time and displays the total number of bad sectors found.
- Certify DVD-RAM media

  This selection reads all of the ID and data fields. It checks for bad data and counts all errors encountered. If an unrecovered error occurs, or recovered errors exceed the threshold value, the data on the media should be transferred to other media and the original media should be discarded.

  The Certify service aid will display the following information:
  - Capacity in bytes
  - Number of Data Errors Not Recovered
  - Number of Equipment Check Errors
  - Number of Recovered Errors

  If the drive is reset during a certify operation, the operation is restarted.

  If the drive is reset again, the certify operation is terminated and the user is asked to run diagnostics on the drive.

  This task can be run directly from the AIX command line. See the following command syntax: `diag -c -d -T certify`

Flag	Description
-c	No console mode
-d	Specifies a device
-T	Specifies the certify task
- Certify Hardfile Attached to a Non-RAID SCSI Adapter

  This selection reads all of the ID and data fields. It checks for bad data and counts all errors encountered. If there are unrecovered data errors that do not exceed the threshold value, then the hard file needs to be formatted and certified. If the unrecovered data errors, recovered data errors, recovered and unrecovered equipment errors exceed the threshold values, the disk needs to be replaced.

  It also makes 2000 random seeks after the read certify of the surface completes. If a disk timeouts before finishing the random seeks, then the disk needs to be replaced. The random seeks also count all errors encountered.

  The Certify service aid will display the following information:
  - Drive capacity in megabytes.
  - Number of Data Errors Recovered.
  - Number of Data Errors Not Recovered.

– Number of Equipment Checks Recovered.
– Number of Equipment Checks Not Recovered.

This task can be run directly from the AIX command line. See the following command syntax: `diag -c -d` *deviceName* `-T "certify"`

Flag	Description
-c	No console mode
-d	Specifies a device
-T	Specifies the certify task

- Format and/or Erase Hardfile Attached to a Non-RAID SCSI Adapter

  Attention: The following commands WILL change the content of the hardfile. Be sure to backup data prior to running the command, and take care in choosing the hardfile upon which you run this task.

  – Hardfile Format

    Writes all of the disk. The pattern written on the disk is device-dependant; for example, some drives may write all 0s, while some may write the hexadecimal number 5F. No bad block reassignment occurs.

  – Hardfile Format and Certify

    Performs the same function as Hardfile Format. After the format is completed, Certify is run. Certify then reassigns all bad blocks encountered.

  – Hardfile Erase Disk

    This option can be used to overwrite (remove) all data currently stored in user-accessible blocks of the disk. The Erase Disk option writes one or more patterns to the disk. An additional option allows data in a selectable block to be read and displayed on the system console.

    To use the Erase Disk option, specify the number (0-3) of patterns to be written. The patterns are written serially; that is, the first pattern is written to all blocks. Then the next pattern is written to all blocks, overlaying the previous pattern. A random pattern is written by selecting the Write Random Pattern option.

    Note: The Erase Disk service aid has not been certified as meeting the Department of Defense or any other organization's security guidelines.

    Use the following steps to overwrite the data on the drive:

    1. Use the Erase Disk selection to overwrite the data on the drive.
    2. Do a format without certify.
    3. Run a second pass of the Erase Disk selection.

    For a newly installed drive, you can ensure that all blocks on the drive are overwritten with your pattern if you use the following procedure:

    1. Format the drive.
    2. Check the defect MAP by running the Erase Disk selection.

       Note: If you use Format and Certify option, there may be some blocks which get placed into the grown defect MAP.

    3. If there are bad blocks in the defect MAP, record the information presented and ensure that this information is kept with the drive. This data is used later when the drive is to be overwritten.
    4. Use you drive as you would normally.
    5. When the drive is no longer needed and is to be erased, run the same version of the Erase Disk selection which was used in step 2.

       Note: Using the same version of the service aid is only critical if any bad blocks were found in step 3.

6. Compare the bad blocks which were recorded for the drive in step 3 with those that now appear in the grown defect MAP.

   Note: If there are differences between the saved data and the newly obtained data, then all sectors on this drive cannot be overwritten. The new bad blocks are not overwritten.

7. If the bad block list is the same, continue running the service aid to overwrite the disk with the chosen pattern(s).

This task can be run directly from the AIX command line. See the command syntax: `diag -c -d` *`deviceName`* `-T "format [-s* fmtcert | erase -a {read | write}] [-F]*`

Flag	Description
fmtcert	Formats and certifies the disk.
erase	Overwrites the data on the disk.
*	Available in no-console mode only.
-F	Force the disk erasure even if all blocks cannot be erased due to errors accessing the grown defect map.

Note: The Erase Disk option in command line mode uses default values. To selectively read or write, use the **diag** command in console mode.

- Certify Hardfile attached to a PCI SCSI RAID Adapter

  This selection is used to certify physical disks attached to a PCI SCSI RAID adapter. Certify reads the entire disk and checks for recovered errors, unrecovered errors, and reassigned errors. If these errors exceed the threshold values, the user is prompted to replace the physical disk.

  This task can be run directly from the AIX command line. See the following command syntax: `diag -c -d` *`RAIDadapterName`* `-T "certify {-l` *`chID`* `| -A}"`

Flag	Description
-c	No console mode
-d	Specifies the RAID adapter to which the disk is attached
-T	Specifies the certify task and its parameters
-l	Specifies physical Disk channel/ID (example: -l 27)
-A	All disks

Change Hardware Vital Product Data

Use this service aid to display the Display/Alter VPD Selection Menu. The menu lists all resources installed on the system. When a resource is selected, a menu displays that lists all the VPD for that resource.

Note: The user cannot alter the VPD for a specific resource unless it is not machine-readable.

Configure Dials and LPF Keys

Note: The Dials and LPF Keys service aid is not supported in standalone mode (CD-ROM and NIM) on systems with 32 MB or less memory. If you have problems in standalone mode, use the hardfile-based diagnostics.

This service aid provides a tool for configuring and removing dials and LPF keys to the asynchronous serial ports.

This selection invokes the SMIT utility to allow Dials and LPF keys configuration. A TTY must be in the available state on the async port before the Dials and LPF keys can be configured on the port. The task allows an async adapter to be configured, then a TTY port defined on the adapter. Dials and LPF keys can then be defined on the port.

Before configuring Dials or LPF keys on a serial port, you must remove all defined TTYs. To determine if there are any defined TTYs, select **List All Defined TTYs**. Once all defined TTYs have been removed, then add a new TTY and configure the Dials or LPF keys.

Configure ISA Adapter

This task uses SMIT to identify and configure ISA adapters on systems that have an ISA bus and adapters.

Diagnostic support for ISA adapters not shown in the list may be supported from a supplemental diskette. You can use the Process Supplemental Media task to add ISA adapter support from a supplemental diskette.

Whenever an ISA adapter is installed, this service aid must be run and the adapter configured before the adapter can be tested. You must also run this service aid to remove an ISA adapter from the system whenever an ISA adapter is physically removed from the system.

If diagnostics are run on an ISA adapter that has been removed from the system, the diagnostics fail because the system cannot detect the ISA adapter.

Configure Reboot Policy

Note: This service aid runs on CHRP system units only.

This service aid controls how the system tries to recover from a system crash.

Use this service aid to display and change the following settings for the Reboot Policy.

Note: Because of system capability, some of the following settings might not be displayed by this service aid.

- Maximum Number of Reboot Attempts

  Enter a number that is 0 or greater.

  Note: A value of 0 indicates 'do not attempt to reboot' to a crashed system.

  This number is the maximum number of consecutive attempts to reboot the system. The term *reboot*, in the context of this service aid, is used to describe bringing system hardware back up from scratch; for example, from a system reset or power-on.

  When the reboot process completes successfully, the reboot attempts count is reset to 0, and a restart begins. The term *restart*, in the context of this service aid, is used to describe the operating system activation process. Restart always follows a successful reboot.

  When a restart fails, and a restart policy is enabled, the system attempts to reboot for the maximum number of attempts.
- Use the O/S Defined Restart Policy (1=Yes, 0=No)

  When 'Use the O/S Defined Restart Policy' is set to Yes, the system attempts to reboot from a crash if the operating system has an enabled Defined Restart or Reboot Policy.

When 'Use the O/S Defined Restart Policy' is set to No, or the operating system restart policy is undefined, then the restart policy is determined by the 'Supplemental Restart Policy'.

- Enable Supplemental Restart Policy (1=Yes, 0=No)

  The 'Supplemental Restart Policy', if enabled, is used when the O/S Defined Restart Policy is undefined, or is set to False.

  When surveillance detects operating system inactivity during restart, an enabled 'Supplemental Restart Policy' causes a system reset and the reboot process begins.
- Call-Out Before Restart (on/off)

  When enabled, Call-Out Before Restart allows the system to call out (on a serial port that is enabled for call-out) when an operating system restart is initiated. Such calls can be valuable if the number of these events becomes excessive, thus signalling bigger problems.
- Enable Unattended Start Mode (1=Yes, 0=No)

  When enabled, 'Unattended Start Mode' allows the system to recover from the loss of ac power.

  If the system was powered-on when the ac loss occurred, the system reboots when power is restored. If the system was powered-off when the ac loss occurred, the system remains off when power is restored.

You can access this service aid directly from the AIX command line, by typing:
`/usr/lpp/diagnostics/bin/uspchrp -b`

Configure Remote Maintenance Policy

Note: This service aid runs on CHRP system units only.

The Remote Maintenance Policy includes modem configurations and phone numbers to use for remote maintenance support.

Use this service aid to display and change the following settings for the Remote Maintenance Policy.

Note: Because of system capability, some of the following settings might not be displayed by this service aid.

- Configuration File for Modem on serial port 1 (S1) Configuration File for Modem on serial port 2 (S2).

  Enter the name of a modem configuration file to load on either S1 or S2. The modem configuration files are located in the directory **/usr/share/modems**. If a modem file is already loaded, it is indicated by `Modem file currently loaded`.
- Modem file currently loaded on S1 Modem file currently loaded on S2

  This is the name of the file that is currently loaded on serial port 1 or serial port 2.

  Note: These settings are only shown when a modem file is loaded for a serial port.
- Call In Authorized on S1 (on/off) Call In Authorized on S2 (on/off)

  Call In allows the Service Processor to receive a call from a remote terminal.
- Call Out Authorized on S1 (on/off) Call Out Authorized on S2 (on/off)

  Call Out allows the Service Processor to place calls for maintenance.
- S1 Line Speed S2 Line Speed

  A list of line speeds is available by using **List** on the screen.
- Service Center Phone Number

  This is the number of the service center computer. The service center usually includes a computer that takes calls from systems with call-out capability. This computer is referred to as ″the catcher.″ The catcher expects messages in a specific format to which the Service Processor conforms. For more

information about the format and catcher computers, refer to the README file in the AIX **/usr/samples/syscatch** directory. Contact the service provider for the correct telephone number to enter here.

- Customer Administration Center Phone Number

  This is the number of the System Administration Center computer (catcher) that receives problem calls from systems. Contact the system administrator for the correct telephone number to enter here.
- Digital Pager Phone Number In Event of Emergency

  This is the number for a pager carried by someone who responds to problem calls from your system.
- Customer Voice Phone Number

  This is the number for a telephone near the system, or answered by someone responsible for the system. This is the telephone number left on the pager for callback.
- Customer System Phone Number

  This is the number to which your system's modem is connected. The service or administration center representatives need this number to make direct contact with your system for problem investigation. This is also referred to as the `Call In phone number`.
- Customer Account Number

  This number is available for service providers to use for record-keeping and billing.
- Call Out Policy Numbers to call if failure

  This is set to either First or All. If the call-out policy is set to First, call out stops at the first successful call to one of the following numbers in the order listed:
  1. Service Center
  2. Customer Administration Center
  3. Pager

  If Call Out Policy is set to All, call-out attempts to call all of the following numbers in the order listed:
  1. Service Center
  2. Customer Administration Center
  3. Pager
- Customer RETAIN Login ID Customer RETAIN Login Password

  These settings apply to the RETAIN service function.
- Remote Timeout, in seconds Remote Latency, in seconds

  These settings are functions of the service provider's catcher computer.
- Number of Retries While Busy

  This is the number of times the system should retry calls that resulted in busy signals.
- System Name (System Administrator Aid)

  This is the name given to the system and is used when reporting problem messages.

  Note: Knowing the system name aids the support team in quickly identifying the location, configuration, history, and so on of your system.

You can access this service aid directly from the AIX command line, by typing:
`/usr/lpp/diagnostics/bin/uspchrp -m`

Configure Ring Indicate Power-On Policy

Note: This service aid runs on CHRP system units only.

This service aid allows the user to power-on a system by telephone from a remote location. If the system is powered off, and Ring Indicate Power On is enabled, the system powers on at a predetermined number of rings. If the system is already on, no action is taken. In either case, the telephone call is not answered, and the caller receives no feedback that the system has powered on.

Use this service aid to display and change the following settings for the Ring Indicate Power-On Policy:

Note: Because of system capability, some of the following settings might not be displayed by this service aid.

- Power On Via Ring Indicate (on/off)
- Number of Rings Before Power On

You can access this service aid directly from the AIX command line, by typing:

```
/usr/lpp/diagnostics/bin/uspchrp -r
```

Configure Scan Dump Policy

Note: This function works only on CHRP systems and only under diagnostics 5.1.0.35 or later.

Configure Scan Dump Policy allows the user to set or view the scan dump policy (scan dump control and size) in NVRAM. Scan Dump data is a set of chip data that the service processor gathers after a system malfunction. It consists of chip scan rings, chip trace arrays, and Scan COM (SCOM) registers. This data is stored in the scan-log partition of the system's Nonvolatile Random Access Memory (NVRAM).

Use this service aid to display and change the following settings for the Scan Dump Policy at run time:

- Scan Dump Control (how often the dump is taken)

and

- Scan Dump Size (size and content of the dump)

The Scan Dump Control (SDC) settings are:

- As Needed: This setting allows the platform firmware to determine whether a scan dump is performed. This is the default setting for the dump policy.
- Always: This setting overrides the firmware recommendations and always performs a dump after a system failure.

The Scan Dump Size (SDS) settings are:

- As Requested - Dump content is determined by the platform firmware.
- Minimum - Dump content collected provides the minimum debug information. The intent is to allow the platform to reboot as quickly as possible.
- Optimum - Dump content collected provides a moderate amount of debug information.
- Complete - Dump data provides the most complete error coverage at the expense of reboot speed.

You can access this task directly from the AIX command line by typing:

```
/usr/lpp/diagnostics/bin/uspchrp -d
```

Configure Surveillance Policy

Note: This service aid runs on CHRP system units only. This service aid is only supported for systems running in full machine partition.

This service aid monitors the system for hang conditions; that is, hardware or software failures that cause operating system inactivity. When enabled, and surveillance detects operating system inactivity, a call is placed to report the failure.

Use this service aid to display and change the following settings for the Surveillance Policy:

Note: Because of system capability, some of the following settings might not be displayed by this service aid:

- Surveillance (on/off)
- Surveillance Time Interval

  This is the maximum time between heartbeats from the operating system.
- Surveillance Time Delay

  This is the time to delay between when the operating system is in control and when to begin operating system surveillance.
- Changes are to Take Effect Immediately

  Set this to Yes if the changes made to the settings in this menu are to take place immediately. Otherwise the changes take effect beginning with the next system boot.

You can access this service aid directly from the AIX command line, by typing:
`/usr/lpp/diagnostics/bin/uspchrp -s`

Create Customized Configuration Diskette

This selection invokes the Diagnostic Package Utility Service Aid, which allows the user to create a standalone diagnostic package configuration diskette.

The Standalone Diagnostic Package Configuration Diskette allows the following to be changed from the console:

- Default refresh rate for a low function terminal (LFT)

  The refresh rate used by the standalone diagnostic package is 60 Hz. If the display's refresh rate is 77 Hz, set the refresh rate to 77.
- Different async terminal console

  You can create a console configuration file that allows a terminal attached to any RS232 or RS422 adapter to be selected as a console device. The default device is an RS232 TTY device attached to the first standard serial port (S1).

Delete Resource from Resource List

Use this task to delete resources from the resource list.

Note: Only resources that were previously detected by the diagnostics and have not been deleted from the Diagnostic Test List are listed. If no resources are available to be deleted, then none are listed.

Disk Maintenance

This service aid provides the following options for the fixed-disk maintenance:
- Disk to Disk Copy
- Display/Alter Sector

Disk to Disk Copy

Notes:

1. This service aid cannot be used to update to a different size drive. The service aid only supports copying from a SCSI drive to another SCSI drive of similar size.
2. Use the **migratepv** command when copying the contents to other disk drive types. This command also works when copying SCSI disk drives or when copying to a different size SCSI disk drive. Refer to *AIX System Management Guide: Operating System and Devices* for a procedure on migrating the contents of a physical volume.

   Documentation for the AIX operating system is available from the IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base. Select **AIX documentation**. The *AIX Documentation* CD contains the base set of publications for the operating system, including system-management and end-user documentation.

This selection allows you to recover data from an old drive when replacing it with a new drive. The service aid recovers all logical volume manager (LVM) software reassigned blocks. To prevent corrupted data from being copied to the new drive, the service aid stops if an unrecoverable read error is detected. To help prevent possible problems with the new drive, the service aid stops if the number of bad blocks being reassigned reaches a threshold.

To use this service aid, both the old and new disks must be installed in or attached to the system with unique SCSI addresses. This requires that the new disk drive SCSI address must be set to an address that is not currently in use and the drive be installed in an empty location. If there are no empty locations, then one of the other drives must be removed. When the copy is complete, only one drive can remain installed. Either remove the target drive to return to the original configuration, or perform the following procedure to complete the replacement of the old drive with the new drive:

1. Remove both drives.
2. Set the SCSI address of the new drive to the SCSI address of the old drive.
3. Install the new drive in the old drive's location.
4. Install any other drives (that were removed) into their original location.

To prevent problems that can occur when running this service aid from disk, it is suggested that this service aid be run, when possible, from the diagnostics that are loaded from removable media.

Display/Alter Sector

Note: Use caution when you use this service aid because inappropriate modification to some disk sectors can result in the total loss of all data on the disk.

This selection allows the user to display and alter information on a disk sector. Sectors are addressed by their decimal sector number. Data is displayed both in hex and in ASCII. To prevent corrupted data from being incorrectly corrected, the service aid does not display information that cannot be read correctly.

Display Configuration and Resource List

If a device is not included in the Test List or if you think a Diagnostic Package for a device is not loaded, check by using the Display Configuration and Resource List task. If the device you want to test has a plus (+) sign or a minus (-) sign preceding its name, the Diagnostic Package is loaded. If the device has an asterisk (*) preceding its name, the Diagnostic Package for the device is not loaded or is not available.

This service aid displays the item header only for all installed resources. Use this service aid when there is no need to see the vital product data (VPD). (No VPD is displayed.)

Display Firmware Device Node Information

Note: This service aid runs on CHRP system units only.

This task displays the firmware device node information that appears on CHRP platforms. This service aid is intended to gather more information about individual or particular devices on the system. The format of the output data may differ depending on which level of the AIX operating system is installed.

Display Hardware Error Report

This service aid uses the **errpt** command to view the hardware error log.

The Display Error Summary and Display Error Detail selection provide the same type of report as the **errpt** command. The Display Error Analysis Summary and Display Error Analysis Detail selection provide additional analysis.

Display Hardware Vital Product Data

This service aid displays all installed resources, along with any VPD for those resources. Use this service aid when you want to look at the VPD for a specific resource.

Display Machine Check Error Log

Note: The Machine Check Error Log Service Aid is available only on Standalone Diagnostics.

When a machine check occurs, information is collected and logged in an NVRAM error log before the system unit shuts down. This information is logged in the AIX error log and cleared from NVRAM when the system is rebooted from the hard disk, LAN, or standalone media. When booting from Standalone Diagnostics, this service aid converts the logged information into a readable format that can be used to isolate the problem. When booting from the hard disk or LAN, the information can be viewed from the AIX error log using the Hardware Error Report Service Aid. In either case, the information is analyzed when the **sysplanar0** diagnostics are running in Problem Determination Mode.

Display Microcode Level

This task is used to display the microcode or firmware levels of currently installed resources. When the **sys0** resource is selected, the task displays the levels of both the system firmware and service processor firmware. **sys0** may not be available in all cases.

You can display the current level of the microcode on an adapter, the system, or a device by using the AIX **diag** command. See the following command syntax: `diag -c -d` *device* `-T "disp_mcode"`

Flag	Description
-c	No console mode.
-d	Used to specify a device.
-T	Use the disp_mcode option to display microcode.

The AIX **lsmcode** command serves as a command line interface to the ″Display Microcode Level″ task. For information on the **lsmcode** command, refer to the *AIX Commands Reference* manual.

Display or Change Bootlist

This service aid allows the bootlist to be displayed, altered, or erased.

The system attempts to perform an IPL from the first device in the list. If the device is not a valid IPL device or if the IPL fails, the system proceeds in turn to the other devices in the list to attempt an IPL.

Display or Change Diagnostic Run-Time Options

The Display or Change Diagnostic Run-Time Options task allows the diagnostic run-time options to be set.

Note: The run-time options are used only when selecting the Run Diagnostic task.

The run-time options are:

- Display Diagnostic Mode Selection Menus

  This option allows the user to turn on or off displaying the DIAGNOSTIC MODE SELECTION MENU (the default is on).
- Run Tests Multiple Times

  This option allows the user to turn on or off, or specify a loop count, for diagnostic loop mode (the default is off).

  Note: This option is only displayed when you run the Online Diagnostics in Service Mode.
- Include Advanced Diagnostics

  This option allows the user to turn on or off including the Advanced Diagnostics (the default is off).
- Include Error Log Analysis (not available in diagnostics 5.2.0 or later)

  This option allows the user to turn on or off including the Error Log Analysis (ELA) (the default is off).
- Include Error Log Analysis

  This option allows the user to turn on or off including the Error Log Analysis (ELA) (the default is off).
- Number of Days Used to Search Error Log

  This option allows the user to select the number of days for which to search the AIX error log for errors when running the Error Log Analysis. The default is seven days, but it can be changed from one to sixty days.
- Display Progress Indicators

  This option allows the user to turn on or off the progress indicators when running the Diagnostic Applications. The progress indicators are in a popup box at the bottom of the screen which indicate that the test being run (the default is on).
- Diagnostic Event Logging

  This option allows the user to turn on or off logging information to the Diagnostic Event Log (the default is on).
- Diagnostic Event Log File Size

  This option allows the user to select the maximum size of the Diagnostic Event Log. The default size for the Diagnostic Event Log is 100 KB. The size can be increased in 100 KB increments to a maximum of 1 MB.

Use the **diaggetrto** command to display one or more diagnostic run-time options. Use the following AIX command line syntax:

```
/usr/lpp/diagnostics/bin/diaggetrto [-a] [-d] [-l] [-m] [-n] [-p] [-s]
```

Use the **diagsetrto** command to change one or more diagnostic run-time options. Use the following AIX command line syntax:

```
/usr/lpp/diagnostics/bin/diagsetrto [-a on/off] [-d on/off] [-l size]
[-m on/off] [-n days] [-p on/off]
```

Flag descriptions for the **diaggetrto** and **diagsetrto** commands are as follows:

Flag	Description
-a	Displays or changes the value of the Include Advanced Diagnostics option.
-d	Displays or changes the value of the Diagnostic Event Logging option.
-l	Displays or changes the value of the Diagnostic Event Log File Size. Allowable size are between 100K and 1000K in increments of 100K. The size may never be decreased.
-m	Displays or changes the value of the Display Diagnostic Mode Selection Menu option.
-n	Displays or changes the value of the Number of Days Used To Search the Error Log option. Allowable values are between 1 and 60 days. 7 days is the default.
-p	Displays or changes the value of the Display Progress Indicators option.
-s	Displays all of the diagnostic run-time option.

Display Previous Diagnostic Results

Note: This service aid is not available when you load the diagnostics from a source other than a hard disk drive or a network.

This service aid allows a service representative to display results from a previous diagnostic session. When the Display Previous Diagnostic Results option is selected, the user can view up to 25 no trouble found (NTF) and service request number (SRN) results.

This service aid displays Diagnostic Event Log information. You can display the Diagnostic Event Log in a short version or a long version. The Diagnostic Event Log contains information about events logged by a diagnostic session.

This service aid displays the information in reverse chronological order. If more information is available than can be displayed on one screen, use the Page Down and Page Up keys to scroll through the information.

This information is not from the AIX operating system error log. This information is stored in the **/var/adm/ras** directory.

You can run the command from the AIX command line by typing: `/usr/lpp/diagnostics/bin/diagrpt [[-o] | [-s mmddyy] | [-a] | [-r]]`

Flag	Description
-o	Displays the last diagnostic results file stored in the **/etc/lpp/diagnostics/data** directory
-s *mmddyy*	Displays all diagnostic result files logged since the date specified
-a	Displays the long version of the Diagnostic Event Log
-r	Displays the short version of the Diagnostic Event Log

Display Resource Attributes

This task displays the Customized Device Attributes associated with a selected resource. This task is similar to running the **lsattr -E -l** *resource* command.

Display Service Hints

This service aid reads and displays the information in the CEREADME file from the diagnostics media. This file contains information that is not contained in the publications for this version of the diagnostics. The file also contains information about using this particular version of diagnostics.

Use the arrow keys to scroll through the information in the file.

Display Software Product Data

This task uses SMIT to display information about the installed software and provides the following functions:

- List Installed Software
- List Applied but Not Committed Software Updates
- Show Software Installation History
- Show Fix (APAR) Installation Status
- List Fileset Requisites
- List Fileset Dependents
- List Files Included in a Fileset
- List File Owner by Fileset

Display System Environmental Sensors

Note: This service aid runs on CHRP system units only.

This service aid displays the environmental sensors implemented on a CHRP system. The information displayed is the sensor name, physical location code, literal value of the sensor status, and the literal value of the sensor reading.

The sensor status can be any one of the following:

- **Normal** - The sensor reading is within the normal operating range.
- **Critical High** - The sensor reading indicates a serious problem with the device. Run diagnostics on sysplanar0 to determine what repair action is needed.
- **Critical Low** - The sensor reading indicates a serious problem with the device. Run diagnostics on sysplanar0 to determine what repair action is needed.
- **Warning High** - The sensor reading indicates a problem with the device. This could become a critical problem if action is not taken. Run diagnostics on sysplanar0 to determine what repair action is needed.
- **Warning Low** - The sensor reading indicates a problem with the device. This could become a critical problem if action is not taken. Run diagnostics on sysplanar0 to determine what repair action is needed.
- **Hardware Error** - The sensor could not be read because of a hardware error. Run diagnostics on sysplanar0 in problem-determination mode to determine what repair action is needed.
- **Hardware Busy** - The system has repeatedly returned a busy indication, and a reading is not available. Try the service aid again. If the problem continues, run diagnostics on sysplanar0 in problem-determination mode to determine what repair action is needed.

This service aid can also be run as a command. You can use the command to list the sensors and their values in a text format, list the sensors and their values in numerical format, or a specific sensor can be queried to return either the sensor status or sensor value.

Run the command by entering one of the following: `/usr/lpp/diagnostics/bin/uesensor -l | -a /usr/lpp/diagnostics/bin/uesensor -t` *token* `-i` *index* `[-v]`

Flag	Description
-l	List the sensors and their values in a text format.

-a List the sensors and their values in a numerical format. For each sensor, the following numerical values are displayed as: *token index status measured value location code*

-t token
Specifies the sensor token to query.

-i index
Specifies the sensor index to query.

-v Indicates to return the sensor measured value. The sensor status is returned by default.

Examples

The following are examples from this command:

1. Display a list of the environmental sensors: `/usr/lpp/diagnostics/bin/uesensor -l`

   ```
   Sensor = Fan Speed
   Status = Normal
   Value = 2436 RPM
   Location Code = F1
   Sensor = Power Supply
   Status = Normal
   Value = Present and operational
   Location Code = V1
   Sensor = Power Supply
   Status = Critical low
   Value = Present and not operational
   Location Code = V2
   ```

2. Display a list of the environmental sensors in a numerical list: `/usr/lpp/diagnostics/bin/uesensor -a`

   ```
   3 0 11 87 P1
   9001 0 11 2345 F1
   9004 0 11 2 V1
   9004 1 9 2 V2
   ```

3. Return the status of sensor 9004, index 1: `/usr/lpp/diagnostics/bin/uesensor -t 9004 -i 1`

   ```
   9
   ```

4. Return the value of sensor 9004, index 1: `/usr/lpp/diagnostics/bin/uesensor -t 9004 -i 1 -v`

   ```
   2
   ```

Display Test Patterns

This service aid provides a means of adjusting system display units by providing test patterns that can be displayed. The user works through a series of menus to select the display type and test pattern. After the selections are made, the test pattern displays.

Display USB Devices

The following are the main functions of this service aid:

- Display a list of USB controllers on an adapter.
- Display a list of USB devices that are connected to the selected controller.

To run the USB devices service aid, go to the diagnostics ″TASKS SELECTION″ menu, select ″*Display USB Devices*″. From the controller list that displayed on the screen, select one of the items that begins with ″OHCDX″, where ″X″ is a number. A list of devices attached to the controller displays.

Download Microcode

This service aid provides a way to copy microcode to an adapter or device. The service aid presents a list of adapters and devices that use microcode. After the adapter or device is selected, the service aid provides menus to guide you in checking the current level and downloading the needed microcode.

This task can be run directly from the AIX command line. See the following sections for instructions on downloading to a particular type adapter or device.

Download Microcode to PCI SCSI RAID Adapter

See the following command syntax for a PCI SCSI RAID Adapter:

```
diag -c -d RAIDadapterName -T "download [-B] [-D] [-P]"
```

Flag	Description
-B	Download boot block microcode (default to functional microcode)
-D	Microcode is on diskette (default to **/etc/microcode** directory)
-P	Download the previous level of microcode (default to latest level)

Download Microcode to a PCI-X Dual Channel Adapter

Microcode installation occurs while the adapter and attached drives are available for use. Before installation of the microcode, ensure that there is a current backup of the system available and it is recommended that the installation be scheduled during a non-peak production time period.

Notes:

1. If the source is **/etc/microcode**, the image must be stored in the **/etc/microcode** directory on the system. If the system is booted from a NIM server, the image must be stored in the **usr/lib/microcode** directory of the SPOT the client is booted from.
2. If the source is diskette, the diskette must be in a backup format and the image stored in the **/etc/microcode** directory.

See the following command syntax for a PCI-X Adapter:

```
diag -c -d device_name -T "download [-s {/etc/microcode|diskette}]
[-l {latest|previous}] [-f]"
```

Flag	Description
-c	No console mode. Run without user interaction.
-d	Device name is the name of the adapter.
-f	Force the installation even if the current level of microcode is not on the source.
-l	Level of microcode to install. The default is latest.
-s	Source of the new microcode image. The default is **/etc/microcode**.
-T	Use the download option to download microcode.

Download Microcode to Disk Drive Attached to a PCI SCSI RAID Adapter

See the following command syntax for a disk drive attached to a PCI SCSI RAID Adapter:

```
diag -c -d RAIDadapterName -T "download {-l chID | -A} [-D] [-P]"
```

Flag	Description
-A	All disk drives
-D	Microcode is on diskette (default to **/etc/microcode** directory)
-l	RAID disk drive-physical disk channel/ID (example 27)
-P	Download the previous level of microcode (default to latest level)

Download Microcode to a PCI FC-AL Fibre Channel Adapter

Microcode installation occurs while the adapter and attached drives are available for use. It is recommended that a current backup be available and the installation be scheduled during a non-peak production time period.

Note: If the source is diskette, the diskette must be in a backup format and the image stored in the **/etc/microcode** directory.

Microcode installation occurs while the adapter and attached drives are available for use. Before installation of the microcode, ensure that a current backup of the system is available. It is recommended that the installation be scheduled during a non-peak production time period.

Notes:

1. If the source is **/etc/microcode**, the image must be stored in the **/etc/microcode** directory on the system. If the system is booted from a NIM server, the image must be stored in the **usr/lib/microcode** directory of the SPOT the client is booted from.
2. If the source is diskette, the diskette must be in backup format and the image stored in the **/etc/microcode** directory.

Note: If the source is diskette, the diskette must be in backup format and the image stored in the **/etc/microcode** directory.

See the following command syntax for a PCI FC-AL Fibre Channel Adapter.

```
diag -c -d device_name -T "download [-s {/etc/microcode|diskette}] [-l {latest|previous}] [-f]"
```

Flag	Description
-c	No console mode. Run without user interaction.
-d	Device name is the name of the adapter.
-T	Use the download option to download microcode.
-s	Source of the new microcode image. Default is `/etc/microcode`.
-l	Level of microcode to install. The default is latest.
-f	Force the installation even if the current level of microcode is not on the source.

Download Microcode to DVD-RAM Attached to a PCI SCSI Adapter

See the following command syntax for a DVD-RAM attached to a PCI SCSI Adapter:

```
diag [-c] -d cdX -T "download [-s {/etc/microcode|diskette}]
[-l {latest|previous}] [-f]"
```

Flag	Description
-c	No console mode. Run without user interaction
cdX	Device selected, for example, cd0.
-s	Source of the new microcode. The default is **/etc/microcode**.
-l	Level of microcode image to be installed. The default is latest.
-f	Install the microcode on the device even if the current level is unavailable on the source.

Download Microcode to Disk Attached to PCI SCSI Adapter

See following command syntax for a disk drive attached to a PCI SCSI adapter:

```
 diag [-c] -d hdiskX -T "download [-s {/etc/microcode|diskette}]
[-l {latest|previous}] [-f]"
```

Flag	Description
-c	No console mode. Run without user interaction
-d *hdiskX*	Selected device, for example, hdisk0.
-T *download*	Download microcode task.

-s Source of the new microcode. The default is **/etc/microcode**.
-l Level of microcode image to be installed. The default is latest.
-f Install the microcode on the device even if the current level is unavailable on the source.

Download Microcode to Other Devices

See the following command syntax:

```
diag -c -d device_name -T "download [-s diskette] [-l previous] [-F]"
```

Flag	Description
-F	Force the download microcode even if the current level is unavailable on the source.
-l	Microcode level. The default is latest.
-s	Source of the new microcode. The default is **/etc/microcode**. Default source device is disk.

Fault Indicators

Note: Prior to Diagnostics version 5.1.0.35, this task was also known as the System Fault Indicator task.

This task is used to display or reset the Fault Indicators on the systems that support this function. This task may also be used to set the Fault Indicators for testing purposes, but the Indicators are not set back to normal when you exit this task.

The Fault Indicators are used to identify a fault with the system. These indicators may be set automatically by hardware, firmware, or diagnostics when a fault is detected in the system.

The Fault Indicators are turned off when a Log Repair Action is performed. After a serviceable event is complete, do a System Verification to verify the fix. Also do a Log Repair Action if the test on the resource was good, and that resource had an entry in the error log. If the serviceable event was not a result of an error log entry, use the Log Repair Action Task to turn off the system fault indicator.

For additional information concerning the use of these indicators, refer to the system guide.

Note: The AIX command does not allow you to set the fault indicators to the Fault state.

Use the following command syntax:

```
/usr/lpp/diagnostics/bin/usysfault [-s normal] [-l location code]
```

Flag	Description
-s *normal*	Sets the Fault Indicator to the normal state.
-l *location code*	Identifies the resource by physical location code.

When the command is used without the **-s** flag, the current state of the indicator is displayed as normal or attention.

When the command is used without the **-l** flag, the Primary Enclosure resource is used.

Use the **-l** flag only in systems that have more than one fault indicator.

Note: See also the “Identify and System Attention Indicators” on page 93. Some systems that do not support Fault Indicators have a similar System Attention Indicator.

Fibre Channel RAID Service Aids

The Fibre Channel RAID service aids contain the following functions:

Certify LUN
This selection reads and checks each block of data in the logical unit number (LUN). If excessive errors are encountered, the user is notified.

You can run this task from the AIX command line. Use the following fastpath command: `diag -T "certify"`

Certify Spare Physical Disk
This selection allows the user to certify (check integrity of the data) drives that are designated as spares.

You can run this task from the AIX command line. Use the following fastpath command: `diag -T "certify"`

Format Physical Disk
This selection is used to format a selected disk drive.

You can run this task from the AIX command line. Use the following fastpath command: `diag -T "format"`

Array Controller Microcode Download
This selection allows the microcode on the Fibre Channel RAID controller to be updated when required.

You can run this task from the AIX command line. Use the following fastpath command: `diag -T "download"`

Physical Disk Microcode Download
This selection is used to update the microcode on any of the disk drives in the array.

You can run this task from the AIX command line. Use the following fastpath command: `diag -T "download"`

Update EEPROM
This selection is used to update the contents of the electronically erasable programmable read-only memory (EEPROM) on a selected controller.

Replace Controller
Use this selection when it is necessary to replace a controller in the array.

Flash SK-NET FDDI Firmware

This task allows the Flash firmware on the SysKonnect SK-NET FDDI adapter to be updated.

Format Media

This task allows the selection of diskettes, hardfiles, or optical media to be formatted. Each selection is described below.

Hardfile Attached to SCSI Adapter (non-RAID)

- Hardfile Format

  Writes all of the disk. The pattern written on the disk is device-dependent; for example some drives may write all 0s, while some may write the hexadecimal number 5F. No bad block reassignment occurs
- Hardfile Format and Certify

  Performs the same function as Hardfile Format. After the format is completed, Certify is run. Certify then reassigns all bad blocks encountered.
- Hardfile Erase Disk

This option can be used to overwrite (remove) all data currently stored in user-accessible blocks of the disk. The **Erase Disk** option writes one or more patterns to the disk. An additional option allows data in a selectable block to be read and displayed on the system console.

To use the **Erase Disk** option, specify the number (0-3) of patterns to be written. The patterns are written serially; that is, the first pattern is written to all blocks. Then the next pattern is written to all blocks, overlaying the previous pattern. A random pattern is written by selecting the **Write Random Pattern?** option.

Note: The Erase Disk service aid has not been certified as meeting the Department of Defense or any other organization's security guidelines.

Use the following steps to overwrite the data on the drive:

1. Use the **Erase Disk** selection to overwrite the data on the drive.
2. Do a format without certify.
3. Run a second pass of the **Erase Disk** selection.

For a newly installed drive, you can ensure that all blocks on the drive are overwritten with your pattern if you use the following procedure:

1. Format the drive.
2. Check the defect MAP by running the **Erase Disk** selection.

   Note: If you use the **Format and Certify** option, there may be some blocks which get placed into the grown defect MAP.
3. If there are bad blocks in the defect MAP, record the information presented and ensure that this information is kept with the drive. This data is used later when the drive is to be overwritten.
4. Use the drive as you would normally.
5. When the drive is no longer needed and is to be erased, run the same version of the **Erase Disk** selection which was used in step 2.

   Note: Using the same version of the service aid is only critical if any bad blocks were found in step 3.
6. Compare the bad blocks which were recorded for the drive in step 3 with those that now appear in the grown defect MAP.

   Note: If there are differences between the saved data and the newly obtained data, then all sectors on this drive cannot be overwritten. The new bad blocks are not overwritten.
7. If the bad block list is the same, continue running the service aid to overwrite the disk with the chosen pattern(s).

This task can be run directly from the AIX command line. See the command syntax: `diag -c -d` *deviceName* `-T "format [-s* fmtcert | erase -a {read | write}] [-F]"`

Flag	Description
fmtcert	Formats and certifies the disk.
*	Available in no-console mode only.
-F	Force the disk erasure even if all blocks cannot be erased due to errors accessing grown defect map.

Note: The Erase Disk option in command line mode uses default values. To selectively read or write, use the **diag** command in console mode.

Hardfile Attached to PCI SCSI RAID Adapter

This function formats the physical disks attached to a PCI SCSI RAID adapter. This task can be run directly from the AIX command line. See the following command syntax: `diag -c -d` *RAIDadapterName* `-T "format {-l` *chId* `| -A }"`

Flag	Description
-l	Physical disk channel/ID (An example of a physical disk channel/ID is 27, where the channel is 2 and the ID is 7.)
-A	All disks

Optical Media

Use the following functions to check and verify optical media:

- Optical Media Initialize

  Formats the media without certifying. This function does not reassign the defective blocks or erase the data on the media. This option provides a quick way of formatting the media and cleaning the disk.

  Note: It takes approximately one minute to format the media.
- Optical Media Format and Certify

  Formats and certifies the media. This function reassigns the defective blocks and erases all data on the media.

This task can be run directly from the AIX command line. See the following command syntax: `diag -c -d` *deviceName* `-T "format [-s {initialize | fmtcert} ]"`

Option	Description
initialize	Formats media without certifying
fmtcert	Formats and certifies the media

Diskette Format

This selection formats a diskette by writing patterns to it.

Gather System Information

This service aid uses the AIX snap command to collect configuration information on networks, filesystems, security, the kernel, the ODM, and other system components. You can also choose to collect SSA adapter and disk drive configuration data, or AIX trace information for software debugging.

The output of the SNAP service aid can be used by field service personnel or it can be put on removable media and transferred to remote locations for more extensive analysis.

To use the SNAP task, select Gather System Information from the task list. You can select which components you want to collect information for, and where to store the data (hard disk or removable media).

Generic Microcode Download

The Generic Microcode Download service aid provides a means of executing a genucode script from a diskette or tape. The purpose of this generic script is to load microcode to a supported resource.

The genucode program should be downloaded onto diskette or tape in **tar** format while the microcode image itself goes onto another one in **restore** format. Running the Generic Microcode Download task will

search for the genucode script on diskette or tape and execute it. It will ask for a Genucode media to be inserted into the drive. The service aid moves the genucode script file to the **/tmp** directory and runs the program that downloads the microcode to the adapter or device.

This service aid is supported in both concurrent and standalone modes from disk, LAN, or loadable media.

Hot Plug Task

The Hot Plug Task provides software function for those devices that support hot-plug or hot-swap capability. This includes PCI adapters, SCSI devices, and some RAID devices. This task was previously known as ″SCSI Device Identification and Removal″ or ″Identify and Remove Resource.″

The Hot Plug Task has a restriction when running in Standalone or Online Service mode; new devices may not be added to the system unless there is already a device with the same FRU part number installed in the system. This restriction is in place because the device software package for the new device cannot be installed in Standalone or Online Service mode.

Depending on the environment and the software packages installed, selecting this task displays the following three subtasks:
- PCI Hot Plug Manager
- SCSI Hot Swap Manager
- RAID Hot Plug Devices

To run the Hot Plug Task directly from the command line, type the following: `diag -T"identifyRemove"`

If you are running the diagnostics in Online Concurrent mode, run the Missing Options Resolution Procedure immediately after removing any device.

If the Missing Options Resolution Procedure runs with no menus or prompts, then device configuration is complete. Otherwise, work through the missing options menu to complete device configuration (in diagnostics prior to version 5.2.0) or (in diagnostics version 5.2.0 and later) select the device that has an uppercase `M` shown in front of it in the resource list for missing options processing to be done on that resource.

PCI Hot Plug Manager

The PCI Hot Plug Manager task is a SMIT menu that allows you to identify, add, remove, or replace PCI adapters that are hot-pluggable. The following functions are available under this task:
- List PCI Hot Plug Slots
- Add a PCI Hot Plug Adapter
- Replace/Remove a PCI Hot Plug Adapter
- Identify a PCI Hot Plug Slot
- Unconfigure Devices
- Configure Devices
- Install/Configure Devices Added After IPL

The **List PCI Hot Plug Slots** function lists all PCI hot-plug slots. Empty slots and populated slots are listed. Populated slot information includes the connected logical device. The slot name consists of the physical location code and the description of the physical characteristics for the slot.

The **Add a PCI Hot Plug Adapter** function is used to prepare a slot for the addition of a new adapter. The function lists all the empty slots that support hot plug. When a slot is selected, the visual indicator for the slot blinks at the Identify rate. After the slot location is confirmed, the visual indicator for the specified PCI slot is set to the Action state. This means the power for the PCI slot is off and the new adapter can be plugged in.

The **Replace/Remove a PCI Hot Plug Adapter** function is used to prepare a slot for adapter exchange. The function lists all the PCI slots that support hot plug and are occupied. The list includes the slot's physical location code and the device name of the resource installed in the slot. The adapter must be in the Defined state before it can be prepared for hot-plug removal. When a slot is selected, the visual indicator for the slot is set to the Identify state. After the slot location is confirmed, the visual indicator for the specified PCI slot is set to the Action state. This means the power for the PCI slot, is off and the adapter can be removed or replaced.

The **Identify a PCI Hot Plug Slot** function is used to help identify the location of a PCI hot-plug adapter. The function lists all the PCI slots that are occupied or empty and support hot plug. When a slot is selected for identification, the visual indicator for the slot is set to the Identify state.

The **Unconfigure Devices** function attempts to put the selected device, in the PCI hot-plug slot, into the Defined state. This action must be done before any attempted hot-plug function. If the unconfigure function fails, it is possible that the device is still in use by another application. In this case, the customer or system administrator must be notified to quiesce the device.

The **Configure Devices** function allows a newly added adapter to be configured into the system for use. This function should also be done when a new adapter is added to the system.

The **Install/Configure Devices Added After IPL** function attempts to install the necessary software packages for any newly added devices. The software installation media or packages are required for this function.

Standalone Diagnostics has restrictions on using the PCI Hot-Plug Manager. For example:

- Adapters that are replaced must be exactly the same FRU part number as the adapter being replaced.
- New adapters cannot be added unless a device of the same FRU part number already exists in the system, because the configuration information for the new adapter is not known after the Standalone Diagnostics are booted.
- The following functions are not available from the Standalone Diagnostics and will not display in the list:
  - Add a PCI Hot Plug Adapter
  - Configure Devices
  - Install/Configure Devices Added After IPL

You can run this task directly from the command line by typing the following command: `diag -d` *device* `-T"identifyRemove"`

However, note that some devices support both the PCI Hot-Plug task and the RAID Hot-Plug Devices task. If this is the case for the *device* specified, then the Hot Plug Task displays instead of the PCI Hot Plug Manager menu.

More detailed information concerning PCI Hot-Plug Manager can be found in the *AIX System Management Guide: Operating System and Devices*.

SCSI Hot Swap Manager

This task was known as ″SCSI Device Identification and Removal″ or ″Identify and Remove Resources″ in previous releases. This task allows the user to identify, add, remove, and replace a SCSI device in a system unit that uses a SCSI Enclosure Services (SES) device. The following functions are available:

- List the SES Devices
- Identify a Device Attached to an SES Device
- Attach a Device to an SES Device
- Replace/Remove a Device Attached to an SES Device
- Configure Added/Replaced Devices

The **List the SES Devices** function lists all the SCSI hot-swap slots and their contents. Status information about each slot is also available. The status information available includes the slot number, device name, whether the slot is populated and configured, and location.

The **Identify a Device Attached to an SES Device** function is used to help identify the location of a device attached to a SES device. This function lists all the slots that support hot swap that are occupied or empty. When a slot is selected for identification, the visual indicator for the slot is set to the Identify state.

The **Attach a Device to an SES Device** function lists all empty hot-swap slots that are available for the insertion of a new device. After a slot is selected, the power is removed. If available, the visual indicator for the selected slot is set to the Remove state. After the device is added, the visual indicator for the selected slot is set to the Normal state, and power is restored.

The **Replace/Remove a Device Attached to an SES Device** function lists all populated hot-swap slots that are available for removal or replacement of the devices. After a slot is selected, the device populating that slot is Unconfigured; then the power is removed from that slot. If the Unconfigure operation fails, it is possible that the device is in use by another application. In this case, the customer or system administrator must be notified to quiesce the device. If the Unconfigure operation is successful, the visual indicator for the selected slot is set to the Remove state. After the device is removed or replaced, the visual indicator, if available for the selected slot, is set to the Normal state, and power is restored.

Note: Be sure that no other host is using the device before you remove it.

The **Configure Added/Replaced Devices** function runs the configuration manager on the parent adapters that had child devices added or removed. This function ensures that the devices in the configuration database are configured correctly.

Standalone Diagnostics has restrictions on using the SCSI Hot Plug Manager. For example:
- Devices being used as replacement devices must be exactly the same type of device as the device being replaced.
- New devices may not be added unless a device of the same FRU part number already exists in the system, because the configuration information for the new device is not known after the Standalone Diagnostics are booted.

You can run this task directly from the command line. See the following command syntax:

```
diag -d device-T"identifyRemove"
OR
diag [-c] -d device -T"identifyRemove -a [identify|remove]"
```

Flag	Description
-a	Specifies the option under the task.
-c	Run the task without displaying menus. Only command line prompts are used. This flag is only applicable when running an option such as identify or remove.
-d	Indicates the SCSI device.
-T	Specifies the task to run.

RAID Hot Plug Devices

This selection starts the PCI SCSI-2 F/W RAID Adapter Service Aid.

Identify Indicators

See “Identify and System Attention Indicators” on page 93 for a description of the Identify Indicators task.

Identify and System Attention Indicators

Note: Prior to Diagnostics version 5.1.0.35, this task may also have been known as the System Identify Indicator or Identify Indicators task.

This task is used to display or set the Identify Indicators and the single system attention indicator on the systems that support this function.

Some systems may support the Identify Indicators or the Attention Indicators. The Identify Indicator is used to help physically identify the system in a large equipment room. The Attention Indicator is used to help physically identify a system with a fault in a large equipment room.

When a fault has been detected on a system that supports the Attention Indicator, the Indicator is set to an Attention condition. After the failing system has been identified and the problem fixed, the Attention Indicator changes back to normal. This should be done by the Log Repair Action.

Note: It is important to run the Log Repair Action task. This action keeps the Fault Indicator from reverting to the Fault state due to a previous error in the error log that has already been serviced.

For additional information concerning the use of this indicator, refer to the system guide.

This task can also be run directly from the command line by typing

`/usr/lpp/diagnostics/bin/usysident [-s {normal | identify}] [-l location code]`

Flag	Description
-s {**normal** | **identify**}	Sets the state of the System Identify Indicator to either normal or identify.
-l *location code*	Identifies the resource by physical location code.

When this command is used without the **-l** flag, the Primary Enclosure resource is used.

Use the **-l** flag only in systems that have more than one Identify and System attention indicator.

When this command is used without **-s** flag, the current state of the identify indicator is displayed.

Local Area Network Analyzer

This selection is used to exercise the LAN communications adapters (Token-Ring, Ethernet, and (FDDI) Fibre Distributed Data Interface). The following services are available:

- Connectivity testing between two network stations. Data is transferred between the two stations, requiring the user to provide the Internet addresses of both stations.
- Monitoring ring (Token-Ring only). The ring is monitored for a specified period of time. Soft and hard errors are analyzed.

Log Repair Action

The Log Repair Action task logs a repair action in the AIX Error Log. A Repair Action log indicates that a FRU has been replaced, and error log analysis should not be done for any errors logged before the repair action. The Log Repair Action task lists all resources. Replaced resources can be selected from the list, and when **commit** (F7 key) is selected, a repair action is logged for each selected resource.

Periodic Diagnostics

This selection provides a tool for configuring periodic diagnostics and automatic error log analysis. You can select a hardware resource to be tested once a day, at a user-specified time.

Hardware errors logged against a resource can also be monitored by enabling automatic error log analysis. This allows error log analysis to be performed every time a hardware error is put into the error log. If a problem is detected, a message is posted to the system console and either sent to the Service Focal Point when there is an attached HMC, or a mail message to the users belonging to the system group containing information about the failure, such as the service request number.

The service aid provides the following functions:

- Add or delete a resource to the periodic test list
- Modify the time to test a resource
- Display the periodic test list
- Modify the error notification mailing list
- Disable or enable automatic error log analysis

PCI RAID Physical Disk Identify

This selection identifies physical disks connected to a PCI SCSI-2 F/W RAID adapter.

You can run this task directly from the AIX command line. See the following command syntax: `diag -c -d` *pci RAID adapter* `-T identify`

Process Supplemental Media

Diagnostic Supplemental Media contains all the necessary diagnostic programs and files required to test a particular resource. The supplemental media is normally released and shipped with the resource as indicated on the diskette label. Diagnostic Supplemental Media must be used when the device support has not been incorporated into the latest diagnostic CD-ROM.

This task processes the Diagnostic Supplemental Media. Insert the supplemental media when you are prompted; then press Enter. After processing has completed, go to the Resource Selection list to find the resource to test.

Notes:

1. This task is supported in Standalone Diagnostics only.
2. Process and test one resource at a time. Run diagnostics after each supplemental media is processed. (for example; If you need to process two supplemental media you need to run diagnostic twice. Once after each supplement media is processed.)

Run Diagnostics

The Run Diagnostics task invokes the Resource Selection List menu. When the commit key is pressed, diagnostics are run on all selected resources.

The procedures for running the diagnostics depends on the state of the diagnostics run-time options. See “Display or Change Diagnostic Run-Time Options” on page 80.

Run Error Log Analysis

The Run Error Log Analysis task invokes the Resource Selection List menu. When the commit key is pressed, Error Log Analysis is run on all selected resources.

Run Exercisers

The Run Exercisers task provides a tool to troubleshoot intermittent system problems in AIX 4.3.2 or later, to test hardware, and to verify replacement parts. When AIX error logging is enabled, the Run Error Log Analysis task can be used to analyze errors after the exerciser completes. Hardware errors are logged in the AIX Error Log. Miscompares and recoverable errors are not reported. However, they may be logged in the AIX Error Log when logging thresholds are exceeded.

The diagnostic supervisor typically sets up temporary work files in **/tmp** to log messages and device statistics. These files are deleted before an exerciser session begins. In addition to individual exerciser requirements, the following requirements pertain to all exercisers:

- Only supported on CHRP platforms
- Only supported in concurrent or service modes
- Not supported from standalone diagnostics
- System performance will be degraded while running the exerciser, so it is recommended that customer applications be shut down before it is run.
- At least 1 MB of free storage in **/tmp** is available

From the TASK SELECTION LIST menu, select **Run Exercisers**. The RESOURCES SELECTION LIST menu displays. From this menu, choose the resources you want to exercise, and then select **commit** to start the **Run Exerciser** task. An intermediate pop-up window might display, stating system performance will be degraded. (The pop-up window does not display if the task had previously been selected). Press Enter and the EXERCISER OPTIONS menu prompts for the type of test to run.

The EXERCISER OPTIONS menu displays two options:

- **Option 1 - Short Exercise**. This option exercises the resources within a relatively short time and exits.
- **Option 2 - Extended Exercise**. This option allows greater flexibility and control over resources and test duration.

After choosing the **Short Exercise** option, additional menus, pop-up windows and prompts may display for each resource. Read any text and carefully complete any prompts before committing. The exercisers start, and the **Device Status Screen** displays. The exercisers runs 5 to 10 minutes depending on the number of processors, processor speed, memory size, and I/O configuration.

After choosing the **Extended Exercise** option, additional menus, pop-up windows and prompts may display for each resource. Read any text and carefully complete any prompts before committing. The **System Exerciser Main Menu** displays. From this menu, the exercisers can be activated through:

- Option 1 - Short Exercise
- Option 2 - Extended Exercise
- Option x (where exercisers are exited)

See the help text for information on how to use other available options.

When the task completes any errors that were encountered are displayed for review. Finally, an **Exerciser Complete** pop-up window displays.

To continue, press Enter. The TASK SELECTION LIST menu is displayed.

If miscompare errors were encountered, run diagnostics on the resource. If the problem is not reported, contact your service support structure. If any other errors were encountered, select and run the Error Log Analysis task. If Error Log Analysis does not report a problem, contact your service support structure.

Exerciser Commands (CMD)

Use the following commands as needed in the exerciser menus and reports. Not all commands are available in each menu or report.

CMD	Description
a	Acknowledge an error
b	Back one page
c	Toggle between cycle count and last error
e	View the AIX error log
f	Page forward one page
q	Return to Main Menu
r	Refresh screen
s	Enable or disable beep on error
x	Exit system exerciser

Abbreviations

The following list describes abbreviations used in the exerciser reports.

Abbreviation	Description
COE	Continue on error (use number to select).
CP	Device has run the specified number of cycles and is not running.
DD	The exerciser has been terminated by a signal.
ER	Device has stopped with an error.
HG	The device is hung.
HOE	Halt on error (use number to select).
RN	Device is running.
ST	Device is stopped.

Memory Exerciser

The memory exercisers are labeled `mem`*x*, where *x* is a number for the exerciser. Multiple exercisers can be active.

The memory exerciser requests as many memory buffers as possible from AIX. The exerciser then fills the memory buffers with specified bit patterns, then reads and compares the memory buffers to the specified bit patterns.

The memory exerciser is labeled `mem0`. The exerciser requests as many memory buffers as possible from AIX. The exerciser fills these buffers with specified bit patterns and then compares them to the original bit patterns. If memory is removed as a result of Dynamic Reconfiguration, the exerciser terminates.

On systems with multiple processors, a process is started for each processor. The free memory space is split evenly between the available processors, thus reducing the time required to exercise all of the memory.

Running this service aid requires 128 KB of free space in the **/etc/lpp/diagnostics/data** file.

Tape Exerciser

The tape exerciser is labeled `rmt`*x*, where *x* is the number of a specific device. The exerciser performs read, write, and compare operations using known data patterns. A tape device and Test Diagnostic Cartridge are required to run this exerciser. The actual Test Diagnostics Cartridge depends upon the specific tape device being tested. The exerciser automatically rewinds the tape. Test Requirements are:

- Tape device
- Test Diagnostic Cartridge; (part number depends upon tape device)

Diskette Exerciser

The diskette exerciser is labeled `fd`*x*, where *x* is the number of a specific device. The exerciser performs read, write, and compare operations using known data patterns. A scratch diskette is required to run this exerciser, data on the scratch diskette is destroyed. Test requirements are:

- Diskette device
- Scratch diskette (data on diskette is destroyed)

CD-ROM Exerciser

The CD-ROM exerciser is labeled `cd`*x*, where *x* is the number of a specific device. The exerciser performs read and compare operations using known data patterns. A CD-ROM device and a Test Disc is required to run this exerciser. Test requirements are:

- CD-ROM device
- Test Disc (part number 81F8902)

Floating Point Exerciser

The floating point exerciser is labeled `procx`, where x is the number of the processor containing the floating point unit. The exerciser performs load/store and arithmetic operations using floating point registers and instructions. The floating point instructions are executed using static values and the outcome of the operation is compared with the expected result. Any mismatch results in an error condition. If the processor is in use by the exerciser and is removed as a result of dynamic logical partitioning, the exerciser terminates.

SCSI Bus Analyzer

This service aid allows you to diagnose a SCSI bus problem in a freelance mode.

To use this service aid, the user should understand how a SCSI bus works. Use this service aid when the diagnostics cannot communicate with anything on the SCSI bus and cannot isolate the problem. Normally the procedure for finding a problem on the SCSI bus with this service aid is to start with a single device attached, ensure that it is working correctly, then start adding additional devices and cables to the bus, ensuring that each one works correctly. This service aid works with any valid SCSI bus configuration.

The SCSI Bus Service Aid transmits a SCSI Inquiry command to a selectable SCSI Address. The service aid then waits for a response. If no response is received within a defined amount of time, the service aid displays a timeout message. If an error occurs or a response is received, the service aid then displays one of the following messages:

- `The service aid transmitted a SCSI Inquiry Command and received a valid response back without any errors being detected.`
- `The service aid transmitted a SCSI Inquiry Command and did not receive any response or error status back.`
- `The service aid transmitted a SCSI Inquiry Command and the adapter indicated a SCSI bus error.`
- `The service aid transmitted a SCSI Inquiry Command and an adapter error occurred.`
- `The service aid transmitted a SCSI Inquiry Command and a check condition occur.`

When the SCSI Bus Service Aid is started, a description of the service aid displays.

Pressing the Enter key displays the Adapter Selection menu. Use this menu to enter the address to transmit the SCSI Inquiry Command.

When the adapter is selected, the SCSI Bus Address Selection menu displays. Use this menu to enter the address to transmit the SCSI Inquiry Command.

After the address is selected, the SCSI Bus Test Run menu displays. Use this menu to transmit the SCSI Inquiry Command by pressing Enter. The service aid then indicates the status of the transmission. When the transmission is completed, the results of the transmission displays.

Notes:

1. A Check Condition can be returned when the bus or device is working correctly.
2. AIX does not allow the command to be sent if the device is in use by another process.

SCSD Tape Drive Service Aid

This service aid allows you to obtain the status or maintenance information from a SCSD tape drive. Not all models of SCSD tape drive are supported.

The service aid provides the following options:

- Display time since a tape drive was last cleaned. The time since the drive was last cleaned displays on the screen, as well as a message regarding whether the drive is recommended to be cleaned.
- Copy a tape drive's trace table. The trace table of the tape drive is written to diskettes or a file. The diskettes must be formatted for DOS. Writing the trace table may require several diskettes. The actual number of diskettes is determined by the size of the trace table. Label the diskettes as follows:

  TRACE*x*.DAT (where *x* is a sequential diskette number). The complete trace table consists of the sequential concatenation of all the diskette data files.

  When the trace table is written to a disk file, the service aid prompts for a file name. The default name is: **/tmp/TRACE.***x*, where *x* is the AIX name of the SCSD tape drive being tested.
- Display or copy a tape drive's log sense information. The service aid provides options to display the log sense information to the screen, to copy it to a DOS formatted diskette, or to copy it to a file. The file name **LOGSENSE.DAT** is used when the log sense data is written to the diskette. The service aid prompts for a file name when you have selected that the log sense data is to be copied to a file.

This service aid can be run directly from the AIX command line. See the following command syntax (path is **/usr/lpp/diagnostics/bin/utape**):

```
utape [-h | -?] [-d device] [-n | -l | -t]
OR
utape -c -d device [-v] {-n | {-l | -t} { -D | -f [ filename]}}
```

Flag	Description
-c	Run the service aid without displaying menus. The return code indicates success or failure. The output is suppressed except for the usage statement and the numeric value for hours since cleaning (if **-n** and **-D** flags are used).
-D	Copy data to diskette.
-f	Copy data to the file name given after this flag or to a default file name if no name is specified.
-h, -?	Display a usage statement and/or return code. If the **-c** flag is present, only the return code displays to indicate the service aid did not run. If the **-c** is not used, a usage statement displays and the service aid exits.
-l	Display or copy log sense information.
-n	Display time since drive was last cleaned.
-t	Copy trace table.
-v	Verbose mode. If the **-c** flag is present, the information displays on the screen. If the **-n** flag is present, the information about tape-head cleaning is printed.

Spare Sector Availability

This selection checks the number of spare sectors available on the optical disk. The spare sectors are used to reassign when defective sectors are encountered during normal usage or during a format and certify operation. Low availability of spare sectors indicates that the disk needs to be backed up and replaced. Formatting the disk does not improve the availability of spare sectors.

You can run this task directly from the AIX command line. See the following command syntax: `diag -c -d` *deviceName* `-T chkspares`

SSA Service Aid

This service aid provides tools for diagnosing and resolving problems on SSA-attached devices. The following tools are provided:

- Set Service Mode
- Link Verification
- Configuration Verification
- Format and Certify Disk

System Fault Indicator

For a description of the System Fault Indicator task, see “Fault Indicators” on page 86.

System Identify Indicator

For a description of the System Identify Indicator task, see “Identify and System Attention Indicators” on page 93.

Update Disk-Based Diagnostics

This service aid allows fixes (APARs) to be applied.

This task invokes the SMIT Update Software by Fix (APAR) task. The task allows the input device and APARs to be selected. You can install any APAR using this task.

Update System or Service Processor Flash

Attention: If the system is running on a logically partitioned system, ask the customer or system administrator if a service partition has been designated.

- If it has, ask the customer or system administrator to shut down all of the partitions except the one with service authority. The firmware update can then be done using the service aid or the AIX command line in that partition.
- If a service partition has not been designated, the system must be shut down. If the firmware update image is available on backup diskettes, the firmware update can then be done from the service processor menus as a privileged user. If the firmware update image is in a file on the system, reboot the system in a full machine partition and use the following normal firmware update procedures.

If the system is already in a full machine partition, use the following normal firmware update procedures:

Note: This service aid runs on CHRP system units only.

This selection updates the system or service processor flash for CHRP system units. Some systems may have separate images for system and service processor firmware; newer systems have a combined image that contains both in one image.

Look for additional update and recovery instructions with the update kit. You must know the fully qualified path and file name of the flash update image file provided in the kit. If the update image file is on a diskette, the service aid can list the files on the diskette for selection. The diskette must be a valid backup format diskette.

To determine the current level of the system unit or service processor flash memory, refer to the update instructions with the kit, or the service guide for the system unit.

When this service aid is run from online diagnostics, the flash update image file is copied to the **/var** file system. It is recommended that the source of the microcode that you want to download be put into the **/etc/microcode** directory on the system. If there is not enough space in the **/var** file system for the new flash update image file, an error is reported. If this error occurs, exit the service aid, increase the size of the **/var** file system, and retry the service aid. After the file is copied, a screen requests confirmation before continuing with the flash update. When you continue the update flash, the system reboots using the **shutdown -u** command. The system does not return to the diagnostics, and the current flash image is not saved. After the reboot, you can remove the **/var/update_flash_image** file.

When this service aid is run from standalone diagnostics, the flash update image file is copied to the file system from diskette or from the NIM server. Using a diskette, the user must provide the image on backup format diskette because the user does not have access to remote file systems or any other files that are on the system. If using the NIM server, the microcode image must first be copied onto the NIM server in the **/usr/lib/microcode** directory pointed to the NIM SPOT (from which you plan to have the NIM client boot standalone diagnostics) prior to performing the NIM boot of diagnostics. Next, a NIM check operation must be run on the SPOT containing the microcode image on the NIM server. After performing the NIM boot of diagnostics, you can use this service aid to update the microcode from the NIM server by choosing the **/usr/lib/microcode** directory when prompted for the source of the microcode that you want to update. If not enough space is available, an error is reported, stating that additional system memory is needed. After the file is copied, a screen requests confirmation before continuing with the flash update. When you continue with the update, the system reboots using the **reboot -u** command. If you receive a `Caution: some process(es) wouldn't die` message during the reboot process, you can ignore this message. The current flash image is not saved.

You can use the **update_flash** command in place of this service aid. The command is located in the **/usr/lpp/diagnostics/bin** directory. The command syntax is as follows:

```
update_flash [-q] -f file_name
update_flash [-q] -D device_name -f file_name
update_flash [-q] -D update_flash [-q] -D device_name -l
```

Flag	Description
-D	Specifies that the flash update image file is on diskette. The *device_name* variable specifies the diskette drive. The default *device_name* is `/dev/fd0`.
-f	Flash update image file source. The *file_name* variable specifies the fully qualified path of the flash update image file.
-l	Lists the files on a diskette, from which the user can choose a flash update image file.
-q	Forces the **update_flash** command to update the flash EPROM and reboot the system without asking for confirmation.

Attention: The **update_flash** command reboots the entire system. Do not use this command if more than one user is logged on to the system.

7135 RAIDiant Array Service Aid

The 7135 RAIDiant Array service aids contain the following functions:

- Certify LUN

  Reads and checks each block of data in the logical unit number (LUN). If excessive errors are encountered, the user is notified.
- Certify Spare Physical Disk

  Allows the user to certify (check the integrity of the data) on drives designated as spares.
- Format Physical Disk

  Formats a selected disk drive.
- Array Controller Microcode Download

  Allows the microcode on the 7135 controller to be updated when required.
- Physical Disk Microcode Download

  Updates the microcode on any of the disk drives in the array.
- Update EEPROM

  Updates the contents of the EEPROM on a selected controller.
- Replace Controller

  Replaces a controller in the array.

Command Examples

Use this command syntax to download the adapter microcode:
`diag -c -d` *deviceName* `-T "download [-B][-D][-P]"`

Flag	Description
-B	Download boot block microcode (default to functional microcode)
-D	Microcode is on diskette (default to **/etc/microcode** directory)
-P	Download the previous level of microcode (default to latest level)

Use this command syntax to download physical disk microcode:
`diag -c -d` *deviceName* `-T "download -l` *ChId* `[-D][-P]"`

Flag	Description
-D	Microcode is on diskette (default to /etc/microcode directory)
-I	Physical disk channel/ID (for example, 27)
-P	Download the previous level of microcode (default to latest level)

Use this command syntax to format a physical disk:
`diag -c -d` *deviceName* `-T "format -l` *ChId*`"`

Flag	Description
-I	Physical disk channel/ID (for example, 27)

Use this command syntax to certify a physical disk:
`diag -c -d` *deviceName* `-T "certify -l` *ChId*`"`

Flag	Description
-I	Physical disk channel/ID (for example, 23)

Use this command syntax to identify a physical disk:
`diag -c -d` *deviceName* `-T "identify"`

7318 Serial Communications Network Server Service Aid

This service aid provides a tool for diagnosing terminal server problems.

Chapter 8. Verifying Hardware Operation

Use the system verification procedure discussed in this chapter to check the system for correct hardware operation.

Considerations Before Running This Procedure

Read the following before verifying hardware operation:

- The AIX operating system must be installed on your system before you attempt to perform this procedure.
- If this system unit is directly attached to another system unit or attached to a network, be sure communications with the other systems are stopped.
- This procedure requires use of all of the system resources. No other activity can be running on the system while you are performing this procedure.
- This procedure requires a Hardware Management Console for pSeries (HMC) attached to the HMC port on the processor subsystem.
- This procedure runs the AIX online diagnostics in service mode on a system booted in Full System Partition mode.

Does the system have AIX diagnostics preinstalled?

YES Go to "Loading the Online Diagnostics in Service Mode".

NO Go to "Running Standalone Diagnostics from a Network Installation Management (NIM) Server" on page 104.

Loading the Online Diagnostics in Service Mode

To run the online diagnostics in service mode from the boot hard disk, do the following:

1. From the HMC, select **Partition Management**.

   For more information on full system partitions, refer to the *IBM Hardware Management Console for pSeries Installation and Operations Guide*.
2. Select the desired system in the Contents area, right-click on the mouse, and select **Open Terminal Window**.
3. From the Service Processor menu on the VTERM, select Option 2 **System Power Control**.
4. Select option 6. Verify that the state changes to `currently disabled`. Disabling fast system boot automatically enables slow boot.
5. Select Option 98 to exit the system power control menu.
6. Use the HMC to power on the managed system in Full System Partition mode by selecting the managed system in the Contents area.
7. Highlight the system by right-clicking or selecting the desired system in the Contents area. On the menu, choose **Selected**.
8. Select **Power On**.
9. Select the **Power on Diagnostics Stored Boot List** option.
10. Ensure that there are no removable media in externally-attached SCSI devices.
11. Enter any passwords, if requested.

Note: If you are unable to load the diagnostics to the point when the `DIAGNOSTIC OPERATING INSTRUCTIONS` display, go to "Running Standalone Diagnostics from a Network Installation Management (NIM) Server" on page 104.

Running Standalone Diagnostics from a Network Installation Management (NIM) Server

A client system connected to a network with a network installation management (NIM) server is capable of booting standalone diagnostics from the NIM server if the client system is registered on the NIM server and the NIM boot settings on both the server and client are correct.

Notes:

1. All operations to configure the NIM server require root access.
2. If you replace the network adapter in the client, the network adapter hardware address for the client must be updated on the NIM server.
3. The Control State (Cstate) for standalone clients on the NIM server should be kept in the `diagnostic boot has been enabled` state.
4. On the client partition, the NIM server network adapter can be put in the bootlist after the boot hardfile. This allows the system to boot in standalone diagnostics from the NIM server, if there is a problem booting from the hardfile. Another option is to use the **Select Boot Options** function in the SMS menu to set up the network adapter that is connected to the NIM server for a one-time boot of standalone diagnostics.

NIM Server Configuration

Refer to the ″Advanced NIM Configuration Tasks″ chapter of the *AIX Installation Guide and Reference* for information on doing the following:

- Register a client on the NIM server.
- Enable a client to run diagnostics from the NIM server.

To verify that the client system is registered on the NIM server and diagnostic boot is enabled, do the following:

1. Run the command `lsnim -a Cstate -Z ClientName` from the command line on the NIM server.

   Note: The ClientName is the name of the system you want to run standalone diagnostics on.
2. Refer to the following table for system responses.

System Response	Client Status
#name:Cstate: ClientName: diagnostic boot has been enabled:	The client system is registered on the NIM server and enabled to run diagnostics from the NIM server.
#name:Cstate: ClientName:ready for a NIM operation: or #name:Cstate: ClientName:BOS installation has been enabled:	The client system is registered on the NIM server but not enabled to run diagnostics from the NIM server. **Note:** If the client system is registered on the NIM server but **Cstate** has not been set, no data will be returned.
0042-053 lsnim: there is no NIM object named ″ClientName″	The client is not registered on the NIM server.

Client Configuration and Booting Standalone Diagnostics from the NIM Server

To run standalone diagnostics on a client from the NIM server, do the following:

1. Stop all programs including the AIX operating system (get help if needed).

2. Ensure that the system power is off.
3. Turn the power on to the system unit.
4. When the keyboard indicator is displayed (the word **keyboard** on the HMC or the **keyboard** icon on a graphical display), press the number 1 key on the keyboard to display the SMS menu.
5. Enter any requested passwords.
6. Select **Utilities**.
7. Select **Setup Remote IPL (Initial Program Load)**.
8. Enter the client address, server address, gateway address (if applicable) and subnet mask. Exit to the Network Parameters screen.
9. If the NIM server is set up to allow pinging from the client system, use the **ping** utility in the RIPL utility to verify that the client system can ping the NIM server. Under the ping utility, choose the network adapter that provides the attachment to the NIM server to do the ping operation. If ping returns with an `OK` message, the client is prepared to boot from the NIM server. If **ping** returns with a FAILED prompt, the client does not proceed with the NIM boot.

   Note: If the **ping** fails, refer to ″Boot Problems/Concerns″ in the *@server pSeries 655 Service Guide* and follow the steps for network boot problems.

Use the following procedure to temporarily change the system bootlist so that the network adapter attached to the NIM server network is first in the bootlist.

1. Exit to the SMS main screen.
2. Select **Select Boot Options**.
3. Select **Install or Boot a Device**.
4. On the Select Device Type screen, select **Network**.
5. Set the network parameters for the adapter from which you want to boot.
6. Exit completely from SMS. The system should start loading packets while doing a bootp from the network.
7. Follow the instructions on the screen to select the system console.
   - If `Diagnostics Operating Instructions Version x.x.x` is displayed, standalone diagnostics has loaded successfully.
   - If the AIX login prompt is displayed, standalone diagnostics did not load. Check the following items:
     – The network parameters on the client may be incorrect.
     – Cstate on the NIM server may be incorrect.
     – Network problems might be preventing you from connecting to the NIM server.
8. Verify the settings and the status of the network. If you continue to have problems, refer to ″Boot Problems/Concerns″ in the *@server pSeries 655 Service Guide* and follow the steps for network boot problems.
9. After running diagnostics, reboot the system and use SMS to change the bootlist sequence back to its original setting.

Default Boot List and Service Mode Boot List

The default boot list is as follows:

1. Disk drive (if the operating system is installed)
2. Network adapter
   - Token-ring
   - Integrated Ethernet adapter

To load **standalone diagnostics**, press the 5 key on the HMC.

To load the **online diagnostics** press the 6 key on the HMC. The service mode boot list is loaded. Like the default boot list, the service mode boot list can contain several entries.

Note: The 6 key works like the 5 key with the following exceptions:

- The system searches for a boot record according to the service mode boot list.
- If the service mode boot list is discovered by a cyclical redundancy check to be corrupted, the system rebuilds the service mode boot list according to the default boot list. (The default boot list contains five entries, and for each matching device type found in the system unit, the system makes an entry in the service mode boot list.)
- If no service mode boot list is present, the system uses the default boot list.

Chapter 9. Hardware Problem Determination

This chapter provides information on using standalone or online diagnostics to help you solve hardware problems.

You may obtain more extensive problem isolation by running online diagnostics in service mode. This requires that the partition be rebooted (in a partitioned system) with no other users on that partition or that the system be rebooted (in a full system partition) with no other users on the system. Alternatively, if AIX online diagnostics are installed on the partition or system, you can run online diagnostics in concurrent mode. If the system or partition does not have AIX diagnostics installed, or if you cannot boot AIX or online diagnostics in service mode, run standalone diagnostics instead.

Problem Determination Using the Standalone or Online Diagnostics

Use this procedure to obtain a service request number (SRN) when you load the standalone or online diagnostics. If you are unable to load the standalone or online diagnostics, go to “Problem Determination When Unable to Load Diagnostics” on page 112. The service organization uses the SRN to determine which field replaceable units (FRUs) are needed to restore the system to correct operation.

Step 1. Considerations before Running This Procedure

Note: See the *IBM Hardware Management Console for pSeries Installation and Operations Guide* to find the key sequences you need for your Hardware Management Console for pSeries (HMC) virtual terminal window to respond to the diagnostic programs.

- The diagnostics may be run within a virtual terminal window on the HMC connected to the system.
- This procedure requires that you select the type of diagnostics you want to run.
- Go to “Step 2”.

Step 2

Are the online diagnostics installed on this system?

NO Go to “Step 6” on page 108.

YES Go to “Step 3”.

Step 3

Determine if the partition is accepting commands.

Is the operating system accepting commands?

NO If a partition is not accepting commands (or if the partition has an operating system other than AIX installed), run standalone diagnostics.

YES Go to “Step 4”.

Step 4

Diagnostic tests can be run on many resources while the operating system is running. However, you can obtain more extensive problem isolation by running online diagnostics in service mode.

Do you want to run the online diagnostics in service mode?

NO Go to “Step 5” on page 108.

YES Go to “Step 6” on page 108.

Step 5

This step starts the online diagnostics in concurrent mode.

Note: The AIX operating system must be installed on the partition on which you want to run online diagnostics.

1. Log in as root user or use CE Login.
2. Enter the `diag` command.
3. Wait until the diagnostic operating instructions display, or wait for three minutes.

Are the diagnostic operating instructions displayed without any obvious console display problems?

NO If the diagnostics operating instructions are not displayed on the partition, reboot that partition.

Note: Do not turn off the system unit if the system is running one or more logical partitions.

Go to “Step 6”.

YES Go to “Step 9”.

Step 6

This step loads online diagnostics in service mode.

1. Reboot the system.
2. At the SMS menu, press the numeric 6 key on the keyboard to indicate that diagnostics are to be loaded.
3. Type the requested passwords.
4. Follow the instructions to select a console.

Did the diagnostics operating instructions display without any obvious display problem?

NO Go to “Step 7”.

YES Go to “Step 9”.

Step 7

Is the problem a display problem?

NO Go to “Problem Determination When Unable to Load Diagnostics” on page 112.

YES Go to “Step 8”.

Step 8

This step analyzes a console display problem.

Go to the problem-determination documentation for this type of terminal. For more information, refer to the *IBM Hardware Management Console for pSeries Maintenance Guide*.

Step 9

The diagnostics loaded correctly.

Press Enter.

Is the Function Selection menu displayed?

NO Go to “Step 10”.

YES Go to “Step 11”.

Step 10

There is a problem with the keyboard.

Go to the problem-determination documentation for this type of terminal. For more information, refer to the *IBM Hardware Management Console for pSeries Maintenance Guide*.

Step 11

1. If the terminal type has not been defined, use the **Initialize Terminal** option on the Function Selection menu to initialize the operating system environment before you can continue with the diagnostics. This is a separate and different operation from selecting the console display.
2. Select **Diagnostic Routines**.
3. Press Enter.
4. In the following table, find the menu or system response you received when you selected **Diagnostics**. Perform the action listed in the Action column.

System Response	Action
The Diagnostic Mode Selection menu is displayed.	Select **Problem Determination** and go to “Step 12” on page 110.
The Missing Resource menu is displayed.	Follow the displayed instructions until either the Diagnostic Mode Selection menu or an SRN is displayed. If the Diagnostic Mode Selection menu is displayed, select **Problem Determination** and go to “Step 12” on page 110. If you get an SRN, record it, and go to “Step 14” on page 111.
The New Resource menu is displayed.	Follow the displayed instructions. If the Diagnostic Mode Selection menu is displayed, select Problem Determination and go to “Step 12” on page 110. If you get an SRN, record it, and go to “Step 14” on page 111. If you do not get an SRN, go to “Step 16” on page 111.
The system does not respond to selecting **diagnostics**.	Go to “Step 10”.

Step 12

Did the Diagnostic Selection Menu display?

NO

If **Problem Determination** was selected from the Diagnostic Mode Selection menu, and if a recent error has been logged in the error log, the diagnostics automatically begin testing the resource.

Follow the displayed instructions.

- If the No Trouble Found screen is displayed, press Enter.
- If another resource is tested, repeat this step.
- If the Diagnostic Selection menu is displayed, go to “Step 13” on page 111.

If an SRN is displayed, record it, and go to “Step 14” on page 111.

YES

Go to “Step 13” on page 111.

Step 13

The All Resources option checks most of the configured adapters and devices.

Select and run the diagnostic tests on the resources you are having problems with, or select the **All Resources** option to check all of the configured resources. Find the response in the following table and perform the action listed in the Action column.

Diagnostic Response	Action
An SRN is displayed.	Go to “Step 14”.
The system hangs.	Report SRN 109-200.
The Testing Complete menu and the `No trouble was found` message is displayed, and you have not tested all of the resources.	Press Enter and continue with the testing.
The Testing Complete menu and the `No trouble` was found message displayed and you have tested all of the resources.	Go to “Step 16”.

Step 14

The diagnostics produced an SRN for this problem. Do the following:

1. Record the SRN.
2. Report the SRN to the service organization.
3. **STOP.** You have completed these procedures.

Step 15

This step loads the standalone diagnostics.

1. If you are running one or more logical partitions, reboot the partition.

   Note: Standalone diagnostics may be run from a NIM server. If running from NIM, the NIM server must be set up to allow a diagnostic boot from that partition (both NIM server and client partition must have network adapters). For more information, see Chapter 6, “Using the Online and Standalone Diagnostics”, on page 59.
2. When the **keyboard** POST indicator displays, press the numeric 5 key on the keyboard to indicate that diagnostics should be loaded.
3. Type the requested passwords.
4. Follow the instructions to select a console.

Did the Diagnostics Operating Instructions display without any obvious display problem?

NO Go to “Step 7” on page 108.

YES Go to “Step 9” on page 108.

Step 16

The diagnostics did not detect a hardware problem. If you still have a problem, contact your service organization.

Problem Determination When Unable to Load Diagnostics

Use the following procedure to obtain an error code. The service organization uses the error code to determine which field replaceable units (FRUs) are needed to restore the system to correct operation.

Step 1

Are the online diagnostics installed on this system?

NO Go to “Step 15” on page 111.

YES Go to “Step 2”.

Step 2

This step attempts to load online diagnostics in service mode.

1. Reboot the partition.
2. If the **keyboard** POST indicator displays, press the numeric 6 key on the keyboard to indicate that diagnostics should be loaded from the hard disk.
3. Type the requested passwords.
4. Follow the instructions to select a console.
5. Wait until the diagnostics load or the system appears to stop.

Did the diagnostics load?

NO Go to “Step 4” on page 113.

YES Go to “Step 5” on page 114.

Step 3

This step attempts to load the standalone diagnostics.

1. Reboot the partition.

   Note: Standalone diagnostics may be run from a NIM server. If running from NIM, the NIM server must be set up to allow a diagnostic boot from that partition (both NIM server and client partition must have network adapters). For more information, see Chapter 6, “Using the Online and Standalone Diagnostics”, on page 59.
2. If the **keyboard** POST indicator displays, press the numeric 5 key on the keyboard to indicate that diagnostics are to be loaded from CD-ROM.
3. Type the requested passwords.
4. Follow the instructions to select a console.
5. Wait until the diagnostics load or the system appears to stop.

Did the diagnostics load?

NO Go to “Step 4” on page 113.

YES Go to “Step 5” on page 114.

Step 4

Starting at the top of the following table, locate your symptom and perform the action listed in the Action column.

Symptom	Action
The power LED does not come on, or comes on and does not stay on.	Check the power cable to the outlet. Check the circuit breakers and check for power at the outlet. Ensure that the room temperature is within 60 - 90°F. If you do not find a problem, record error code M0PS0000 and report the problem to the service organization.
The diagnostics are loaded and there was NO beep heard from the system unit during the IPL sequence.	Record error code M0SPK001.
The system stops with the diagnostic operating instructions displayed.	Go to “Step 5” on page 114.
The system stops with a prompt to enter a password.	Enter the password. You are not allowed to continue until a correct password has been entered. When you have entered a valid password, wait for one of the other conditions to occur.
The system stops with a three-, four- or eight-digit error code(s) displayed on the console.	Record the error code(s) and report the problem to the service organization.
The system login prompt is displayed.	You may not have pressed the correct key or you may not have pressed the key soon enough when you were to indicate a service mode boot of diagnostic programs. If this was the case, start over at the beginning of this step. If you are sure that you pressed the correct key in a timely manner, go to “Step 6” on page 114.
The system does not respond when the password is entered.	Go to “Step 6” on page 114.
The system stopped and an indicator is displayed on the system console and an eight-digit error code is not displayed.	If the indicator represents: • A keyboard: record error code M0KBD000 and report the problem to the service organization. • Memory: record error code M0MEM002 and report the problem to the service organization. • SCSI: record error code M0CON000 and report the problem to the service organization. • Network: record error code M0NET000 and report the problem to the service organization. • Speaker/audio: record error code M0BT0000 and report the problem to the service organization.

Symptom	Action
The System Management Services menu is displayed.	The device or media that you are attempting to boot from might be faulty. 1. Check the SMS error log for any errors. To check the error log: • Select **View Error Log**. • If an error is logged, check the time stamp. • If the error was logged during the current boot attempt, record it and report it to your service representative. • If no recent error is logged in the error log, continue to the next step. 2. If you are attempting to load the online diagnostics, try loading the standalone diagnostics. Otherwise, record error code M0SCSI01 and report to the service organization.
The system appears to be stopped, the disk activity light is on continuously, and a beep was heard from the system unit.	Record error code M0MEM001 and report the problem to the service organization.
The system stops and the message `STARTING SOFTWARE PLEASE WAIT ...` is displayed.	Report error code M0BT0000.
The message `The system will now continue the boot process` is displayed continuously on the system unit's console.	Report error code M0SCSI01.

Step 5

The diagnostics loaded correctly.

Go to "Problem Determination Using the Standalone or Online Diagnostics" on page 107.

Step 6

There is a problem with the keyboard.

Go to the problem-determination documentation for this type of terminal. For more information, refer to the *IBM Hardware Management Console for pSeries Maintenance Guide*.

Appendix A. Environmental Notices

Product Recycling and Disposal

This unit contains materials such as circuit boards, cables, electromagnetic compatibility gaskets and connectors which may contain lead and copper/beryllium alloys that require special handling and disposal at end of life. Before this unit is disposed of, these materials must be removed and recycled or discarded according to applicable regulations. IBM offers product return programs in several countries, for country specific instructions please refer to the following web site:
http://www.ibm.com/ibm/environment/products/prp.phtml

This product may contain a sealed lead acid battery(s) or nickel-cadmium battery(s). The battery(s) must be recycled or disposed of properly. Recycling facilities may not be available in your area. In the United States, IBM has established a collection process for reuse, recycling, or proper disposal of used sealed lead acid, nickel cadmium and nickel metal hydride batteries and battery packs from IBM equipment. For information on proper disposal of the batteries in this product, please contact IBM at 1-800-426-4333. For information on disposal of sealed lead acid or nickel cadmium batteries outside the United States, contact your local waste disposal or recycling facility.

Environmental Design

The environmental efforts that have gone into the design of this system signify IBM's commitment to improve the quality of its products and processes. Some of these accomplishments include the elimination of the use of Class 1 ozone-depleting chemicals in the manufacturing process and reductions in manufacturing wastes. For more information, contact an IBM account representative.

Acoustical Noise Emissions[1, 2]

Product Configuration	Declared A-Weighted Sound Power Level, L_{WAd} (B)		Declared A-Weighted Sound Pressure Level, LpAm (dB)	
	Operating	Idle	Operating	Idle
One @server pSeries 655 processor node processor node (maximum 16 per system), nominal conditions, non-acoustical doors	7.2	7.2	55	55
One @server pSeries 655 processor node processor node (maximum 16 per system) nominal conditions, acoustical doors	6.7	6.7	50	50
Typical configuration of @server pSeries 655 processor node system (3 processor nodes, bulk power, 1 I/O drawer), nominal conditions, non-acoustical doors	8.1	8.1	63	63
Typical configuration of @server pSeries 655 processor node system (3 processor nodes, bulk power, 1 I/O drawer), nominal conditions, acoustical doors	7.5	7.5	57	57
Maximum configuration of @server pSeries 655 processor node system (16 processor nodes, bulk power), nominal conditions, non-acoustical doors	8.3[3]	8.3[3]	65[3]	69[3]
Maximum configuration of @server pSeries 655 processor node system (16 processor nodes, bulk power), nominal conditions, acoustical doors	7.7[3]	7.7[3]	59[3]	59[3]

Notes:

1. **L_{WAd}** is the upper-limit A-weighted sound level; **L_{pAm}** is the mean A-weighted sound pressure level measured at the 1-meter bystander positions; 1 B = 10 dB.
2. All measurements made in conformance with ISO 7779 and declared in conformance with ISO 9296
3. **Attention:** Your server installation may be subject to government regulations (such as those prescribed by OSHA or European Community Directives) that cover noise-level exposure in the workplace. The 7040 Model W42 rack is available with an optional acoustical door feature that can reduce the likelihood of exceeding noise-level exposure limits for racks densely populated with pSeries 655 processor subassemblies. The actual sound-pressure levels in your installation will depend on a variety of factors, including the number of racks in the installation; the size, materials, and configuration of the room where the racks are installed; the noise levels from other equipment; the room ambient temperature, and employees' location in relation to the equipment. It is recommended that a qualified person, such as an industrial hygienist, be consulted to determine whether the sound-pressure levels to which employees may be exposed exceed regulatory limits.

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

The manufacturer may not offer the products, services, or features discussed in this document in other countries. Consult the manufacturer's representative for information on the products and services currently available in your area. Any reference to the manufacturer's product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any intellectual property right of the manufacturer may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any product, program, or service.

The manufacturer may have patents or pending patent applications covering subject matter described 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 manufacturer.

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: THIS MANUAL IS PROVIDED ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. The manufacturer may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Information concerning products made by other than the manufacturer was obtained from the suppliers of those products, their published announcements, or other publicly available sources. The manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products made by other than the manufacturer. Questions on the capabilities of products made by other than the manufacturer should be addressed to the suppliers of those products.

Index

Numerics

A

B

C

D

E

F

G

P

R

S

T

U

V

W

Readers' Comments — We'd Like to Hear from You

pSeries 655
User's Guide

Publication No. SA38-0617-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

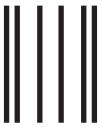
Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SA38-0617-00

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department H6DS-905-6C006
11501 Burnet Road
Austin, TX 78758-3493

Fold and Tape | **Please do not staple** | Fold and Tape

SA38-0617-00

Cut or Fold
Along Line

Printed in U.S.A.

November 2002

SA38-0617-00