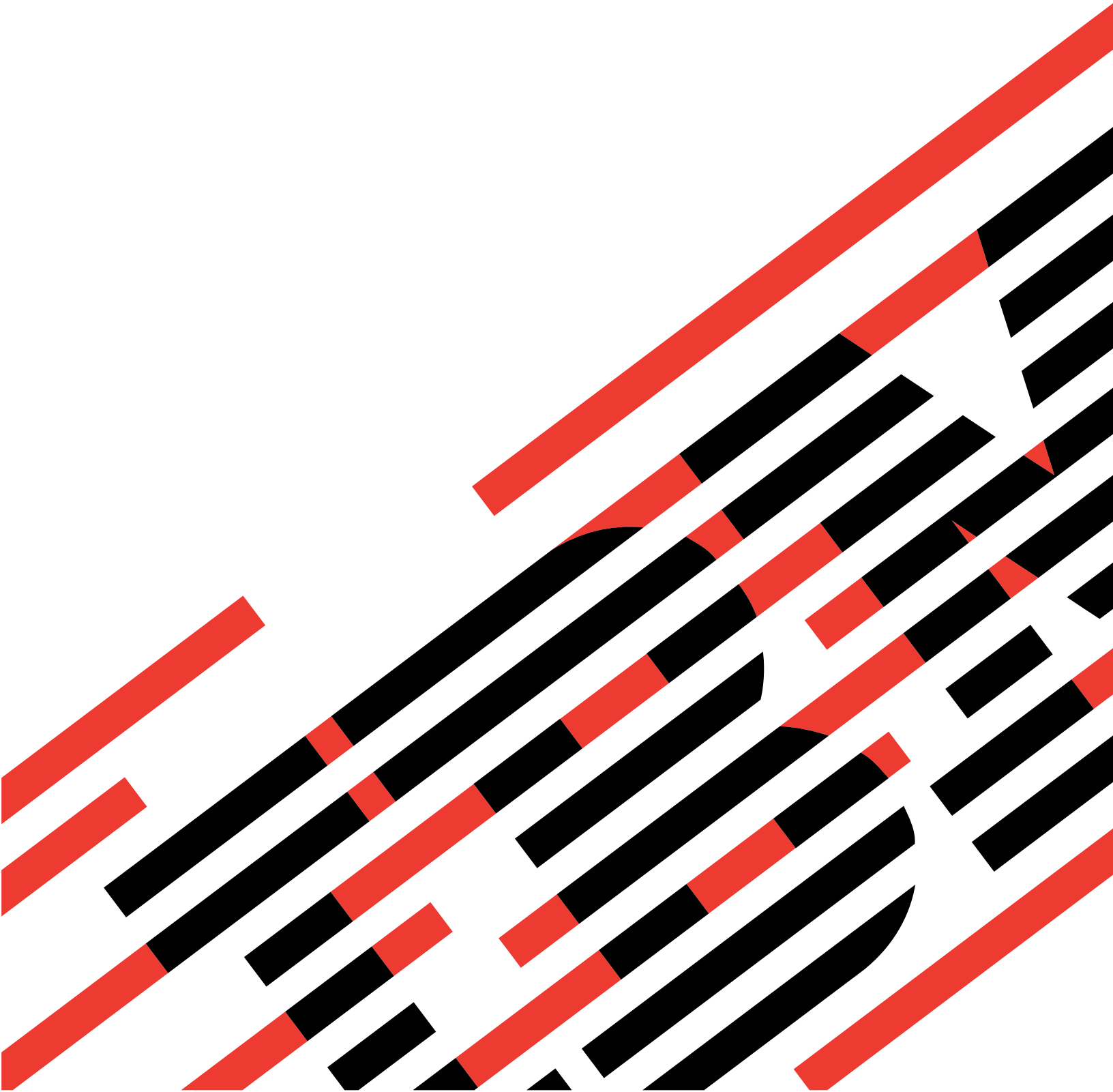
IBM

eserver

Service provider information
Reference information



IBM

@server

Service provider information
Reference information

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 119 and the manual *IBM eServer Safety Information*, G229-9054.

Fourth Edition (December 2004)

© Copyright International Business Machines Corporation 2004. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Reference information 1

i5/OS data recovery information 1
- Disk unit recovery procedures 2
- System reference code (SRC) address formats . . 17
- Storage I/O card modes and jumpers. 21
- Logical partitions 23
- Load-source disks and alternate IPL devices . . 23
- Reclaiming IOP cache storage 25

Working with AIX diagnostics 26
- General AIX diagnostic information 28
- Loading the AIX online diagnostics or the @server standalone diagnostics 37
- AIX tasks and service aids 44

Powering on and powering off 82
- Powering off an expansion unit. 83
- Powering off a system with multiple logical partitions 87
- Using the control panel power button to power off 87

Hardware Management Console Maintenance . . . 88
Using System Management Services (SMS) 90
Component and attention LEDs 101
Setting expansion unit configuration ID and MTMS value 106
Updating the world-wide port name for a new 2766 or 2787 IOA 108
System safety inspection. 109
Forms 110
- Problem reporting forms. 111
- Work with electrostatic discharge-sensitive parts 113
- Service log 114
- HSL cable location form 116

Chapter 2. Related information for service provider information 117

Appendix. Notices 119

Trademarks 120
Communications statements 121
- Federal Communications Commission (FCC) statement. 121
- Federal Communications Commission (FCC) statement. 123

Terms and conditions for downloading and printing information 124
Product recycling and disposal 125
Battery return program 125
IBM Cryptographic Adapter Card Return Program 126

© Copyright IBM Corp. 2004

Chapter 1. Reference information

This information is intended to provide IBM® service providers with supplemental information for servicing a customer's model 520, 550, 9124-720, 570, 590, or 595 system.

Before using this information and the products it supports, be sure to read Safety notices.

"i5/OS data recovery information"
Provides recovery information specific to i5/OS™.

"Working with AIX diagnostics" on page 26
Provides diagnostic information specific to AIX®.

"Powering on and powering off" on page 82
Provides information for powering on and powering off the system.

"Hardware Management Console Maintenance" on page 88
Provides information for servicing the HMC.

"Using System Management Services (SMS)" on page 90
Provides information for using the System Management Services.

"Component and attention LEDs" on page 101
Provides information about component and attention LEDs.

"Setting expansion unit configuration ID and MTMS value" on page 106
Provides instructions for setting important system values.

"Updating the world-wide port name for a new 2766 or 2787 IOA" on page 108
Provides instructions for updating the world-wide port name after exchanging certain IOAs.

"System safety inspection" on page 109
Provides instructions for performing a safety inspection on the system.

"Forms" on page 110
Includes various forms that may be needed during the service activity.

i5/OS data recovery information

"Disk unit recovery procedures" on page 2

"System reference code (SRC) address formats" on page 17

"Storage I/O card modes and jumpers" on page 21

"Logical partitions" on page 23

"Load-source disks and alternate IPL devices" on page 23

"Reclaiming IOP cache storage" on page 25

© Copyright IBM Corp. 2004

Disk unit recovery procedures

This topic contains the procedures and information to recover from disk unit failures with a minimum loss of customer data.

The procedures in this section do not give support to rack-mounted disk units such as an IBM 9337. For disk service support on rack-mounted disk units, use the *FC 504x Problem Analysis and Repair and Parts, SY44-4934* information. These procedures also do not give support to IBM 2105 disk units. Use the *"IBM 2105 maintenance"* information for disk service support.

Start all service actions at "Starting disk service" and follow the steps in the procedures to determine the following:

- The storage protection method that is used by the customer
- When and how to save customer data
- When to exchange a failing disk unit
- How to restore saved data
- How to resume storage protection

Starting disk service

Before exchanging a disk unit, you must attempt to save customer data. This procedure directs you to the correct recovery procedure to use when attempting to save customer data.

1. Is the disk unit a type 673x?

   No: Continue with the next step.

   Yes: Type 673x is a read cache which does not contain data that needs to be saved. Exchange the read cache using procedures in Disk drive. **This ends the procedure.**

   Note: Exchange the cache with the system powered on if you can get to a Dedicated Service Tools (DST) or System Service Tools (SST) screen.

2. Choose one of the following options:
   - If your system has mirrored protection for the failing disk unit, go to "Exchanging a disk unit with mirrored protection" on page 4. **This ends the procedure.**
   - If your system has device parity protection for the failing disk unit, go to "Exchanging a disk unit with device parity protection" on page 3. **This ends the procedure.**

     Note: If you are not sure whether the system has mirror protection or device parity protection, see Determine storage protection status below.
   - If neither of the above conditions apply, then continue with the next step.
3. You are exchanging the disk unit. Choose from the following:
   - To save the data by copying to tape, go to "Saving data and initializing the disk unit" on page 7. **This ends the procedure.**
   - To save the data by copying to another disk, go to "Initializing the disk unit and copying to disk" on page 13. **This ends the procedure.**

Determine storage protection status

The customer should know if the system is configured for storage protection and should have kept a printout of the storage protection configuration. Ask the customer for this information.

If the customer does not know if the system has storage protection configured, then perform the following:

1. Does the system IPL to Dedicated Service Tools (DST)?

   Yes: Continue with the next step.

No: Contact your next level of support. **This ends the procedure.**

2. Select **System Service Tools** (SST). If you cannot get to SST, select DST (see Dedicated Service Tools (DST)).

   Note: Do not IPL the system to get to DST.

3. From the Service Tools display, select **Work with disk units** > **Display disk configuration** > **Display disk configuration status**.
4. A list of each auxiliary storage pool (ASP) will display, showing the disk units that are members of the ASP. The status column shows one of the following protection statuses for the ASP:
   - **Mirrored**
     These ASPs are configured for mirrored protection. If the failing disk unit has mirrored protection, write down the status of the failing disk unit and its mirrored pair. You will need this information later in one of the recovery procedures.
   - **Unprotected**
     An ASP with a status of *unprotected* may contain disk units that are data parity protected. Look in the status column of the Display Disk Configuration Status display. A unit with one of the following statuses has data parity protection only if all other units in the array are operational:
     - DPY/Active
     - DPY/Failed
     - DPY/HDW Failure
     - DPY/Degraded
     - DPY/Power Loss
     - DPY/Not Ready
     - DPY/Unknown

     A unit with any other status (such as *DPY/Rebuild* or *DPY/Unprotected*) does not have data parity protection.

     Examples:
     - Suppose one unit has a status of *DPY/Failed* while all other units have a status of *DPY/Unprotected*. In this case, only the unit with the *DPY/Failed* status is protected. Servicing the failed unit will not result in data loss. Removing any of the unprotected units could result in data loss.
     - If all units have a status of *DPY/Active* or *DPY/Degraded*, all units are protected. In this case, exchanging any unit will not result in data loss.

     Note: For more information about the meaning of a status for any unit, use the Help key as indicated on the display.
5. Return to the procedure that sent you here. **This ends the procedure.**

Exchanging a disk unit with device parity protection

1. Does the failing unit have data parity protection that allows service without possible data loss (see Determine storage protection status)?

   No: Customer data may be lost if serviced. Ask your next level of support for assistance. **This ends the procedure.**

   Yes: Perform the following:

   a. Record the disk unit location and resource name for later use. If you do not already have the disk unit location information, use the location information in the Service Action Log (SAL). If the location is not available, find the address (see Addresses), which can be used to find the location.
   b. Exchange the failing disk unit with the system powered on (see Disk drive).

c. If the concurrent procedure fails, go to step 4. Otherwise, continue with the next step of this procedure.

2. Perform the following:
   a. Select System Service Tools (SST). If you cannot get to SST, select Dedicated Service Tools (DST) (see Dedicated Service Tools (DST) for details).

      Note: Do not IPL the system to get to DST.
   b. From the Service Tools display, select **Work with disk units** > **Work with disk unit recovery** > **Rebuild disk unit data**.
   c. Does the resource name of the disk unit you just exchanged appear on the display as a unit that can be rebuilt?

      Yes: Continue with the next step.

      No: It can take up to five minutes for the input/output processor (IOP) to report the device to the system. Keep trying the **Rebuild Disk Unit Data** option until the device is available. If the Rebuild Disk Unit Data Failed display continues to appear even after 5 minutes, try a different disk unit or ask your next level of support for assistance. Once the device becomes available, continue with the next step.
3. Perform the following steps:
   a. Select the disk unit on the display with the resource name of the disk unit you just exchanged.
   b. Rebuild the disk unit data. When the new disk unit is rebuilt, the display will show that the status is complete (this may take 30 minutes or longer).

      Note: Once the rebuild has started, it is not necessary to wait to verify the array rebuild completes successfully.
   c. Return to the procedure that sent you here. **This ends the procedure.**
4. Exchange the failing disk unit (see Disk drive).
5. Perform the following:
   a. Ask the customer to stop all active applications on the system and power the system off with the Power Down System (`PWRDWNSYS`) command.
   b. Perform an IPL to DST (see Dedicated Service Tools (DST)).
   c. From the Service Tools display, select **Work with disk units** > **Work with disk unit recovery** > **Rebuild disk unit data**.
   d. Select the disk unit on the display that was installed in place of the failing disk unit.
   e. Rebuild the disk unit data. When the new disk unit is rebuilt, the display shows that the status is complete (this may take 30 minutes or longer).
   f. After verifying that the status is complete, press Enter.
6. Perform the following:
   a. Return to the Use Dedicated Service Tools (DST) display.
   b. Select **Perform an IPL** to complete the IPL.
   c. Return to the procedure that sent you here. **This ends the procedure.**

Exchanging a disk unit with mirrored protection

Definitions:

- **Local load source:** A disk used as the source for IPL data.
- **Remote load source:** A load source disk unit that is not a local load source.

1. Display the disk unit status by performing the following:
   a. Select System Service Tools (SST). If you cannot get to SST, select Dedicated Service Tools (DST) (see Dedicated Service Tools (DST)).

Notes:

1) If the customer is running applications on the system, do not power off or IPL the system to get to DST.
2) If you cannot get to SST or DST, and the system fails during the IPL to DST, the local load source disk unit may be in the wrong location or in a failed state. SRC B1xx4504 is displayed during the IPL to DST if a functional load source disk unit is failing or not in one of the positions indicated by the local load source definition above.

   Systems that have remote load source mirror protection can be recovered by performing the Recover the remote load source procedure (see "Copy the contents of the LIC log" on page 17). If you do not know if this system has remote load source mirror protection, contact your next level of support.

b. From the Service Tools display, select **Work with disk units** > **Display disk configuration** > **Display disk configuration status**.

c. Does the failing disk unit have a status of *suspended*?

   Yes: Go to step 10 on page 6.

   No: Continue with the next step.

2. Does the disk unit that is mirrored to the failing disk unit have a status of *suspended*?

   No: Go to step 8.

   Yes: Continue with the next step.

3. Is the failing disk unit the load source (disk unit 1)?

   Yes: Continue with the next step.

   No: Go to step 5.

4. Is the failing load source disk unit a local load source?

   No: Go to step 6.

   Yes: Continue with the next step.

5. Ask the customer to end all applications that are running on the system and power off the system off with the Power Down System command (PWRDWNSYS). Then choose from the following options:
   - To save the data by copying to tape, go to "Saving data and initializing the disk unit" on page 7.
   - To save the data by copying to another disk, go to "Initializing the disk unit and copying to disk" on page 13.

   This ends the procedure.

6. Perform the following to attempt to repair the local load source. Performing this procedure reduces the duration of the repair time.

a. Record the location of the local load source disk unit.

b. Exchange the local load source disk unit using concurrent maintenance for the model or system unit that you are working on (see Disk drive).

c. Was the disk unit exchanged successfully using the concurrent maintenance procedure?

   Yes: Go to step 11 on page 6.

   No: Continue with the next step.

7. Ask the customer to stop all applications that are running on the system and power the system off with the Power Down System command (PWRDWNSYS). Was the local load source disk unit exchanged with the power off?

   No: Exchange the failing local load source disk unit with the power off (see Disk drive). After exchanging the disk unit, go to "Copy the contents of the LIC log" on page 17. **This ends the procedure.**

   Yes: Go to "Copy the contents of the LIC log" on page 17.**This ends the procedure.**

8. Is the disk unit that is mirrored to the failing disk unit missing?

Note: A note at the bottom of the display with an asterisk (*) indicates the unit is missing from the configuration.

Yes: Ensure that the customer is not running any jobs before performing the following:

a. Power off the system.
b. Go to LICIP11 and use cause code 0002.
c. If you cannot determine why the unit is missing, contact your next level of support.
d. If you correct the missing disk unit problem, go to "Starting disk service" on page 2 to locate and perform the correct recovery procedure. **This ends the procedure.**

No: Continue with the next step.

9. Does the disk unit that is mirrored to the failing disk unit have a status of *active*?

   No: Continue with the next step.

   Yes: Suspend mirrored protection on the failing disk unit by performing the following:

   a. Return to the Work With Disk Units menu.
   b. Select **Work with disk unit recovery** > **Suspend mirrored protection**.
   c. Follow the instructions on the display to suspend mirrored protection on the failing disk unit. Continue with the next step.

10. Record the disk unit location for later use. Then exchange the failing disk unit (see Disk drive). Did the concurrent remove and replace procedure fail?

    Yes: Go to step 14.

    No: Continue with the next step.

11. Perform the following:

    a. Select System Service Tools (SST). If you cannot get to SST, select DST (see Dedicated Service Tools (DST)).

       Note: Do not IPL the system to get to DST.

    b. Select **Work with disk units** > **Display disk configuration** > **Display non-configured units**.

       Note: It can take up to 5 minutes for the IOP to report the device to the system. If the disk unit you just exchanged does not appear as a non-configured unit on the display, wait a few minutes. Then press **F5** to refresh the display.

    c. When the disk unit you just exchanged appears as a non-configured unit on the display, continue with the next step.

12. Format and initialize the disk unit by performing the following:

    a. From the Service Tools display, select **Work with disk units** > **Work with disk unit recovery** > **Disk unit problem recovery procedures** > **Initialize and format disk unit**.
    b. Select the disk unit that you just installed.
    c. Initialize and format the disk unit. When the new disk unit is initialized and formatted, the display shows that the status is complete (this may take 30 minutes or longer).

13. Perform the following:

    a. Return to the Work with Disk Unit Recovery display and select **Replace configured unit**.
    b. On the Select Configured Unit to Replace display, select the configured disk unit you want to exchange.
    c. On the Select Replacement Unit display, select the replacement disk unit. Return to the procedure that sent you here. **This ends the procedure.**

14. Is the failing disk unit a load source?

    No: Go to step 16 on page 7.

    Yes: Continue with the next step.

15. Is the disk unit that is mirrored to the failing disk unit also a local load source?

Yes: Continue with the next step.

No: Ask the customer to end all applications that are running on the system and power the system off with the Power Down System command (PWRDWNSYS). Then go to "Copy the contents of the LIC log" on page 17. **This ends the procedure.**

16. Ask the customer to end all applications that are running on the system and power the system off with the Power Down System command (PWRDWNSYS). Then, exchange the failing disk unit (see Disk drive). Continue with the next step.
17. Perform an IPL to DST (see Performing an IPL to DST).
18. Format and initialize the disk unit by performing the following:
    a. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery** > **Disk unit problem recovery procedures** > **Initialize and format disk unit**.
    b. On the display, select the disk unit that you just installed.
    c. Initialize and format the disk unit. When the new disk unit is initialized and formatted, the display shows that the status is complete (this may take 30 minutes or longer).
19. Perform the following:
    a. Select the **Replace configured unit** option on the Work with Disk Unit Recovery display.
    b. On the Select Configured Unit to Replace display, select the configured disk unit you want to exchange.
    c. On the Select Replacement Unit display, select the replacement disk unit.
20. Perform the following:
    a. Return to the Use Dedicated Service Tools (DST) display.
    b. Select **Perform an IPL** to complete the IPL. The system copies data to the new disk unit during the IPL.
    c. Return to the procedure that sent you here. **This ends the procedure.**

Resuming mirrored protection

Use this procedure to resume mirrored protection on suspended disk units.

1. From the System Service Tools (SST) display or on the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery** > **Resume mirrored protection**.

   Note: See 5250 Console in the Managing your server topic for details on accessing a 5250 console session on the HMC.
2. On the Resume Mirrored Protection display, select the disk unit that you just replaced. It should have a status of *suspended*.
3. Is the disk unit in an Independent Auxiliary Storage Pool (IASP)?

   Yes: The disk unit that you selected will become active when the IASP is varied on. **This ends the procedure.**

   No: Continue with the next step.
4. Are you in SST?

   Yes: The disk unit that you selected will become active when the system is operational. **This ends the procedure.**

   No: Return to the Use Dedicated Service Tools (DST) display and perform an IPL. The disk unit that you selected will become active during the IPL. **This ends the procedure.**

Saving data and initializing the disk unit

To complete this procedure, you might need the latest set of Save System (SAVSYS) or SAVSTG tapes that were made before the problem occurred. You will also need three blank tapes.

1. Are you exchanging a disk unit because a disk unit failure caused system operations to stop completely?

   Yes: Continue with the next step.

No: You may be able to use the Remove Units from Configuration function of DST. This function allows you to move all data from the disk unit you want to exchange to the other disk units in the same auxiliary storage pool (ASP). Go to step 20 on page 11.

2. Perform an IPL to Dedicated Service Tools (DST) (see Performing an IPL to DST). Does the Use Dedicated Service Tools (DST) display appear?

   Yes: Go to step 5.

   No: Continue with the next step.

3. Did any messages regarding missing disk units appear?

   Yes: Ignore the messages and go to step 5.

   No: Continue with the next step.

4. Repeat step 2. Does the same SRC occur again?

   Yes: The customer data is not recoverable. Go to step 7.

   No: Use the new SRC to correct the problem. Go to Start of call procedure. **This ends the procedure.**

5. From the Use Dedicated Service Tools (DST) display, perform the following to save the customer data from the failing disk unit:
   a. Select **Work with disk units** > **Work with disk unit recovery** > **Save disk unit data**.
   b. On the Select Disk Unit Data to Save display, select the disk unit from which you want to save the data. Record the ASP of the disk unit that you are saving.

      Note: If the disk unit is missing, you cannot save the customer data to tape at this time. Go to step 7.

   c. Install a tape in the tape unit. The Specify Volume Identifier prompt appears.
   d. Enter the volume identifier for the tape. Write down the tape volume identifier. You will use the tape volume identifier later in this procedure. The Select Tape Unit prompt appears.
   e. Select the tape unit that you loaded with a tape. The Function Status display shows the percent of disk data saved.

      Note: If the tape volume identifier that you entered does not match the tape volume identifier on the tape you loaded, the Device Intervention Required prompt appears. The message ″Wrong volume loaded″ appears at the bottom of the display. Select the Format option and press **Enter** to continue the save operation.

   f. If the tape is full, the Device Intervention display appears. The message ″Load next volume″ appears at the bottom of the display. Insert the next tape into the tape unit and select the option to retry, and then press **Enter** to continue the save operation.
   g. Continue saving the disk unit data until the status of the save is complete.

      Note: Customer data is not recoverable if one of the following occurs:
      - The copy operation does not complete.
      - A large number of unreadable pages must be copied from the disk unit.

6. Does the display show that the status of the save is complete?

   No: Continue with the next step.

   Yes: Go to step 8 on page 9.

7. Have you already exchanged the storage IOA?

   Yes: Continue with the next step.

   No: Perform the following:
   a. Power off the system.
   b. Exchange the storage IOA (see Removing and replacing parts). If you do not know the part number, see Finding part locations.

c. Perform an IPL to Dedicated Service Tools (DST) (see Performing an IPL to DST).
d. Choose from the following:
   - If the same SRC occurs, go to step 8.
   - If a different SRC occurs, use it to correct the problem. Go to Start of call procedure.
   - If no SRC occurs, then the problem has been resolved. **This ends the procedure.**

8. Power off the system and exchange the failing disk unit (see Disk drive).
9. Did you just exchange disk unit 1 in the system unit?

   Yes: Go to step 11.

   No: Format and initialize the new disk unit by performing the following:

   a. Perform an IPL to DST (see Performing an IPL to DST). You may ignore any messages regarding missing disk units.
   b. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery** > **Disk unit problem recovery procedures** > **Initialize and format disk unit**.
   c. Select the disk unit you wish to initialize and format.
   d. Press **F10** on the confirmation display. The system formats and initializes the new disk unit. The display shows when the status is complete (this may take 30 minutes or longer). Continue with the next step.

10. Is most of the customer data recoverable (see step 5 on page 8)?

    No: Go to step 18 on page 11.

    Yes: Restore the customer data from the tape to the new disk unit by performing the following:

    a. Return to the Work With Disk Unit Recovery display and select **Restore disk unit data**.
    b. Enter the tape volume identifier. This is the volume identifier that you entered during the save procedure.
    c. Install into the tape unit the first tape that the data was saved to.
    d. On the Select Tape Unit display, select the tape unit that you want the data restored from.
    e. On the Restore Disk Unit Data display, select the disk unit on which you want to restore the data.
    f. Press **F10** to confirm the restore. The Function Status display shows the percentage of customer data restored. The system will IPL to the Use Dedicated Service Tools (DST) display when the restore has completed.

       Note: Any damaged objects that were restored must be loaded again by the customer. Refer the customer to the Backup and Recovery book.

    g. The system is ready for the next IPL. **This ends the procedure.**

11. Is the customer data recoverable (see step 5 on page 8)?

    No: Go to step 14 on page 10.

    Yes: Perform an IPL from removable media and select the option to install Licensed Internal Code and restore disk unit data. See Utilities to Install and Restore Licensed Internal Code. Then continue with the next step.

12. Did you get a Disk Configuration Error Report with a *Unit has incorrect logical partition configuration* warning?

    No: Continue with the next step.

    Yes: You have logical partitions that need to be recovered before you can continue with this disk unit recovery procedure. Perform the following:

    a. Select the **Use Dedicated Service Tools (DST)** option from the IPL or Install the System display.

b. Enter the password 22222222. If this password is not valid, ask the customer for the correct password.
c. From the Use Dedicated Service Tools (DST) display, select **Work with system partitions** > **Recover configuration data** > **Recover primary partition configuration data**.
d. Review the information on the Select Disk Unit for Configuration Data Recovery display. Select the disk unit with the most recent date and the correct system serial number, and then press **Enter**. The system automatically copies the configuration data to the primary partition's load source, and performs an IPL. Continue with the next step.

13. Restore the customer data from the tape to the new disk unit by performing the following:
    a. Select **Use Dedicated Service Tools (DST)** from the IPL or Install the System display.
    b. Enter the password 22222222. If this password is not valid, ask the customer for the correct password.
    c. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery** > **Restore disk unit data**.
    d. Enter the tape volume identifier. This is the volume identifier that you entered during the save procedure.
    e. Install the first tape to which the data was saved in the tape unit.
    f. On the Select Tape Unit display, select the tape unit that you want the data restored from.
    g. On the Restore Disk Unit Data display, select the disk unit on which you want to restore the data.
    h. Press **F10** to confirm the restore. The Function Status display shows the percentage of customer data restored.

       Note: When the load-source disk is restored, the system automatically performs an IPL to the Use Dedicated Service Tools (DST) display. This occurs after the restore operation completes.

    i. When all customer data from the tape to the disk restores successfully, the display shows that the status of the restore operation as complete. Press **Enter** to complete the restore operation.
    j. Power off the system.

       Note: Any damaged objects that were restored must be loaded again by the customer. Refer the customer to the Backup and Recovery book.

    k. The system is ready for the next IPL. **This ends the procedure.**
14. Perform an IPL from removable media and select the option to install Licensed Internal Code and recover configuration. See Utilities to Install and Restore Licensed Internal Code. Then continue with the next step.
15. Did you get a Disk Configuration Error Report with a *Unit has incorrect logical partition configuration* warning?

    No: Continue with the next step.

    Yes: You have logical partitions that need to be recovered before you can continue with this disk unit recovery procedure. Perform the following:
    a. Enter **Use Dedicated Service Tools (DST)** from the IPL or Install the System display.
    b. Enter the password 22222222. If this password is not valid, ask the customer for the correct password.
    c. From the Use Dedicated Service Tools (DST) display, select **Work with system partitions** > **Recover configuration data** > **Recover primary partition configuration data**.
    d. Review the information on the Select Disk Unit for Configuration Data Recovery display. Select the disk unit with the most recent date and the correct system serial number, and then press **Enter**. The system will automatically copy the configuration data to the primary partition's load source, and then perform an IPL. Continue with the next step.

16. The system ASP will be cleared because customer data was not recoverable. Recover the configuration to disk unit 1 in the system unit by performing the following:
    a. Enter **Use Dedicated Service Tools (DST)** from the IPL or Install the System display.
    b. Enter the password 22222222. If this password is not valid, ask the customer for the correct password.
    c. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery**.
    d. Select **Recover configuration** on the Work with Disk Unit Recovery display. This option assembles the system configuration information on disk unit 1 in the system unit. Continue with the next step.

       Note: A warning message will appear stating that recovering the configuration destroys all system data.
17. Did a message appear stating that your request to recover the configuration was not successful?

    Yes: You are working on a system with only one disk unit, and the recover configuration function cannot be performed with only one disk unit. Go to step 18.

    No: Go to step 19.
18. Because the disk data was not recoverable, clear the auxiliary storage pool (ASP) to which the disk unit is assigned by performing the following:
    a. Return to the Work with Disk Units display. Select **Work with disk configuration** > **Work with ASP configuration** > **Delete ASP data**.
    b. Enter the **Delete** option for the ASP that you recorded in step 5 on page 8, and confirm the deletion.
    c. Return to the Work with Disk Units display, and select **Work with disk unit recovery** > **Replace configured unit**.
    d. On the Select Configured Unit to Replace display, select the configured disk unit to exchange.
    e. On the Select Replacement Unit display, select the new disk unit.
    f. Press **Enter** to confirm the replace operation (this operation takes 10 to 15 minutes to complete). **This ends the procedure.**

       Attention: The auxiliary storage pool to which the disk unit is assigned was erased. The customer must restore the data to the auxiliary storage pool. Refer the customer to the Backup and Recovery book.
19. The ASP to which the failing disk unit was assigned was erased. The customer should perform one of the following:

    - If the disk unit you exchanged is in ASP 1, refer the customer to the Backup and Recovery book to restore the operating system and all customer data. **This ends the procedure.**
    - If the disk unit is in a user ASP (ASP 2 through ASP 16), data in the ASP is lost. See the Backup and Recovery book. **This ends the procedure.**
20. The remaining steps of this procedure require a dedicated system. Have the customer do a normal power-off procedure of the system. Then continue with the next step.
21. Perform an IPL to DST (see Performing an IPL to DST). Is the IPL or Install the System display shown, or is DST available?

    No: Go to step 2 on page 8.

    Yes: Select **Use dedicated service tools (DST)** on the display or use a function key. Have the customer enter their password to get to the Use Dedicated Service Tools (DST) display. Continue with the next step.
22. Perform the following:

a. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk configuration** > **Display disk configuration** > **Display disk configuration status**.
b. Record the ASP, unit, serial number, type, and resource name of the disk unit.
c. On the Display Disk Configuration Status display, ensure the following:
   - The disk unit is not the load-source disk unit (disk unit 1).
   - No disk units are missing from the configuration (indicated by an asterisk (*) next to the unit number).
   - The status field of the disk unit to be removed shows *Configured*.

Are all of the above conditions true?

Yes: Continue with the next step.

No: You cannot use the Remove Units from Configuration function. Go to step 2 on page 8.

23. Return to the Display Disk Configuration display and select **Display disk configuration capacity**. Does the *% Used* field for the disk unit to be removed show an asterisk (*)?

    No: Continue with the next step.

    Yes: You cannot use the Remove Units from Configuration function. Go to step 2 on page 8.

24. Return to the Work with Disk Units display and perform the following:
    a. Select **Work with disk unit recovery** > **Disk unit problem recovery procedures** > **Analyze disk unit surface**.
    b. Select the disk unit to analyze.
    c. Press **F10** to analyze the disk unit surface.
    d. Wait until the Analyze function is complete. This will take several minutes.

    Are there any pages with errors?

    No: Continue with the next step.

    Yes: You cannot use the Remove Units from Configuration function. Go to step 2 on page 8.

25. Return to the Work with Disk Units display and perform the following:
    a. Select **Work with disk configuration** > **Work with ASP configuration** > **Remove units from configuration**.
    b. Select the disk unit to be removed. If the disk unit does not display, go to step 2 on page 8.
    c. If the Confirm Continuation display appears, press **Enter** to continue. Wait for the next display.
    d. If there is enough storage in the ASP, the Confirm Remove Disk Units display appears. If there is not enough storage, an error message display appears. Does any error message display appear?

       No: Continue with the next step.

       Yes: Go to step 2 on page 8.

26. Press **Enter** to verify the Remove Disk Units function. The Remove Disk Units function takes several minutes. When it is complete, a message will appear stating whether it was successful. Was the Remove Disk Units function successful?

    Yes: Continue with the next step.

    No: Go to step 2 on page 8.

27. On the Work with ASP Configuration display, select **Display disk configuration capacity**. Press **F11** twice to display non-configured units. Is the unit you removed shown as a non-configured unit?

    Yes: Continue with the next step.

    No: Go to step 2 on page 8.

28. You can exchange the disk unit at a later time because the disk unit is removed from the configuration. Do you want to exchange the disk unit now?

    Yes: Continue with the next step.

    No: This ends the procedure.

29. Power off the system and exchange the failing disk unit (see Disk drive).

30. Format and initialize the new disk unit by doing the following:
    a. Perform an IPL to DST (see Performing an IPL to DST).
    b. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery** > **Disk unit problem recovery procedures** > **Initialize and format disk unit**.
    c. Select the disk unit you wish to initialize and format.
    d. Press **F10** on the confirmation display.
    e. The system initializes and formats the new disk unit. The display shows when the status is complete (this may take 30 minutes or longer). Continue with the next step.
31. In this step, you use the ASP, unit, serial number, type, and resource name information that you recorded in step 22 on page 11. Perform the following:
    a. Return to the Work with Disk Units display and select **Work with disk configuration** > **Work with ASP configuration** > **Add units to ASPs**.
    b. Specify the ASP from which the disk units were removed.
    c. Select the unit to add to the ASP.
    d. When the Confirm Add Units display appears, press **Enter** to continue. Wait for the next display.
32. The Add Disk Units function takes several minutes. When it is complete, a message appears stating whether it was successful. Was the Add Disk Units function successful?

    No: Continue with the next step.

    Yes: On the Work with ASP Configuration display, select **Display disk configuration capacity**. The unit you that added should be shown in the correct ASP. **This ends the procedure.**
33. Do you have more field replaceable units (FRUs) to exchange?

    Yes: Go to step 29 on page 12.

    No: Ask your next level of support for assistance. **This ends the procedure.**

Initializing the disk unit and copying to disk

1. Perform an IPL to Dedicated Service Tools (DST) (see Performing an IPL to DST). Does the Use Dedicated Service Tools (DST) display appear?

   Yes: Continue with the next step.

   No: Repeat this step and then choose one of the following:
   - If the same system reference code (SRC) occurs again, the customer data is not recoverable. Go to step 12 on page 14.
   - If a different SRC occurs, go to the Start of call procedure to fix the problem. **This ends the procedure.**
2. Is this a single disk unit system?

   No: Continue with the next step.

   Yes: Perform "Saving data and initializing the disk unit" on page 7. **This ends the procedure.**
3. Is the failing disk unit the load-source disk unit (disk unit 1 contains the load-source disk unit)?

   Yes: Continue with the next step.

   No: Go to step 17 on page 15.
4. Find another disk unit on the system and perform the following to install the new disk unit:
   a. Power off the system.
   b. Slide the disk unit you found out of the system (see Disk drive). Be very careful with the disk unit. You will install it again when the service actions to the failing load-source disk unit are complete.
   c. Install the new disk unit.
5. Perform an IPL to DST (see Performing an IPL to DST). Does the Use Dedicated Service Tools (DST) display appear?

   Yes: Continue with the next step.

No: Repeat step 1 on page 13.

6. Perform the following to format and initialize the disk drive that you installed in step 4 on page 13:
   a. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery** > **Disk unit problem recovery procedures** > **Initialize and format disk unit**.
   b. Select the unconfigured unit that you installed in step 4 on page 13 as the unit to work with.
   c. Press F10 to verify the initialization and formatting. The initialization and formatting may take 30 minutes or longer to complete.
7. Perform the following to copy data from the load-source disk unit to the disk drive you installed in step 4 on page 13:
   a. Return to the Work with Disk Unit Recovery display.
   b. Select **Copy disk unit data**.
   c. Select the load-source disk unit (disk unit 1) as the unit to copy.
   d. Select the unconfigured unit that you installed in step 4 on page 13 as the unit to copy to.
   e. The console displays the percentage of the data copied. Write down the number of unreadable pages if it displays; you will use it later in this procedure.
   f. Wait until the status of the copy is *Complete*. Customer data is not recoverable if one of the following occurs:
      - The copy operation does not complete.
      - There is a large number of unreadable pages to copy from the disk unit.
8. Perform the following to remove the failing load-source disk unit from the system:
   a. Power off the system.
   b. Find the load-source disk unit. Slide the disk unit out of the system (see Disk drive).
9. Perform the following to move the new disk unit into the load-source disk unit location:
   a. Slide the disk unit at the location you found in step 4 on page 13 out of the system (see Disk drive). Be very careful with the disk unit—it contains the load-source data.
   b. Install the new disk unit into the location that used to contain the load-source disk unit.
10. Install the disk unit that you removed in step 4 on page 13.
11. Were any pages unreadable during the copy operation (see step 7)?

    No: The system is ready for the next IPL. **This ends the procedure.**

    Yes: Perform an IPL from removable media and restore the Licensed Internal Code (see Utilities to Install and Restore Licensed Internal Code).

    Note: Some objects may be damaged. The customer may have to load the damaged objects again.

    See the Backup and Recovery book.

    This ends the procedure.
12. Perform the following to remove the failing load-source disk unit on the system:
    a. Power off the system.
    b. Find the load-source disk unit. Slide the disk unit out of the system (see Disk drive).
    c. Install the new disk unit.
13. Perform an IPL from removable media and select the option to install Licensed Internal Code and recover the configuration (see Utilities to Install and Restore Licensed Internal Code).
14. Did you get a Disk Configuration Error Report with a *Unit has incorrect logical partition configuration* warning?

    No: Continue with the next step.

    Yes: You have logical partitions that need to be recovered. Go to Restoring profile data and then continue with the next step.

15. The system ASP will be cleared because customer data was not recoverable. Recover the configuration to disk unit 1 in the system unit by performing the following:
    a. Select **Use Dedicated Service Tools** (DST) from the IPL or Install the System display.
    b. Enter the password 22222222. If this password is not valid, ask the customer for the correct password.
    c. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery**.
    d. Select **Recover configuration option** on the Work With Disk Unit Recovery display. This option assembles the system configuration information on disk unit 1 in the system unit.

       Notes:

       1) A warning message will appear stating that recovering the configuration destroys all system data.
       2) The recover configuration function cannot be performed on a system with only one disk unit. A message may appear stating that your request to recover the configuration was not successful.

    e. Continue with the next step.
16. The ASP to which the failing disk unit was assigned is cleared. The customer should do the following:

    - If the disk unit you exchanged is in ASP 1, have the customer see the Backup and Recovery book. You must restore the operating system and all customer data.
    - If the disk unit is in a user ASP (ASP 2 through ASP 16), data in the ASP is lost. See the Backup and Recovery book. **This ends the procedure.**
17. Is the failing unit missing from the configuration?

    No: Find another disk unit on the system, other than the load-source disk unit. Continue with the next step.

    Yes: Go to step 26 on page 16.
18. Perform the following to install a new disk unit on the system:
    a. Power off the system. Slide the disk unit that you found in the previous step of this procedure out of the system (see Disk drive). Be very careful with the disk unit—you will install it again when the repair actions to the failing disk unit are complete.
    b. Install the new disk unit.
19. Perform an IPL to DST (see Performing an IPL to DST). Does the Use Dedicated Service Tools (DST) display appear?

    Yes: Continue with the next step.

    No: Repeat step 1 on page 13.
20. Perform the following to format and initialize the disk drive you installed in step 18:
    a. From the Use Dedicated Service Tools (DST) display, select **Work with disk units** > **Work with disk unit recovery** > **Disk unit problem recovery procedures** > **Initialize and format disk unit**.
    b. Select the unconfigured disk unit that you installed in step 18 as the unit to work with.
    c. Press F10 to verify the initialization and formatting. The initialization and formatting may take 30 minutes or longer to complete.
    d. Return to the Work with Disk Unit Recovery display.
21. Perform the following to copy data from the failing disk drive to the disk drive you installed in step 18:
    a. Select **Copy disk unit data** on the Work with Disk Unit Recovery display.
    b. Select the failing unit as the unit to copy.
    c. Select the unconfigured unit that you installed in step 18 as the unit to copy to.

d. The console displays the percentage of the data copied. Write down the number of unreadable pages if it displays; you will use it later in this procedure.
e. Wait until the status of the copy is *Complete*. Continue with the next step.

Note: Customer data is not recoverable if one of the following occurs:

- The copy operation does not complete.
- A large number of unreadable pages must be copied from the disk unit.

22. Perform the following to remove the failing disk unit from the system:
    a. Power off the system.
    b. Find the failing disk unit. Slide the disk unit out of the system.
23. Perform the following to move the new disk unit into the location that held the failing disk unit:
    a. Remove the new disk unit from the location you found in step 17 on page 15. Be very careful with the disk unit—it contains sensitive data.
    b. Install the new disk unit into the location that contained the failing disk unit, which you removed in step 22.
24. Install the disk unit you removed in step 18 on page 15.
25. Were any pages unreadable during the copy operation performed in step 21 on page 15?

    No: The system is ready for the next IPL. **This ends the procedure.**

    Yes: Some objects may be damaged. The customer may have to load the damaged objects again.

    Refer the customer to the Backup and Recovery book. **This ends the procedure.**
26. Are there multiple failing disk units under the same IOA?

    No: Continue with the next step.

    Yes: Perform the following:
    a. Power off the system.
    b. Exchange the storage IOA (see Removing and replacing parts). If you do not know the part number, see Finding part locations.
    c. Go to step 1 on page 13.
27. Because the disk data was not recoverable, clear the auxiliary storage pool (ASP) to which the disk unit is assigned by doing the following:
    a. Return to the Work with Disk Units display and select **Work with disk configuration** > **Work with ASP configuration** > **Delete ASP data**.
    b. Enter **Delete** for the ASP that you recorded in step 3 on page 13, and confirm the deletion.
    c. Return to the Work with Disk Units display and select **Work with disk unit recovery** > **Replace configured unit**.
    d. On the Select Configured Unit to Replace display, select the configured disk unit to exchange.
    e. On the Select Replacement Unit display, select the replacement disk unit.
    f. Press **Enter** to confirm the replace operation (this operation takes 10 to 15 minutes to complete).

    Attention: The auxiliary storage pool to which the disk unit is assigned was erased. The customer must restore the data to the auxiliary storage pool. Refer the customer to the Backup and Recovery book.
28. The ASP to which the failing disk unit was assigned is cleared. The customer should do the following:

- If the disk unit you exchanged is in ASP 1, refer the customer to the Backup and Recovery book. You must restore the operating system and all customer data. **This ends the procedure.**

- If the disk unit is in a user ASP (ASP 2 through ASP 16), data in the ASP is lost. See the Backup and Recovery book. **This ends the procedure.**

Copy the contents of the LIC log

1. From the Use Dedicated Service Tools (DST) display, select **Start a Service Tool** > **Licensed Internal Code log**.
2. Select either:
   - Dump entries to tape from the LIC log
   - Dump entries to diskette from the LIC log
3. At the bottom of the display, type a **3** to dump entry header and complete entry, and press **Enter**.
4. Follow the on-screen prompts. When the copy of the LIC log finishes, a message appears indicating that the dump (copy) completed. Press **Enter**. Then select **End Licensed Internal Code**. **This ends the procedure.**

   Attention: The file does not close until you select **End Licensed Internal Code**. If you remove the tape or diskette before selecting this option, do **not** use the information that is on the tape or diskette.

System reference code (SRC) address formats

Use this procedure to determine the IOP, IOA, or device address from either a control panel or a console display.

1. Was the SRC and addressing information obtained either from a control panel display, the Main Storage Dump Manager display, or the HMC Partition Properties Reference Code words display?

   No: Continue with the next step.

   Yes: Addressing information is in the Bus-Bus-Bus-Bus/Card-card/board-board (BBBBCcbb) format as follows:

   – If characters 7 and 8 of the top 16-character line of function 12 (word two) are 60:
     - The IOP address is characters 1-8 of the bottom 16-character line of function 12 (word four) in the format ″BBBBCcbb″.
     - The device address is characters 9-16 of the bottom 16-character line of function 12 (word five) in the format ″abcd efgh″.

   – If characters 7 and 8 of the top 16-character line of function 12 (word two) are 13, 17, 27, or 29:
     - The IOP address is characters 9-16 of the top 16-character line of function 12 (word three) in the format ″BBBBCcbb″.
     - The device address is characters 1-8 of the bottom 16-character line of function 12 (word four) in the format ″abcd efgh″.

   – If characters 7 and 8 of the top 16-character line of function 12 (word two) are 62:
     - The IOP address may be characters 9-16 of the top 16-character line of function 13 (word seven) in the format ″BBBBCcbb″.
     - The device address may be characters 1-8 of the top 16-character line of function 13 (word six) in the format ″abcd efgh″.

   Go to step 9 on page 19.

2. Are you using the Service Focal Point on the HMC?

   No: Continue with the next step.

   Yes: Go to the i5/OS partition with the problem and use the Service Action Log (SAL) to find the entry related to this problem (see Using the Service Action Log), and then go to step 7 on page 19.

3. Are you using the Service Action Log (SAL)?

   No: Continue with the next step.

   Yes: Go to step 7 on page 19.

4. Are you using i5/OS communication-diagnostic panels that are displayed by the commands VFYCMN, WRKPRB, or ANZPRB?

   Yes: Go to step 11 on page 20.

   No: Continue with the next step.

5. Addressing information is in the Bus/Board/Card format.

   Note: This format shows the system bus number in decimal form.

   If no address information is available in the console error message, check the Product Activity Log (PAL) entry that is associated with the console error message. Below is an example of a PAL display for a storage device. Other devices (for example, workstations or communications) have similar displays. For more information about the PAL, see Product Activity Log in the Service functions.

Figure 1. Product Activity Log display example

```
+-------------------------------------------------------------------------------+
|Display Address Information for Resource                                       |
|                                                                               |
|                                    Serial                   Resource          |
|Name            Type       Model    Number                   Name              |
|STORAGE         6718       050      83-00834                 DD001             |
|                                                                               |
|Physical Location:                                                             |
|  U7879.001.10ABCDE-P3-D3                                                      |
|                                                                               |
|                                                                               |
|                                                                               |
|Logical Address:                                                               |
|PCI Bus:                           Storage:                                    |
|System Bus  . . . . . :      3      I/O Adapter . . . . . :     2              |
|System Board  . . . . . :    0      I/O Bus . . . . . . . :     1              |
|System Card . . . . . :     32      Controller. . . . . . . :   4              |
|                                    Device  . . . . . . . :     0              |
|                                                                               |
+-------------------------------------------------------------------------------+
```

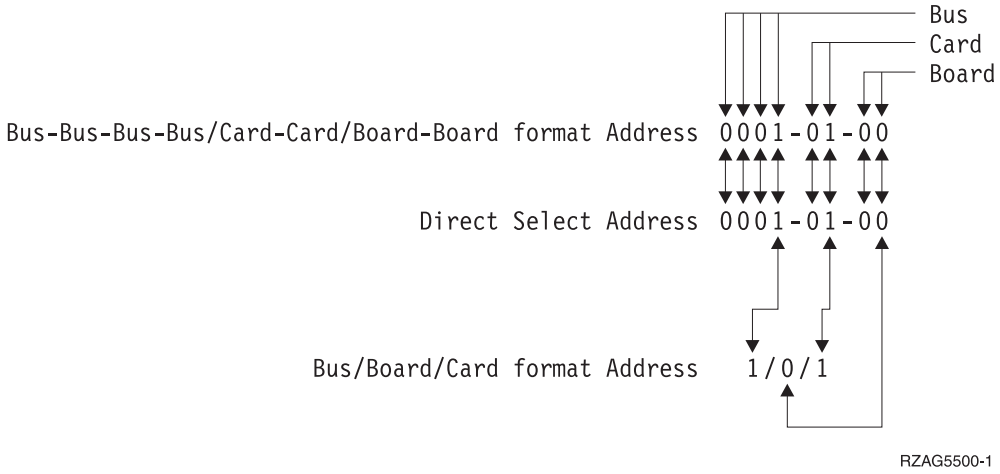
In the above example, the contents of ″Storage″ are defined as follows.

Table 1. Storage definitions

Reference	Description
I/O Bus	This is the SCSI bus to which the device is connected.
I/O Adapter	This is the adapter that the I/O bus connects to on the I/O processor.
Controller	This is the logical controller for the addressed device.
Device	This is the *logical* device that is attached to the *logical* device controller.

6. Use the figure below to understand how addresses in the Bus/Board/Card format relate to the Bus-Bus-Bus-Bus/Card-Card/Board-Board format. You can also use it to understand how addresses in the Bus/Board/Card format relate to the direct select addresses used in Finding part locations.

Figure 2. Format conversion



Note: When converting from Bus/Board/Card format to Bus-Bus-Bus-Bus/Card-Card/Board-Board format, the numbers must be converted from Decimal to Hexadecimal.

Go to step 10 on page 20 for IOA and device address information.

7. Display the FRU details for the problem that you are attempting to fix. The location information in the field-replacable unit detail is only available for IOPs, IOAs, and devices.

   Is the FRU an IOP, IOA, or device, *and* is there location information in the Location field of the display?

   No: Continue with the next step.

   Yes: Use the location information and return to the procedure that sent you here. **This ends the procedure.**

8. There is no location information in the Location field. Are there additional words displayed at the top of the screen?

   No: Go to Hexadecimal Product Activity Log data in Service functions to obtain the address information. Then return here and continue with the next step.

   Yes: Use the additional words to find the address information:

   – If characters 7 and 8 of word two are 60:
     - The IOP address is word four in the format ″BBBBCcbb″.
     - The device address is word five in the format ″abcd efgh″.
   – If characters 7 and 8 of word two are 13, 17, 27, or 29:
     - The IOP address is word three in the format ″BBBBCcbb″.
     - The device address is word four in the format ″abcd efgh″.
   – If characters 7 and 8 of word two are 62:
     - The IOP address may be word seven in the format ″BBBBCcbb″.
     - The device address may be word six in the format ″abcd efgh″.

   Continue with the next step.

9. The BBBBCcbb format is the hexadecimal direct select address of a card location in the system unit. The format definition is:

   • BBBB—System Bus
   • Cc—System Card
   • bb—System Board

   Continue with the next step for IOA and device address information.

10. Unit (Device) Address Definitions are explained in an ″abcd efgh″ format. For example, if the unit address is 0001 00FF, the address relates to the ″abcd efgh″ format as follows:

    Figure 3. Example of Unit (Device) Address definitions

    ```
     0 0 0 1   0 0 F F
    (a b c d   e f g h)
    ```

    The characters ″abcd efgh″ can have different meanings, depending on the subsystem that reports the problem. However, they define the information that is contained in the unit (device) address as follows.

Table 2. Character definitions

Disk, tape, or optical	
a	I/O adapter
b	I/O bus
cd	Controller
ef	Device
gh	FF
Communications	
a	I/O bus
b	Adapter
c	0
d	Port
e	0
f	Channel
GH	FF
Workstation	
a	I/O Bus
b	Adapter
cd	Port
e	0
f	Device
g	0
h	Session

Note: If the failing item or procedure that sent you here indicates that the I/O adapter is the failing item, but you only have a device address, convert the device address into an I/O adapter address by making the last 7 digits FFFFFFF so that the address becomes xFFFFFFF, where x is the I/O adapter number.

Note: If the unit (device) address appears as FFFF FFFF, the address cannot be determined.
This ends the procedure.

11. i5/OS communication-diagnostic panels that are displayed by the commands VFYCMN, WRKPRB, and ANZPRB use the following address format:

    ```
    x1  x2  x3x4
    ```

Table 3. Decimal address values

Value	Description
x1 = System bus	The one, two, or three digit decimal representation of the hexadecimal **Bus** value of the **Bus-Bus-Bus-Bus/Card-Card/Board-Board format Address** at the top of Figure 2. Format conversion.
x2 = System board	The one or two digit decimal representation of the hexadecimal **Board** value of the **Bus-Bus-Bus-Bus/Card-Card/Board-Board format Address** at the top of Figure 2. Format conversion.
x3 = System card	The one or two digit decimal representation of the hexadecimal **Card** value of the **Bus-Bus-Bus-Bus/Card-Card/Board-Board format Address** at the top of Figure 2. Format conversion.
x4 = Adapter location	The one or two digit decimal representation of the hexadecimal **b Adapter** value of the **Communications unit address** value in step **9** (See 10 on page 20).

12. Return to the procedure that sent you here. **This ends the procedure.**

    Note: See Hardware SRC formats in Service functions for more formatting information.

Storage I/O card modes and jumpers

The 2748 and 2778 I/O cards can run in either compression mode or enhanced mode.

- **Compression Mode:** Compression mode should only be used when you want to run Integrated Hardware Disk Compression. In compression mode, the write cache size is 4 MB.
- **Enhanced Mode:** Enhanced mode has an enhanced write cache size. In enhanced mode, the write cache size for the 2748 I/O card is 26MB, and the maximum compressed write cache size for the 2778 I/O card is 104MB. Enhanced mode also provides support for Extended Adaptive Cache (by attachment of a read cache device) and Extended Adaptive Cache Simulator.

The following subtopics are included here:

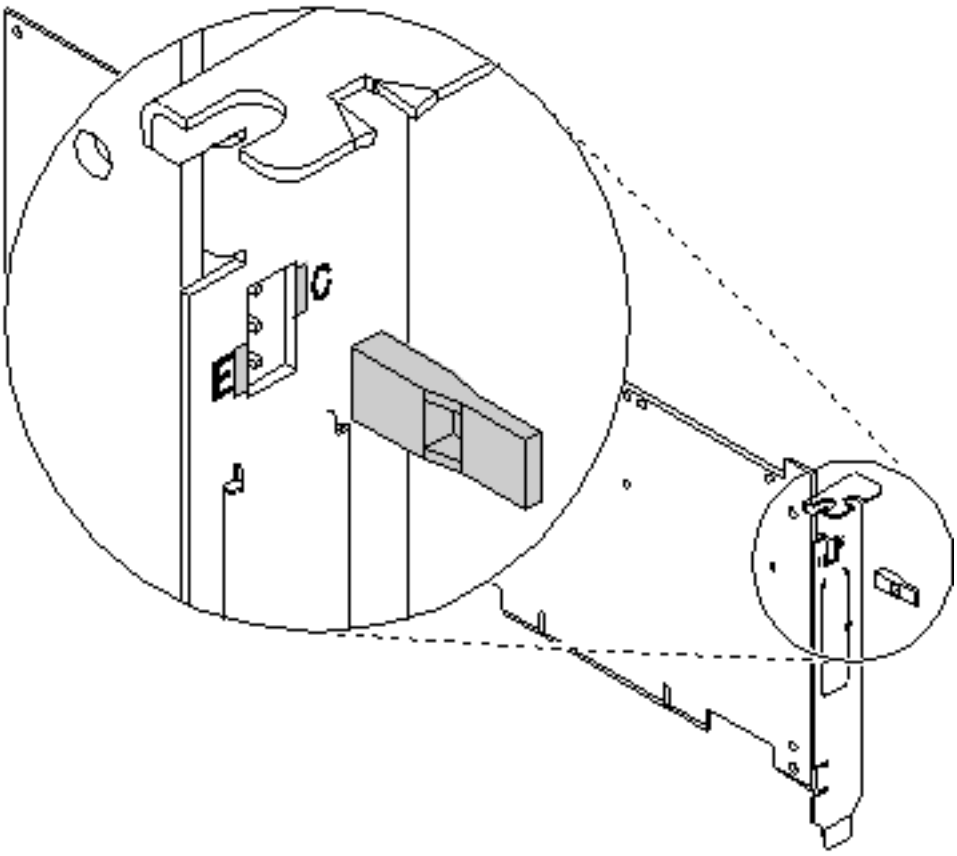
- "Setting or changing the mode of an I/O card."
- When an error regarding the mode of the storage I/O card appears, the error message indicates whether the jumper is missing or overridden.
  - If the error message is CPPEA20, the I/O card has overridden the mode set by the jumper. See "Mode jumper has been overridden" on page 22.
  - If the error message is CPPEA21, the I/O card has detected that the jumper is missing. See "Mode jumper is missing" on page 23.

Setting or changing the mode of an I/O card

The 2748 and 2778 I/O cards support two modes: compression and enhanced. The rear of the I/O card is marked with a **C**, indicating compression mode, and an **E**, indicating enhanced mode. Three pins on the rear of the I/O card determine the mode of the card, depending on which of the pins have a jumper placed on them.

The jumper may be moved at any time, but changes only take effect during a system IPL. Refer to the illustration below while changing the mode jumper.

Figure 1. Changing the mode jumper



1. Power off the system, ensuring that no jobs are currently processing (see Powering on and powering off).
2. Choose from the following options:
   - To set the mode of the card to compressed (**C**), place the jumper on the top and middle pins.
   - To set the mode of the card to enhanced (**E**), place the jumper on the middle and bottom pins.
3. Select the IPL type and mode. See IPL type, mode, and speed options for details.
4. Power on the system.

For information on disk compression, see the "Choose compression type" information in the Backup and Recovery book.

Mode jumper has been overridden

The error message `CPPEA20` appears when the mode jumper has been overridden. This is due to cache data that is in a conflicting mode.

1. To begin correcting this error, examine the mode jumpers in the rear section of the storage I/O card.

   Note: The mode jumper is accessible without requiring the removal of the I/O card.
2. Choose from the following options:
   - If the mode jumper is not in the desired position, follow the steps in "Setting or changing the mode of an I/O card" on page 21.
   - If the mode jumper is in the desired position and any other I/O card or device reference codes occurred at about the same time as this error, contact your service representative.
   - If the mode jumper is in the desired position and no other I/O card or device reference codes occurred at about the same time as this error, then power the system down normally and IPL. See Powering on and powering off. **This ends the procedure.**

Mode jumper is missing

The error message CPPEA21 appears when the mode jumper is missing from the storage I/O card.

1. Locate the jumper.
2. Power off the system. See Powering on and powering off.
3. Install the jumper in the correct position. See "Setting or changing the mode of an I/O card" on page 21.
4. Power on the system. **This ends the procedure.**

Logical partitions

The procedures in this topic will help you with the following:

"Determining if the system has logical partitions"

"Determining if the system has guest partitions"

"Determining the release level of a guest partition"

"Determining the hosting partition of a guest partition"

Determining if the system has logical partitions

This procedure will help you determine if the system has logical partitions.

1. Is the system managed by an HMC?

   Yes: Continue with the next step.

   No: You must have an HMC to have logical partitions. Return to the procedure that sent you here. **This ends the procedure.**

2. Determine if the system has multiple logical partitions by performing the following from the HMC:
   a. Expand the **Server and Partition** folder in the Navigation area.
   b. Click the **Server Management** icon.
   c. Click the plus (+) sign next to the name of the managed system you are working with. Each partition on the system will be listed underneath the managed system you expanded.

   Are there more than one logical partitions listed?

   No: The system does not have multiple logical partitions. Return to the procedure that sent you here. **This ends the procedure.**

   Yes: The system has multiple logical partitions. Return to the procedure that sent you here. **This ends the procedure.**

Determining if the system has guest partitions

Guest partitions are not supported on these models. Return to the procedure that sent you here.

Determining the release level of a guest partition

Guest partitions are not supported on these models. Return to the procedure that sent you here.

Determining the hosting partition of a guest partition

Guest partitions are not supported on these models. Return to the procedure that sent you here.

Load-source disks and alternate IPL devices

If you have a system configuration list that shows the load-source disk unit and the alternate IPL device, use that information. If not, use the following information and, when found, make a note of the locations. See Finding part locations for details.

Choose from the following:

- "Finding the load-source disk on systems without mirrored protection"
- "Finding the load-source disk on systems with mirrored protection"
- "Performing an alternate IPL"

Finding the load-source disk on systems without mirrored protection

The load source disk is disk unit 1 in the system unit.

Finding the load-source disk on systems with mirrored protection

Definitions:

- **Local load source:** A disk unit that is used as the source for IPL data.
- **Remote load source:** A backup load source disk unit that is only used as the source for IPL data when the local load source is not operational.

For systems in which both of the mirrored load source disk units are local load sources:

The system can use either disk as its source for IPL data. The disk that first reports to the service processor is the one that is used. The system starts the IPL with this device and later synchronizes the second load source disk with the first.

If the first load source disk fails after the Licensed Internal Code determines that the system has mirrored protection, the Licensed Internal Code performs the IPL by using the second load source disk.

If the first load source disk fails before the Licensed Internal Code determines that the system has mirrored protection, the IPL stops with a system reference code (SRC) displayed.

If the system starts the IPL on a load source disk that contains data which is back level compared to the data on the other load source, the Licensed Internal Code attempts to start the IPL from the second load source disk. If the second attempt fails, the IPL stops with an SRC displayed.

For systems in which one of the mirror load source disk units is a local load source, and one load source is a remote load source:

The system starts the IPL from the local load source. In a later step of the IPL, the system synchronizes the remote load source disk with data from the local load source disk unit. If that local loadsource device is not operational, the remote load source disk unit is used as the source for IPL data.

Finding the load-source disk

When the system auxiliary storage pool (ASP1) has mirrored protection, the system has two disk units that are load source disks. Use the Work with disk units option under Dedicated Service Tools (DST) or System Service Tools (SST) to display the configuration.

Performing an alternate IPL

The process of performing an IPL from removable media is an alternate, or type *D*, IPL. The device that contains the IPL media is the alternate IPL device. The alternate IPL device is attached to the system either internally or externally.

In almost all cases the HMC is used to select the device that will be used for the alternate IPL (see Alternate restart device in the Partitioning for i5/OS topic). If the alternate IPL device has not been configured by using the HMC or by a previous alternate IPL, see Default search sequence for the alternate IPL device below.

Default search sequence for the alternate IPL device

The system attempts an IPL from the first alternate IPL device it finds that is ready and contains IPL media.

Note: Once the system has successfully performed an alternate IPL, the Virtual Service Processor (VSP) will remember the address of the device and use it for any subsequent alternate IPLs until either the HMC is used to select a different alternate IPL device or the alternate IPL fails. Once an alternate IPL fails the VSP will go back to using the default search sequence.

The following IOA slot will be used:

- For model 520: bus 3, slot 005
- For models 550 and 9124-720: bus 3, slot 004
- For model 570: bus 3, slot 007

The following search sequence is used to search for an alternate IPL device attached to the IOA:

1. Device attached to SCSI bus 0 with a controller address of 7 (SCSI address 0).
2. Device attached to SCSI bus 0 with a controller address of 6 (SCSI address 1).
3. Device attached to SCSI bus 0 with a controller address of 5 (SCSI address 2).

If the system cannot find a device to use as the alternate IPL device, it displays a reference code on the control panel.

Note: The reference code that is displayed is for the most severe error that is found during the search sequence for the alternate IPL device. There may not be an association between the error and the alternate IPL device that you are using. Before using the displayed reference code to analyze the problem, ensure that the alternate IPL device is ready and contains the correct IPL media.

External device addressing

The external alternate IPL device must have a controller address of 7, 6, or 5. For most devices, the controller comes with the address preset to 7, and you cannot alter it. For devices that have changeable addresses, use the following information:

For 34xx, 35xx, and type 7208 model 342 tape devices you must set the SCSI address to 0, 1, or 2. For an IBM 9427 8mm tape cartridge library, you must set the tape library address for the drive that is used as the alternate IPL device to 0, 1, or 2.

For the location of the address switch on external devices, see the information in the device service manual.

Reclaiming IOP cache storage

Use this procedure to reclaim IOP cache storage.

1. If you are not already using Dedicated Service Tools, perform an IPL to DST. See Performing an IPL to DST for details. If you cannot perform a type A or B IPL, perform a type D IPL from removable media.

   Did you get to DST with a Type D IPL?

   - **No**: Continue with the next step.
   - **Yes**: Perform the following:
     a. Select **Work with disk units** > **Reclaim IOP cache storage**.
     b. Follow the on-line instructions to reclaim cache storage. The system will automatically perform an IPL to a Disk Configuration Attention Report or a Disk Configuration Warning Report display. Select the option to display the report. Because the Reclaim Cache Storage was selected after a D-IPL, the system will now require another Reclaim Cache Storage to be performed.

2. Select **Work with disk units** > **Work with disk unit recovery** > **Reclaim IOP Cache Storage**.
3. Follow the on-line instructions to reclaim cache storage. Depending on the reason for performing the Reclaim IOP Cache procedure, there may be a message requiring the ASP be cleared before performing this option, or a message stating the number of lost sectors.

   Note: If there are lost sectors, some objects may be damaged. The customer may have to load the damaged objects again. Refer the customer to the Backup and Recovery book.

When the IOP performs a Reset/Reload, if there is a storage IOA attached that is running the local load source, Cxxx xxxx codes will be displayed in the system control panel. The DST console may then have a blank screen with 01B displayed on the system control panel for up to 15 minutes before it is restored.
This ends the procedure.

Working with AIX diagnostics

Working with AIX diagnostics is divided into three topics.

Use "General AIX diagnostic information" on page 28 when you need to refer to information on the following subtopics:

- AIX operating system message files
- Firmware and microcode
- CEREADME file
- CE login
- Automatic diagnostic tests
- CPU and memory testing and error log analysis
- Diagnostic programs
- Periodic diagnostics
- Automatic error log analysis (diagela)
- Log repair action
- System fault indicator and system identify indicator
- Array bit steering
- Running diagnostics on the native serial port on a full machine partition with a HMC attached
- Enhanced I/O error handling

Use "Loading the AIX online diagnostics or the @server standalone diagnostics" on page 37 when you need to reference information on the following subtopics:

- Standalone and online diagnostic operating considerations
- Online diagnostics mode of operations
- Standalone diagnostic operation
- General information about multiple systems
- Determining system architecture
- high-availability SCSI
- Diagnostic summary
- Diagnostics tasks and resources
- PCI SCSI RAID descriptions and diagnostic procedures

Use "AIX tasks and service aids" on page 44 when you need to reference information on the following tasks or service aids:

- 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 (RSPC)
- Configure Ring Indicate Power-On Policy
- Configure Service Processor (RSPC)
- 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 Multipath I/O (MPIO) Device Configuration
- 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
- Identify Indicators
- Identify and Remove Resource Task (See ″Hot Plug Task″ for AIX 4.3.3.10 or higher)
- Identify and System Attention Indicators
- Local Area Network Analyzer
- Log Repair Action
- Periodic Diagnostics
- PCI SCSI Disk Identify Array Manager
- PCI RAID Physical Disk Identify
- Process Supplemental Media
- Run Diagnostics
- Run Error Log Analysis
- Run Exercisers
- Save or Restore Hardware Management Policies
- Save or Restore Service Processor Configuration (RSPC)
- SCSI Bus Analyzer
- SCSI RAID Physical Disk Status and Vital Product Data

- 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
- Update System Flash (RSPC)
- 7135 RAIDiant Array Service Aids
- 7318 Serial Communication Network Server

General AIX diagnostic information

Information in this section is common to all system units. Any service information or diagnostic procedure that is specific to a certain system unit or device is in the operator guide or service guide for that system unit or device.

AIX Operating System Message Files

English is the default language displayed by the diagnostic programs when run from disk. If you want to run the diagnostic programs in a language other than English you must install on the system the AIX operating system message locale fileset for the desired language you want displayed.

Firmware and Microcode

Detailed scenarios that describe how to identify firmware and microcode levels on your server, and updating firmware and microcode on your server, can be found in Getting fixes.

There are several types of firmware used by the system:
- Power subsystem firmware (if applicable)
- Service power control network (SPCN) firmware (if applicable)
- Service processor firmware (if applicable)
- System firmware

The following types of microcode are used by the system:
- Adapter microcode
- Device microcode

If an HMC is attached to the server, the HMC should be used to manage the server's firmware and microcode levels. To manage the server's firmware and microcode levels using the HMC GUI, see HMC graphical user interface.

If an HMC is not attached to the server, AIX diagnostic tasks can be used to display device and adapter microcode levels as well as update device and adapter microcode. AIX diagnostic tasks also provide the capability to update firmware.

To determine the level of server firmware, and device and adapter microcode, use the Display Microcode Level task in AIX diagnostic service aids. This task presents a list of resources that are currently installed and supported by this task; you then select the resource whose microcode level you with to check. The **lsmcode** command and the **diag** command can also be used to display the firmware and microcode levels of individual entities in the system from the AIX command line; for additional information, refer to Display Microcode Level. For adapters and devices not supported by this task, refer to the manufacturer's instructions to determine the microcode levels.

Use the Update and manage system flash task to update a server's firmware. When the flash update is complete, the server automatically reboots. Refer to Getting fixes for detailed scenarios that explain how to use the update and manage system flash task.

Use the Download microcode service aid on systems running AIX 5.2.0.30 or later to update the microcode on adapters and devices. For details on updating adapter and device microcode, refer to Getting fixes.

For systems that are running only Linux, the stand-alone diagnostics booted from CD-ROM or a NIM server contain service aids that can be used to update most system flash, adapter and device microcode.

CEREADME File

A CEREADME (CE readme) file is available on all diagnostic media. This file may contain information such as:

- Errata information for the service guides
- Service hints for problems
- Diagnostic information that may not be included in service guides
- Other pertinent (usually release-specific) information

The CEREADME file is helpful in describing differences in diagnostics between the current version and the preceding version.

You can view the CEREADME file by using the Service Hints service aid after the diagnostics are loaded. Also, you can read the file directly from the disk using the AIX **pg** command to display **/usr/lpp/diagnostics/CEREADME**. The CEREADME file can be copied or printed using the normal commands. For information about using the service hints, refer to "Display Service Hints" on page 59.

Printing the CEREADME file from disk

You can print the CEREADME file from disk using the **cat** command. The path to this file is as follows: **/usr/lpp/diagnostics/CEREADME**

A copy of this file should be printed and stored with the Service Information. **lp0** is normally the printer attached to the parallel port. If a printer is attached to the parallel port and is considered as **lp0**, the command for printing the file is as follows:

```
cat /usr/lpp/diagnostics/CEREADME > /dev/lp0
```

Printing the CEREADME file from a source other than disk

The CEREADME file cannot be printed while diagnostics are being executed from a source other than from the disk. The file can be printed on a system when the AIX operating system is running in a normal user environment. The procedure involves copying the file from the diagnostic media to a temporary file on disk, printing the file, and then deleting the file from disk. Check for directory **/tmp/diag**. To determine if this directory already exists, enter:

```
cd /tmp/diag
```

If the directory does not exist, the message `/tmp/diag: not found` displays. *Do not* attempt to print the CEREADME file if this message is not displayed. To print the CEREADME file, choose the appropriate section below and follow the steps listed.

Printing the CEREADME file from CD-ROM

Insert the diagnostic CD-ROM disc into the CD-ROM drive, and then enter the following commands:

```
mkdir /tmp/diag
mount -o ro -v cdrfs /dev/cd0  /tmp/diag
cd /tmp/diag/usr/lpp/diagnostics
cat CEREADME > /dev/lp0
cd /tmp
unmount /dev/cd0
```

The CEREADME file prints on **lp0**, which is the printer normally attached to the parallel port. If this file is not the same as the CEREADME file on the disk, a copy of this file should be printed and stored with the Service Information.

CE Login

CE login enables a user to perform operating system commands that are required to service the system without being logged in as a root user. CE login must have a role of **RunDiagnostics** and a primary group of **system**. This enables the user to:

- Run the diagnostics including the service aids, such as hot plug tasks, certify, format, and so forth.
- Run all the operating system commands run by **system** group users.
- Configure and unconfigure devices that are not busy.

In addition, CE login can have **shutdown** group enabled to allow:

- Use of the Update System Microcode service aid.
- Use of shutdown and reboot operations.

To use CE login, ask the customer to create a unique user name and configure these characteristics for that name. (Refer to the Users and Groups section of the *AIX 5L Version 5.1 System Management Guide: Operating System and Devices*.) After this is set up, you will need to obtain the user name and password from the customer to log in with these capabilities. The recommended CE login user name is **qserv**.

Automatic diagnostic tests

All automatic diagnostic tests run after the system unit is turned on and before the AIX operating system is loaded.

The automatic diagnostic tests display progress indicators (or checkpoints) to track test progress. If a test stops or hangs, the checkpoint for that test remains in the display to identify the unsuccessful test. The descriptions of these tests are contained in AIX IPL progress codes.

Power-on self-test

Power-On Self-Test (POST) programs check the devices needed to accomplish an initial program load. The POST also checks the memory, and portions of the central electronics complex, common interrupt handler, and the direct memory access (DMA) handler.

Configuration program

The configuration program determines the features, adapters, and devices are present on the system. The configuration program, which is part of the AIX operating system, builds a configuration list that is used by the diagnostic programs to control which tests are run during system checkout.

On systems running AIX, the configuration program displays numbers between `2E6` through `9FF` and `2300` through `27FF` in the operator panel display (if present). Refer to AIX Diagnostic Numbers and Location Codes AIX IPL Progress codes for a listing of program actions associated with displayed numbers. On systems running logical partitions, `LPAR` displays in the operator panel (if present) after the hypervisor (the system firmware that controls the allocation of resources) is loaded. When a partition running AIX is subsequently booted, the configuration codes display on the virtual operator panel on the HMC.

Devices attached to serial and parallel ports are not configured. The Dials and Lighted Program Function Keys (LPFKs) can be tested from online diagnostics after they are manually configured. No other device attached to the serial and parallel ports is supported by the diagnostics.

CPU and memory testing and error log analysis

Except for the floating-point tests, all CPU and memory testing on the system units are done by POST and BIST. Memory is tested entirely by the POST. The POST provides an error-free memory MAP. If POST cannot find enough good memory to boot, it halts and displays an error message. If POST finds enough good memory, the memory problems are logged and the system continues to boot.

If any memory errors were logged, they are reported by the base system or memory diagnostics, which must be run to analyze the POST results.

The CPU and memory cannot be tested after the AIX diagnostics are loaded; however, they are monitored for correct operation by various checkers such as processor runtime diagnostics. Exercisers can be run on memory and the floating point unit of the processor to help troubleshoot intermittent problems with those functions (see Run exercisers). If the threshold value of correctable errors is reached, an error is logged in the error log.

Single-bit memory errors are corrected by ECC (Error Checking and Correction) on systems equipped with ECC memory.

Diagnostic programs

This section provides overview of the various diagnostic programs.

Diagnostic controller

The diagnostic controller runs as an application program on the AIX operating system. The diagnostic controller carries out the following functions:

- Displays diagnostic menus
- Checks availability of needed resources
- Checks error log entries under certain conditions
- Loads diagnostic application programs
- Loads task and service aid programs
- Displays test results

To test an adapter or device, select the device or adapter from the diagnostic selection menu. The diagnostic controller then loads the diagnostic application program for the selected device or adapter.

The diagnostic application program loads and runs test units to check the functions of the device or adapter.

The diagnostic controller checks the results of the tests done by the diagnostic application and determines the action needed to continue the testing.

The amount of testing that the diagnostic application does depends on the mode (service, maintenance, or concurrent) under which the diagnostic programs are running.

Error log analysis

When you select **diagnostics** or **advanced diagnostics**, the diagnostic selection menu displays (other menus may display before this menu). This menu allows you to select the purpose for running diagnostics.

When you select the **problem determination** option, the diagnostic programs read and analyze the contents of the error log.

Note: Most hardware errors in the operating system error log contain *sysplanar0* as the resource name. The resource name identifies the resource that detected the error; it does not indicate that the resource is faulty or should be replaced. Use the resource name to determine the appropriate diagnostic to analyze the error.

If the error log contains recent errors (approximately the last 7 days), the diagnostic programs automatically select the diagnostic application program to test the adapter or device that the error was logged against.

If there are no recent errors logged or the diagnostic application program runs without detecting an error, the diagnostic selection menu is displayed. This menu allows you to select a resource for testing.

If an error is detected while the diagnostic application program is running, the A PROBLEM WAS DETECTED screen displays a Service Request Number (SRN).

Note: After a FRU is replaced based on an error log analysis program, the error log entries for the problem device must be removed or the program may continue to indicate a problem with the device. To accomplish this task, run the **errclear** command from the command line, or use System Management Interface Tool (SMIT) to select **Problem Determination/Error Log/Clear the Error Log**. Fill out the appropriate menu items.

Enhanced FRU isolation

The diagnostics provide enhanced Field Replaceable Unit (FRU) isolation by automatically selecting associated resources. The typical way in which diagnostics select a resource is to present a list of system resources, and you are then asked to select one. Diagnostics begin with that same type of selection.

If the diagnostic application for the selected resource detects a problem with that resource, the diagnostic controller checks for an associated resource. For example, if the test of a disk drive detects a problem, the diagnostic controller tests a sibling device on the same controller to determine if the drive or the controller is failing. This extra FRU isolation is apparent when you test a resource and notice that the diagnostic controller continues to test another resource that you did not select.

Advanced diagnostics function

The advanced diagnostics function are normally used by a service representative. These diagnostics may ask you to disconnect a cable and install a wrap plug.

The advanced diagnostics run in the same modes as the diagnostics used for normal hardware problem determination. The advanced diagnostics provide additional testing by allowing the service representative to do the following:

- Use wrap plugs for testing.
- Loop on a test (not available in concurrent mode) and display the results of the testing.

Task and service aid functions

If a device does not show in the test list or you think a device's diagnostic package 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.

Tasks and service aids provide a means to display data, check media, and check functions without being directed by the hardware problem determination procedure. Refer to AIX tasks and service aids for information and procedures about tasks and service aids.

System checkout

The system checkout program uses the configuration list generated by the configuration procedure to determine which devices and features to test. These tests run without interaction. To use system checkout, select **All Resources** on the resource selection menu.

Missing resource description

In diagnostics version earlier than 5.2.0, missing devices are presented on a missing resource screen. This happens as a result or running **diag -a** or by booting online diagnostics in service mode.

In diagnostics version 5.2.0 and later, missing devices are identified on the diagnostic selection screen by an uppercase `M` preceding the name of the device that is missing. The diagnostic selection menu is displayed anytime you run the diagnostic routines or the advanced diagnostics routines. The diagnostic selection menu can also be entered by running **diag -a** when there are missing devices or missing paths to a device.

When a missing device is selected for processing, the missing resource menu will ask whether the device has been turned off, removed from the system, moved to a different physical location, or if it is still present.

When a single device is missing, the fault is probably with that device. When multiple devices with a common parent are missing, the fault is most likely related to a problem with the parent device.

The diagnostic procedure may include testing the device's parent, analyzing which devices are missing, and any manual procedures that are required to isolate the problem.

Missing path resolution for MPIO resources

Diagnostics also identifies a multipath I/O device that has multiple configured paths, all of which are missing as a missing device. If some, but not all, paths to a multipath I/O device are missing, then diagnostics identifies those paths as missing. In such an instance, an uppercase `P` displays in front of the multipath I/O device.

When a device with missing paths is selected from the **diagnostic selection** menu, the **missing path selection** menu displays showing the missing paths for the device. The menu requests the user to select a missing path for processing. If the device has only one missing path, then the selection menu is bypassed. In either case, a menu is displayed showing the selected missing path and other available paths to the device (which may be missing or available). The menu asks if the missing path has been removed, has not been removed, or should be ignored. The procedures are as follows:

- If the **Path Has Been Removed** option is selected, diagnostics removes the path from the data base.
- If the **Path Has Not Been Removed** option is selected, diagnostics determines why the path is missing.
- If the **Run Diagnostics on the Selected Device** option is selected, diagnostics runs on the device and does not change the system configuration.

Periodic testing of the processors is enabled by default. If a problem is detected, information about the failure, such as the service request number, is posted to the system console and to the following:

1. If an error notification mailing list has been configured, information about the failure is sent to the e-mail addresses and system users in this list.
2. If there is an attached HMC, information about the failure is sent to Service Focal Point.
3. If the mailing list has not been configured and there is not an attached HMC, information about the failure is sent to all users belonging to the system group.

Periodic diagnostics are controlled by the periodic diagnostic service aid. The periodic diagnostic service aid allows a hardware resource to be tested once a day. If the resource cannot be tested because it is busy, error log analysis is performed if supported on the resource. In diagnostics version 5.1.0.15 and later, periodic diagnostics only supports testing of processors. Disk drives and system planars are no longer supported by periodic diagnostics because testing is not supported in concurrent diagnostics and coverage is provided by automatic error log analysis.

Processors that are dynamically removed from the system are also removed from the periodic test list. Processors that are dynamically added are automatically added to the periodic test list.

Periodic diagnostic reminders

Periodic diagnostic reminders are notifications about failed or deconfigured resources that are reported by firmware to the operating system. Periodic diagnostic reminder mode is run following a successful system boot and then every Tuesday at 8 a.m. Only the resources in the periodic test list are tested for failed or deconfigured status. Adding or removing a resource from the periodic test list enables or disables the periodic diagnostic reminder for that resource.

In diagnostics version 5.1.0.15 and later, periodic diagnostic reminder mode is only run for processors. Periodic diagnostic reminder mode for processors also performs testing on the processors. If a problem is detected, information about the failure, such as the service request number, is posted to the system console and to the following:

1. If an error notification mailing list has been configured, information about the failure is sent to the e-mail addresses and system users in this list.
2. If there is an attached HMC, information about the failure is sent to Service Focal Point.
3. If the mailing list has not been configured and there is not an attached HMC, information about the failure is sent to all users belonging to the system group.

Periodic diagnostics

Periodic testing of physical processors is enabled by default. If a problem is detected, information about the failure, such as the service request number, is posted to the system console and to the following:

1. If an error notification mailing list has been configured, then information about the failure is sent to the e-mail addresses and system users in this list.
2. If there is an attached HMC, then information about the failure is sent to Service Focal Point.
3. If the mailing list has not been configured and there is not an attached HMC, then information about the failure is sent to all users belonging to the system group.

Periodic diagnostics are controlled by the periodic diagnostic service aid. The periodic diagnostic service aid allows a hardware resource to be tested once a day. If the resource cannot be tested because it is busy, error log analysis is performed if supported on the resource.

In diagnostics versions at or above 5.1.0.15 or 5.2.0.0, periodic diagnostics only supports testing of processors. Disk drives and system boards are no longer supported by periodic diagnostics because testing is not supported in concurrent diagnostics, and coverage is provided by automatic error log analysis.

Processors that are dynamically removed from the system are also removed from the periodic test list. Processors that are dynamically added are automatically added to the periodic test list. Periodic diagnostics does not occur on systems or partitions that have only virtual or shared processors.

Periodic Diagnostics Reminders

Periodic diagnostic reminders are notifications about failed or deconfigured resources that are reported by firmware to the operating system. Periodic diagnostic reminder mode is run following a successful system boot and then every Tuesday at 8 a.m. Only the resources in the periodic test list are tested for failed or deconfigured status. Adding or removing a resource from the periodic test list enables or disables the periodic diagnostic reminder for that resource.

In diagnostics versions at or above 5.1.0.15 or 5.2.0.0, periodic diagnostic reminder mode is only run for physical processors. Periodic diagnostic reminder mode for processors also performs testing on the processors. If a problem is detected, information about the failure, such as the service request number, is posted to the system console and to the following:

1. If an error notification mailing list has been configured, information about the failure is sent to the email addresses and system users in this list.
2. If there is an attached HMC, then information about the failure is sent to Service Focal Point.
3. If the mailing list has not been configured and there is not an attached HMC, information about the failure is sent to all users belonging to the system group.

Periodic diagnostics reminders do not occur on systems or partitions that have only virtual or shared processors.

Automatic Error Log Analysis (diagela)

Automatic Error Log Analysis (**diagela**) provides the capability to perform error log analysis when a permanent hardware error is logged, by enabling the **diagela** program on all platforms.

The **diagela** program determines if the error should be analyzed by the diagnostics. If the error should be analyzed, a diagnostic application is invoked and the error is analyzed. No testing is done if the diagnostics determine that the error requires a service action. Instead it sends a message to your console, and either the Service Focal Point for systems with a HMC, or to all system groups. The message contains the SRN.

Running diagnostics in this mode is similar to using the **diag -c -e -d** *Device* command.

Notification can also be customized by adding a stanza to the **PDiagAtt** object class. The following example illustrates how a customer's program can be invoked in place of the normal mail message, or in addition to sending the message to the Service Focal Point when there is a HMC:

```
PDiagAtt:
     DClass = " "
     DSClass = " "
     DType = " "
     attribute = "diag_notify"
     value = "/usr/bin/customer_notify_ program $1 $2 $3 $4 $5"
     rep = "s"
```

If DClass, DSClass, and DType are blank, then the `customer_notify_program` applies for *all* devices. Filling in the DClass, DSClass, and DType with specifics causes the `customer_notify_program` to be invoked only for that device type.

After the above stanza is added to the ODM data base, problems are displayed on the system console and the program specified in the value field of the `diag_notify` predefined attribute is invoked. The following keyword is expanded automatically as arguments to the notify program:

- $1 the keyword `diag_notify`
- $2 the resource name that reported the problem
- $3 the Service Request Number
- $4 the device type
- $5 the error label from the error log entry

In the case where no diagnostic program is found to analyze the error log entry, or analysis is done but no error was reported, a separate program can be specified to be invoked. This is accomplished by adding a stanza to the **PDiagAtt** object class with an attribute = **diag_analyze**. The following example illustrates how a customer's program can be invoked for this condition:

```
PDiagAtt:
     DClass = " "
     DSClass = " "
     DType= " "
     attribute = "diag_anaylze"
     value = "/usr/bin/customer_analyzer_program $1 $2 $3 $4 $5"
     rep = "s"
```

If DClass, DSClass, and DType are blank, then the `customer_analyzer_program` applies for all devices. Filling in the DClass, DSClass, and DType with specifics causes the `customer_analyzer_program` to be invoked only for that device type.

After the above stanza is added to the ODM data base, the program specified is invoked if there is no diagnostic program specified for the error, or if analysis was done, but no error found. The following keywords expand automatically as arguments to the analyzer program:

- $1 the keyword **diag_analyze**
- $2 the resource name that reported the problem
- $3 the error label from the error log entry if from ELA, the keyword PERIODIC if from Periodic Diagnostics, or the keyword REMINDER if from a Diagnostic Reminder.
- $4 the device type
- $5 the keywords:
  - **no_trouble_found** if the analyzer was run, but no trouble was found.
  - **no_analyzer** if the analyzer is not available.

To activate the automatic error log analysis feature, log in as root user (or use the CE login) and type the following command:

```
/usr/lpp/diagnostics/bin/diagela ENABLE
```

To disable the automatic error log analysis feature, log in as root user (or use the CE login) and type the following command:

```
/usr/lpp/diagnostics/bin/diagela DISABLE
```

The **diagela** program can also be enabled and disabled using the periodic diagnostic service aid.

Log repair action

The diagnostics perform error log analysis on most resources. The default time for error log analysis is seven days; however, this time can be changed from 1 to 60 days using the **display or change diagnostic run time options** task. To prevent false problems from being reported when error log analysis is run, repair actions need to be logged whenever a FRU is replaced. A repair action can be logged by using the **log repair action** task or by running advanced diagnostics in system verification mode.

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.

System fault indicator and system identify indicator

Some systems support the system identify indicator and/or the system fault indicator.

The system identify indicator is used to help physically identify a particular system in a room. The system fault indicator is used to help physically identify a particular system that has a fault condition.

On a system that supports system fault indicator, the indicator is set to fault condition when a fault is detected. After the problem with the system is fixed, the system fault indicator should be set back to normal. This is done by using the log repair action task. For additional information, see Log repair action.

Note: This action keeps the system fault indicator from being set to the fault state due to a previous error, that has already been serviced, in the error log.

Both of these indicator functions can be managed by using the system identify indicator and system fault indicator tasks. See “System Fault Indicator” on page 80 or “System Identify Indicator” on page 80 for additional information.

Array bit steering

An advanced feature of many systems is array bit steering. The processors in these systems have internal cache arrays with extra memory capacity that can be configured to correct certain types of array faults.

This reconfiguration can be used to correct arrays for faults detected at IPL or run time. In the case of a fault detected during run time, the recoverable fault is reported with a ″Repair Disposition Pending Reboot″ indicator set. This allows diagnostics to call out a service request number that identifies the array and directs the service representative to a MAP for problem resolution that uses array bit steering. If the array bit steering cannot be used for the reported fault, then the FRU with that array is replaced.

Running diagnostics on the native serial port on a full machine partition with a HMC attached

For a full machine partition, the output of the S1 serial port is redirected, or wrapped to the virtual console window. When the S1 serial port is wrapped, the output of any command is directed from the S1 serial port to the virtual console terminal. If you close the virtual console window on the managed system, normal function is restored to the S1 serial port.

The implication of this is that the serial port wrap diagnostics may fail with a false SRN if the virtual console window on the managed system is not closed. Another method to prevent the false SRN is to unplug the HMC from its port before running the wrap tests.

After running diagnostics on the serial port, make sure that the S1 serial port is enabled for login (AIX command `chdev -l 'tty'x -a login='enable'` where x is the tty number corresponding to the S1 serial port).

Enhanced I/O error handling

Enhanced I/O Error Handling (EEH) is an error recovery strategy for errors that can occur during I/O operations on the PCI bus. Not all systems support EEH; if you get an SRN involving an EEH error, follow the action listed.

Loading the AIX online diagnostics or the @server standalone diagnostics

Use this procedure to check the server or partition for correct hardware operation after removing and replacing a part or installing a feature.

Before you begin:

- The AIX operating system must be installed on your server or the @server standalone diagnostics must be available from another source (CD or Network Installation Management (NIM) server) before you start this procedure.
- If this server is directly attached to another server or attached to a network, be sure communications with the other servers are stopped.
- This procedure requires use of all of the partition resources. No other activity can be running on the partition while you are performing this procedure.
- This procedure requires access to the server's system console which can be either a display attached to a graphics adapter or an HMC.

1. **Does the server have AIX diagnostics preinstalled?**

   Yes: If there is an HMC attached to the system, go to Using the HMC to load the online diagnostics in service mode. If an HMC is not attached to the system, go to Loading the online diagnostics on a system without an HMC attached on page 40.

   No: If there is an HMC attached to the system, go to Using the HMC to load the standalone diagnostics from CD-ROM on page 39. If an HMC is not attached to the system, go to Loading the standalone diagnostics on a system without an HMC attached on page 40.

   Note: If the server does not have an optical drive to load standalone diagnostics, go to Running Standalone Diagnostics from a Network Installation Management (NIM) Server with an HMC Attached to the System on page 41.

2. **Using the HMC to load the online diagnostics in service mode**

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

   If the system is powered down, do the following. If it is powered up, and you are activating a partition, go to substep 2j on page 39.

   a. If the ASMI is available, do the following. If the ASMI is not available, go to substep 2b.
      1) Access the ASMI. Login with your user ID and password.
      2) On the Welcome screen, click on **Power/Restart Control**.
      3) On the Power/Restart Control menu, click on **Power On/Off System**.
      4) On the Power On/Off System menu, set the system boot speed to **slow**. Also verify that the Boot to System server firmware option is set to **Running**.
      5) Click on **Save Settings**.
      6) Go to substep 2c.

   b. Slow boot can be set using the control panel. Do the following:
      1) Use panel function 02 to set the system boot speed to S (slow). Refer to Control panel functions for more information.
      2) Go to substep 2c.

   c. If you are powering on the server, continue with 2d. If you are activating a partition, go to substep 2j on page 39.

   d. Use the HMC to power on the server by selecting the managed system in the **Server and Partition: Server Management** area.

   e. Highlight the desired system by right-clicking on or selecting the system in the **Server and Partition: Server Management** area. On the menu, choose **Selected**.

   f. Select **Power On**. Enter any passwords that are requested.

   g. After the keyboard POST indicator displays on the firmware console and before the last POST indicator (speaker) displays, press the numeric 6 key on either the directly attached keyboard or the ASCII terminal to indicate that a service mode boot should be initiated using the customized service mode boot list.

Note: If you are unable to load the diagnostics to the point where the DIAGNOSTIC OPERATING INSTRUCTIONS display, go to Using the HMC to load the standalone diagnostics from CD-ROM.

h. Go to Running system verification.

i. Right-click on the partition name. On the menu, select the **Power on Diagnostics Stored Boot List** option.

j. Enter any passwords that are requested.

k. After the keyboard POST indicator displays on the firmware console and before the last POST indicator (speaker) displays, press the numeric 6 key on either the directly attached keyboard or the ASCII terminal to indicate that a service mode boot should be initiated using the customized service mode boot list.

Note: If you are unable to load the diagnostics to the point where the DIAGNOSTIC OPERATING INSTRUCTIONS display, go to Using the HMC to load the standalone diagnostics from CD-ROM.

l. Go to Running system verification.

3. **Using the HMC to load the standalone diagnostics from CD-ROM**

To run the standalone diagnostics CD-ROM, an optical drive must be assigned to the partition in which you want to run standalone diagnostics. Ask the customer to verify that an optical drive is available to the partition before continuing.

If the system is powered down, do the following. If it is powered up, and you are activating a partition, go to substep 3m on page 40.

a. Stop all programs, including the operating system (get help if needed).

b. Remove all tapes, diskettes, and optical media.

c. Power off the server. See Stopping the system.

d. If the ASMI is not available, skip to substep 3e. If the ASMI is available, do the following:

1) Access the ASMI. Login with your user ID and password.

2) On the Welcome screen, click on **Power/Restart Control**.

3) On the Power/Restart Control menu, click on **Power On/Off System**.

4) On the Power On/Off System menu, set the system boot speed to **slow**. Also verify that the setting for the **Boot to system server firmware** is set to **Running**.

5) Click on **Save Settings**.

6) Go to substep 3f.

e. Slow boot can be set using the control panel. Do the following:

1) Use panel function 02 to set the system boot speed to S (slow). Refer to Control panel functions for more information.

2) Go to substep 3f.

f. If you are powering on the server, continue with substep 3g. If you are activating a partition, go to substep 3l on page 40.

g. Highlight the desired system by right-clicking on or selecting the system in the **Server and Partition: Server Management** area. On the menu, select **Selected**.

h. Select **Power On**. As soon as the optical drive has power, insert the AIX stand-alone diagnostic CD-ROM into the optical drive.

i. Enter any passwords that are requested.

j. After the **keyboard** POST indicator displays on the firmware console and before the last POST indicator (**speaker**) displays, press the numeric 5 key on either the directly attached keyboard or the ASCII terminal to indicate that a service mode boot should be initiated using the default service mode boot list.

Note: If you are unable to load the diagnostics to the point where the DIAGNOSTIC OPERATING INSTRUCTIONS display, call your service support center for assistance.

k. Go to Running system verification.

l. Right-click on the partition name. On the menu, select the **Activate** option. As soon as the optical drive has power, insert the AIX stand-alone diagnostic CD-ROM into the optical drive.

m. Enter any passwords that are requested. .

n. After the keyboard POST indicator displays on the firmware console and before the last POST indicator (speaker) displays, press the numeric 5 key on either the directly attached keyboard or the ASCII terminal to indicate that a service mode boot should be initiated using the default service mode boot list.

Note: If you are unable to load the diagnostics to the point where the DIAGNOSTIC OPERATING INSTRUCTIONS display, call your service support center for assistance.

o. Go to Running system verification.

4. **Loading the online diagnostics on a system without an HMC attached**

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

a. Stop all programs including the AIX operating system (get help if needed).

b. Remove all tapes, diskettes, and optical media.

c. Turn off the system unit power.

d. If the ASMI is not available, skip to substep 4e. If the ASMI is available, do the following:

1) Access the ASMI. Login with your user ID and password.

2) On the welcome screen, click on **Power/Restart Control**.

3) On the ″Power/Restart Control″ menu, click on **Power On/Off System**.

4) On the ″Power On/Off System″ menu, set the system boot speed to ″slow″. Also verify that ″Boot to System Hypervisor″ is set to ″Running″.

5) Click on ″Save Settings″.

6) Go to substep 4f.

e. Slow boot can be set using the control panel. Do the following:

Use panel function 02 to set the system boot speed to S (slow). Refer to Control panel functions for more information.

f. Turn on the system unit power.

g. After the **keyboard** POST indicator displays on the firmware console and before the last POST indicator (**speaker**) displays, press the numeric 6 key on either the directly attached keyboard or the ASCII terminal to indicate that a service mode boot should be initiated using the Customized service mode boot list.

h. Enter any requested password.

Note: If you are unable to load the diagnostics to the point when the DIAGNOSTIC OPERATING INSTRUCTIONS display, call your service support center for assistance.

i. Go to “Running system verification” on page 43.

5. **Loading the standalone diagnostics on a system without an HMC attached**

To run the standalone diagnostics from CD-ROM, do the following:

a. Stop all programs including the AIX operating system (get help if needed).

b. Remove all tapes, diskettes, and optical media.

c. Turn off the system unit power.

d. If the ASMI is not available, skip to substep 5e on page 41. If the ASMI is available, do the following:

1) Access the ASMI. Login with your user ID and password.

2) On the welcome screen, click on **Power/Restart Control**.
3) On the ″Power/Restart Control″ menu, click on **Power On/Off System**.
4) On the ″Power On/Off System″ menu, set the system boot speed to ″slow″. Also verify that ″Boot to System Hypervisor″ is set to ″Running″.
5) Click on ″Save Settings″.
6) Go to substep 5f.

e. Slow boot can be set using the control panel. Do the following:

   Use panel function 02 to set the system boot speed to S (slow). Refer to Control panel functions for more information.

f. Turn on the system unit power and immediately insert the diagnostics CD-ROM into the CD-ROM drive.

g. After the **keyboard** POST indicator displays on the firmware console and before the last POST indicator (**speaker**) displays, press the numeric 5 key on either the directly attached keyboard or the ASCII terminal to indicate that a service mode boot should be initiated using the default service mode boot list.

h. Enter any requested password.

   Note: If you are unable to load the diagnostics to the point when the `DIAGNOSTIC OPERATING INSTRUCTIONS` display, call your support center for assistance.

i. If you want to verify server or partition operations, go to Running system verification.

6. **Performing additional system verification**

   To perform additional system verification, do the following:

   a. Press Enter to return to the Diagnostic Selection menu.

   b. To check other resources, select the resource. When you have checked all of the resources you need to check, go to “Stopping the diagnostics” on page 44.

7. **Running Standalone Diagnostics from a Network Installation Management (NIM) Server with an HMC Attached to the System**

   A client system connected to a network with a Network Installation Management (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:

   a. All operations to configure the NIM server require root user authority.

   b. 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.

   c. The **Cstate** for each standalone diagnostics client on the NIM server should be kept in the *diagnostic boot has been enabled* state.

   d. On the client system, the NIM server network adapter should 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. For information about setting the bootlist, see Accessing the Advanced System Management Interface.

   For information about:

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

   Refer to “Advanced NIM configuration tasks” information on the AIX documentation Web site (http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix.htm)

   NIM Server Configuration:

To verify that the client system is registered on the NIM server and the diagnostic boot is enabled, run the **lsnim -a Cstate -Z *ClientName*** command 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.

8. **Client Configuration and Booting Standalone Diagnostics from the NIM Server**

   To run the standalone diagnostics from a NIM server, the network adapter from which you want to boot from the NIM server must be assigned to the partition in which you want to run standalone diagnostics. Ask the customer to verify that a network adapter is available to the partition before continuing.

   If the system is powered down, do the following. If it is powered up, and you are activating a partition, go to substep 8j on page 43.

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

   a. Remove any removable media (tape or optical disc).
   b. Stop all programs including the operating system (get help if needed).
   c. If the ASMI is available, do the following. If the ASMI is not available, go to substep 8d.
      1) Access the ASMI. Login with your user ID and password.
      2) On the welcome screen, click on **Power/Restart Control**.
      3) On the Power/Restart Control menu, click on **Power On/Off System**.
      4) On the Power On/Off System menu, set the system boot speed to "slow". Also verify that "Boot to System Hypervisor" is set to "Running".
      5) Click on **Save Settings**.
      6) Go to substep 8e.
   d. Slow boot can be set using the control panel. Do the following:
      1) Use panel function 02 to set the system boot speed to S (slow). Refer to Control panel functions for more information.
      2) Go to substep 8e.
   e. If you are powering on the server, continue with substep 8f. If you are activating a partition, go to substep 8i.
   f. Highlight the desired system by right-clicking on or selecting the system in the **Server and Partition: Server Management** area. On the menu, choose Selected.
   g. Select **Activate**.
   h. Enter any requested passwords. Go to step 8j on page 43.
   i. Right-click on the desired partition name and select the **Activate** option.

j. After the **keyboard** POST indicator displays on the firmware console and before the last POST indicator (**speaker**) displays, press the numeric 1 key on either the directly attached keyboard or the ASCII terminal to enter the SMS (system management services) menus.

k. Select **Setup Remote IPL (Initial Program Load)**.

l. Enter the client address, server address, gateway address (if applicable), and subnet mask. Exit to the Network Parameters screen.

m. 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, check the connections between the server and the NIM server.

n. Exit the SMS menus completely. The system starts loading packets while doing a **bootp** from the network.

o. Go to Running system verification.

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

a. Exit to the SMS Main screen.

b. Select **Select Boot Options**.

c. Select **Install or Boot a Device**.

d. On the Select Device Type screen, select **Network**.

e. Set the network parameters for the adapter from which you want to boot.

f. 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 operating system 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.

Note: If the ping fails, check the connections between the server and the NIM server.

Verify the connections between the server and the NIM server and check the settings and status for the network.

Note: If you are unable to load the diagnostics to the point where the DIAGNOSTIC OPERATING INSTRUCTIONS display, go to Using the HMC to load the standalone diagnostics from CD-ROM.

Running system verification

When the Diagnostic Operating Instructions display, do the following to run system verification:

1. Press Enter.
2. If the terminal type is requested, you must use the **Initialize Terminal** option on the Function Selection menu to initialize the operating system before you can continue with the diagnostics.
3. Select the **System Verification** option on the Diagnostic Mode Selection menu.
4. To run a general checkout of all installed resources, select the **All Resource** option on the Diagnostic Selection menu. Follow the instructions on the screen to complete the checkout procedure.

To check one particular resource, select that resource on the Diagnostic Selection menu.

The checkout program ends with either of the following results:

- The Testing Complete screen displays a message stating `No trouble was found`.
- The A Problem Was Detected On (Time Stamp) menu displays, with either a service request number (SRN) or an error code. Make a note of any codes displayed on the display or operator panel.

Note: If you received an error code, record the code and then contact your service support center.

To stop diagnostics, do the following:

Stopping the diagnostics

1. To exit the diagnostics, press the F3 key (from a defined terminal) or press 99 (from an undefined terminal).
2. If you changed any attributes on your terminal to run the diagnostics, change the settings back to normal.

   This completes the system verification.

If the server passed all the diagnostic tests, the verification process is complete and your server is ready to use.

AIX 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. This chapter describes the tasks available in the AIX diagnostic programs.

Notes:

1. 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 may be accessible only from standalone diagnostics.
2. The specific tasks available will be dependent on the hardware attributes or capabilities of the system you are servicing. Not all service aids nor tasks will be available on all systems.
3. If the system is running on a logically partitioned system, the following tasks can be executed only in a partition with service authority:
   - Configure Reboot Policy
   - Configure Remote Maintenance Policy
   - Configure Ring Indicate Power On
   - Configure Ring Indicate Power-On Policy
   - Update System or Service Processor Flash
   - Save or Restore Hardware Management Policies
   - 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 Reboot Policy
- Configure Remote Maintenance Policy
- Configure Ring Indicate Power On (RSPC)
- Configure Ring Indicate Power-On Policy
- Configure Service Processor (RSPC)
- 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 Multipath I/O (MPIO) Device Configuration
- 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
- Identify Indicators
- Identify and System Attention Indicators
- Local Area Network Analyzer
- Log Repair Action

- Periodic Diagnostics
- PCI SCSI Disk Identify Array Manager
- PCI RAID Physical Disk Identify
- Process Supplemental Media
- Run Diagnostics
- Run Error Log Analysis
- Run Exercisers
- Save or Restore Hardware Management Policies
- Save or Restore Service Processor Configuration (RSPC)
- SCSI Bus Analyzer
- SCSI RAID Physical Disk Status and Vital Product Data
- SCSD Tape Drive Service Aid
- Spare Sector Availability
- SSA Service Aid
- System Fault Indicator
- System Identify Indicator
- Update Disk-Based Diagnostics
- Update and Manage System Flash
- 7135 RAIDiant Array Service Aids

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 under the following 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, run Certify if after running diagnostics on a drive and its media, no problem is found, but you suspect that a problem still exists.

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 media can 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 data errors occurs, the data on the media should be transferred to another media and the original media should be discarded. If an unrecovered equipment error occurs or recovered errors exceed the threshold value, the original media should be discarded.

  The certify service aid displays the following information:
  - Capacity in bytes
  - Number of data errors recovered
  - Number of data errors not recovered
  - Number of equipment check errors
  - Number of equipment checks not recovered

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. The command line syntax is: `diag -c -d -T certify`

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

- Certify Hard file Attached to a Non-RAID and PCI-X RAID SCSI Adapter

  For pdisks and hdisks, this selection reads all of the ID and data fields on the hard file. If bad-data errors are encountered, the certify operation counts the errors.

  If there are non-recovered data errors that do not exceed the threshold value, do one of the following:

  For hdisk hard files, the hard file must be formatted and then certified again.

  For pdisk hard files, diagnostics should be run on the parent adapter.

  If the non-recovered data errors, recovered data errors, recovered and non-recovered equipment errors exceed the threshold values, the hard file must be replaced.

  After the read certify of the disk surface completes for hdisk hard files, the certify operation performs 2000 random-seek operations. Errors are also counted during the random-seek operations. If a disk timeout occurs before the random seeks are finished, the disk needs to be replaced.

  The Certify service aid displays the following information:

  – For hdisks:
    - 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.

  – For pdisks:
    - Drive capacity in megabytes.
    - Number of data errors not recovered.
    - Number of LBA reassignments
    - Number of equipment checks not recovered.

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

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

- Certify Hard File 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. The command line syntax is: `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

-I Specifies physical disk channel/ID (for 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 the VPD 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 Reboot Policy

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, describes 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

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

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:

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

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

The Scan Dump Control (SDC) settings are as follows:
- 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 follows:
- As Requested - Dump content is determined by the platform firmware.
- Minimum - Dump content collected provides the minimum debug information, enabling 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 service aid directly from the AIX command line by typing:
`/usr/lpp/diagnostics/bin/uspchrp -d`

Surveillance Setup

Note: Surveillance is only supported for systems running in full machine partition.

This selection allows you to display and change the NVRAM settings for the surveillance capability of the service processor.

The settings allow you to:
- Enable or disable surveillance
- Set the surveillance time interval, in minutes
- Set the surveillance delay, in minutes

The current settings are read from NVRAM and displayed on the screen. Any changes made to the data shown are written to NVRAM.

Modem Configuration

Use this selection when setting the NVRAM for a modem attached to any of the service processor's serial ports. The user inputs the file name of a modem configuration file and the serial port number. The formatted modem configuration file is read, converted for NVRAM, and then loaded into NVRAM.

Call In/Out Setup

This selection allows the user to display and change the NVRAM settings for the call in/call out capability of the service processor.

The settings allow the user to:

- Enable or disable call in on either serial port
- Enable or disable call out on either serial port
- Set the line speed on either serial port

Site Specific Call In/Out Setup

This selection allows you to display and change the NVRAM settings that are site-specific for the call-in or call-out capability of the service processor.

The site-specific NVRAM settings allow you to set the following:

- Phone number for the service center
- Phone number for the customer administration center
- Phone number for a digital pager
- Phone number for the customer system to call in
- Phone number for the customer voice phone
- Customer account number
- Call-out policy
- Customer RETAIN ID
- Customer RETAIN password
- Remote timeout value
- Remote latency value
- Number of retries while busy
- System name

The current settings are read from NVRAM and displayed on the screen. Any changes made to the data shown are written to NVRAM.

Reboot/Restart Policy Setup

This selection 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 setup.

- 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 allowed to reboot the system. The term *reboot*, when used in context of this service aid, describes the system hardware being brought back up from scratch. Examples would be a system reset or turning on the power.

  When the maximum number of reboot attempts is exceeded, the system calls out if that function has been enabled.

  When the reboot process completes successfully, the reboot-attempts count is reset to 0, and a restart begins. The term *restart*, when used in context of this service aid, describes 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 reboot attempts.

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

  When the service processor detects operating system inactivity, an enabled ″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 call-outs can be valuable if the number 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.

Configure Surveillance Policy

Note: This service aid is supported only 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 a drive of a different size. The service aid only supports copying from a SCSI drive to another SCSI drive of the same 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 SCSI disk drive that is not the same size. Refer to *System Management Guide: Operating System and Devices* for a procedure on to migrate the contents of a physical volume.

   This publication is located on the *AIX documentation* CD. The documentation information is made accessible by loading the documentation CD onto the hard disk or by mounting the CD in the CD-ROM drive.

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 drives 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

This task displays the firmware device node information. 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 selections provide the same type of report as the **errpt** command. The display error analysis summary and display error analysis detail selections 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 display 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. The command syntax is: `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 MultiPath I/O (MPIO) Device Configuration

This service aid displays the status of MPIO devices and their connections to their parent devices.

This service aid is capable of sending SCSI commands on each available path regardless of the default MPIO path algorithm. Therefore, it is useful for testing the unused path for integrity.

Run this service aid if it is suspected that there is a problem with the path between MPIO devices and their parent devices.

This service aid is capable of:

- Listing MPIO devices
- Listing the parents of MPIO devices
- Displaying the status and location of specified MPIO devices
- Displaying the hierarchy of MPIO adapters and devices.

If there are no devices with multiple paths, this service aid will not be shown on the "Task Selection" menu.

Access this service aid directly from the AIX command line by typing:

```
/usr/lpp/diagnostics/bin/umpio
```

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).
- 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, in a box at the bottom of the screen, indicate that the test is 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 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 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 options.

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.

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.

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

This service aid displays the environmental sensor information for the 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 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 for systems using AIX 5.2.0.30 and later

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 installing the new microcode.

This task can be run directly from the AIX command line. Most adapters and devices use a common syntax as identified in the ″Microcode Installation to Adapters and Devices″ section. Information for adapters and devices that do not use the common syntax can be found following this section.

Microcode installation to adapters and devices

For many adapters and devices, microcode installation occurs and becomes effective while the adapters and devices are in use. It is recommended that a current backup be available and the installation be scheduled during a non-peak production 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 CD (cdX), the CD must be in ISO 9660 format. There are no restrictions as to what directory in which to store the image.
3. If the source is diskette (fdX), the diskette must be in backup format and the image stored in the /etc/microcode directory.

The following is the common syntax command:

```
diag [-c] -d <device> -T "download [-s {/etc/microcode|<source>}] [-l {latest|previous}] [-f]"
```

Flag Description

-c No console mode. Run without user interaction.

-d <device>
Run the task on the device or adapter specified.

-T download
Install microcode.

-s /etc/microcode
Microcode image is in /etc/microcode.

-s <source>
Microcode image is on specified source. For example, fd0, cd0.

-l latest
Install latest level of microcode. This is the default.

-l previous
Install previous level of microcode.

-f Install microcode even if the current level is not on the source.

Microcode installation to a SES device

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 CD (cdX), the CD must be in ISO 9660 format. There are no restrictions as to what directory to store the image.
3. If the source is diskette (fdX), the diskette must be in backup format and the image stored in the /etc/microcode directory.

The following is the common syntax command:

```
diag [-c] -d <device> -T "download [-s {/etc/microcode|<source>}]"
```

Flag Description

-c No console mode. Run without user interaction.

-d <device>
Run the task on the device or adapter specified.

-T download
Install microcode.

-s /etc/microcode
Microcode image is in /etc/microcode.

-s <source>
Microcode image is on specified source. For example, fd0, cd0.

Microcode installation to PCI SCSI RAID adapters

PCI SCSI RAID adapters that support this type of installation are:

- Type 4-H, PCI SCSI-2 Fast/Wide RAID Adapter (Feature Code 2493)
- Type 4-T, PCI 3-Channel Ultra2 SCSI RAID Adapter (Feature Code 2494)
- Type 4-X, PCI 4-Channel Ultra3 SCSI RAID Adapter (Feature Code 2498)

Notes:

1. If the image is on the hard drive, it 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 image is on a diskette, the diskette must be in backup format and the image stored in the /etc/microcode directory.

syntax:

```
diag [-c] -d <RAIDadapterName> -T "download [-B][-D][-P]"
```

Flag Description

-c No console mode. Run without user interaction.

-d <RAIDadapterName>
Run the task on the RAID adapter specified.

-T download
Install microcode.

-B Install boot block microcode. Default is functional microcode.

-D Microcode image is on diskette. Default is /etc/microcode.

-P Install the previous level of microcode. Default is latest level.

Microcode installation to disk drive attached to PCI SCSI RAID adapters

Microcode for a disk drive attached to a PCI SCSI RAID adapter is installed through the adapter to the drive. PCI SCSI RAID adapters that support this type of installation are:

- Type 4-H, PCI SCSI-2 Fast/Wide RAID Adapter (Feature Code 2493)

- Type 4-T, PCI 3-Channel Ultra2 SCSI RAID Adapter (Feature Code 2494)
- Type 4-X, PCI 4-Channel Ultra3 SCSI RAID Adapter (Feature Code 2498)

Notes:

1. If the image is on the hard drive, it 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 image is on a diskette, the diskette must be in backup format and the image stored in the /etc/microcode directory.

syntax:

```
diag [-c] -d <RAIDadapterName> -T "download {-l <chID> | -A} [-D][-P]"
```

Flag **Description**

-c No console mode. Run without user interaction.

-d <RAIDadapterName>
Name of the RAID adapter the disk is attached to.

-T download
Install microcode.

-l Physical disk channel/ID of RAID disk drive (example: 27).

-A All disk drives attached to specified RAID adapter.

-D Microcode image is on diskette. Default is /etc/microcode.

-P Install the previous level of microcode. Default is latest level.

Fault Indicators

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 Component and attention LEDs.

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 | -d device name]
```

OR

```
/usr/lpp/diagnostics/bin/usysident [-t]
```

Flag	Description
-s *normal* |identity	Sets the Fault Indicator to the normal state.
-l *location code*	Identifies the resource by physical location code.
-d *device name*	Identifies the resource by device name.
-t	Displays a list of all supported identify indicators by physical location codes.

When this command is used with neither the -l nor the -d flag, the primary enclosure resource is used.

Use the -l flag only in systems that have more than one identify indicator. The -d flag is only supported in levels of diagnostics 5.2.0.30 and higher. Use of the -d flag is preferred over use of the -l flag.

When this command is used without the **-s** flag, the current state of the indicator is displayed as normal or attention.

Note: See also the Identify and system attention indicators. 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 fast-path 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 fast-path 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 fast-path 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 fast-path 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 fast-path 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 derase 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. 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.

  To overwrite the data on the drive, use the following steps :
  1. Select **Erase Disk**.
  2. Do a format without certify.
  3. Select **Erase Disk** to run it a second time.

  For a newly installed drive, you can ensure that all blocks on the drive are overwritten with your pattern by using the following procedure:
  1. Format the drive.
  2. Check the defect MAP by running the erase disk option.

     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 option 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, 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. The command syntax is: `diag -c -d` *`deviceName`* `-T "format [-s* fmtcert | erase -a {read | write} -P {comma separated list of patterns}] [-F]*`

Note: The following flags are not available for pdisk devices.

Flag	Description
fmtcert	Formats and certifies the disk.
erase	Overwrites the data on the disk.
*	Available in no-console mode only.
-F	Forces the disk erasure even if all blocks cannot be erased because of errors accessing the grown defect map.
-P	Comma separated list of hexadecimal patterns to be written to the drive serially. Up to eight patterns can be specified using a single command. The patterns must be 1, 2, or 4 bytes long without a leading 0x or 0X. Example using five patterns: -P ff, a5c0, 00, fdb97531, 02468ace

Notes:

1. If no patterns are specified for the erase disk option in command line mode, then the default pattern of 00 is used.
2. 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. The command line syntax is: `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. The command line syntax is: `diag -c -d` *deviceName* `-T "format [-s {initialize | fmtcert} ]"`

Option	Description
initialize	Formats media without certifying
fmtcert	Formats and certifies the media

DVD-RAM Media

- Initialize

  Formats the media without certifying. This function does not reassign the defective blocks or erase the data on the media. This format type can only be used with previously formatted media.
- Format and Certify

Formats and certifies the media. This function reassigns the defective blocks and erases the data on the media by writing an initialization pattern to the entire media.

This task can be run directly from the AIX command line. The command line syntax is:
`diag -c -d deviceName -T"format [-s{initialize|fmtcert}]"`

Flag	Description
-c	No console mode
-d	Used to specify a device
-s initialize	Initialize the media (quick format). This is the default.
-s fmtcert	Formats and certifies the media.
-T	Used to specify the format task

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, file systems, security, the kernel, the ODM, and other system components. You can also 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

Attention: The Linux operating system does not support some hot-pluggable procedures. Also, Linux does not support hot-plugging any hot-pluggable PCI adapters or devices. A system with Linux installed on one or more partitions must be shut down and powered off before replacing any PCI adapter or device assigned to a Linux partition. Follow the non-hot-pluggable adapter or device procedures when replacing a PCI adapter or device in any partition with Linux installed.

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 cannot 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 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, device configuration is complete. Select the device that has an uppercase `M` in front of it in the resource list so that missing options processing can be done on that resource.

PCI Hot Plug Manager

Attention: The Linux operating system does not support some hot-pluggable procedures. Also, Linux does not support hot-plugging any hot-pluggable PCI adapters or devices. A system with Linux installed on one or more partitions must be shut down and powered off before replacing any PCI adapter or device assigned to a Linux partition. Please follow the non-hot-pluggable adapter or device procedures when replacing a PCI adapter or device in any partition with Linux installed.

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 the PCI hot-plug manager can be found in the *AIX Operating System System Management Guide*.

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 an 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: Before you remove the device, be sure that no other host is using 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. The command line syntax is:

```
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.

SCSI and SCSI RAID Hot-Plug Manager

This task was previously called ″SCSI hot-swap manager″, ″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 hot-swap enclosure device. This task also performs these functions on a SCSI RAID device attached to a PCI-X RAID controller. The following functions are available:
- List the SCSI Hot Swap Enclosure Devices
- Identify a Device Attached to a SCSI Hot Swap Enclosure Device
- Attach a Device to a SCSI Hot Swap Enclosure Device
- Replace/Remove a Device Attached to an SCSI Hot Swap Enclosure Device

- Configure Added/Replaced Devices

The list the SCSI hot-swap enclosure 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 SCSI hot-swap enclosure device function is used to help identify the location of a device attached to a SCSI hot-swap enclosure 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 a SCSI hot-swap enclosure 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 SCSI hot-swap enclosure 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, 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: Before you remove the device, be sure that no other host is using 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. The command syntax is:

```
diag -d device -T"identifyRemove
```

OR

```
diag -d device -T"identifyRemove -a [identify|remove ]
```

Flags	Description
-a	Specifies the option under the task.
-d	Indicates the SCSI device.
-T	Specifies the task to run.

RAID Hot-Plug Devices

This task allows the user to identify or remove a RAID device in a system unit that uses a SCSI Enclosure Services (SES) device. The following subtasks are available:
- **Normal**

- **Identify**
- **Remove**

The normal subtask is used to return a RAID hot plug device to its normal state. This subtask is used after a device has been identified or replaced. This subtask lists all channel/IDs of the RAID and the status of the devices that are connected. A device in its normal state has power and the check light is off.

The identify subtask is used to identify the physical location of a device or an empty position in the RAID enclosure. This subtask lists all channel/IDs of the RAID and the status of the devices that are connected to the RAID enclosure. If a device is attached to the selected channel/ID, the check light on the device will begin to flash. If the channel/ID does not have a device attached, the light associated with the empty position on the enclosure will begin to flash.

The remove subtask is used to put the RAID hot plug device in a state where it can be removed or replaced. This subtask lists all channel/IDs of the RAID adapter that have devices that can be removed. Only devices with a status of `Failed`, `Spare`, `Warning`, or `Non Existent` can be removed. A device's status can be changed with the AIX **smitty pdam** command. After a device is selected for removal, the check light on the device will begin to flash, indicating that you may physically remove that device.

Standalone diagnostics has restrictions on using the RAID hot-plug manager:

- 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. The command line syntax is:

```
diag -c -d <device name> -T "identifyRemove -l <ChId> -s {identify|remove|normal}
```

Flags	Description
-c	Run the task without displaying menus. Only command line prompts are used.
-d	Raid adapter device name (for example, `scraid0`).
-s	Subtask to execute such as identify, remove, or normal.
-l	*CHId* is the channel number of the RAID adapter and SCSI ID number of the position in the enclosure concatenated together (for example, 27 for channel 2, device 7).
-T	Task to run.

Identify Indicators

See the Component and attention LEDs for a description of the identify indicators task.

Identify and System Attention Indicators

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 task.

Note: It is important to run the log repair action function. This action keeps the fault indicator from going back 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 Component and attention LEDs.

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) Fiber 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.

To locate the failing part in a system or partition running AIX, do the following:

1. Log in as root user.
2. At the command line, enter **diag**.
3. Select the **Diagnostics Routines** option.
4. When the DIAGNOSTIC MODE SELECTION menu displays, select **Problem Determination**.
5. When the ADVANCED DIAGNOSTIC SELECTION menu displays, do one of the following: To test a single resource, select the resource from the list. To test all the resources available to the operating system, select All Resources.
6. Press **Enter**, and wait until the diagnostic programs run to completion, responding to any prompts that appear on the console.
7. Use the location information for the failing part to activate the indicator light that identifies the failing part. For instructions, see Activate the indicator light for the failing part.

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 a HMC attached, 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

For a description of the PCI RAID physical disk identify task, see "SCSI RAID Physical Disk Status and Vital Product Data" on page 78.

PCI SCSI Disk Array Manager

This service aid calls the **smitty pdam** fastpath, and is used to manage a RAID array connected to a SCSI RAID adapter. It may also be run from standalone diagnostics, which are available on systems or partitions with operating systems other than AIX installed on them (these environments do not allow you to run the **smitty pdam** command).

Some of the tasks performed using this service aid include:

- Check device status for the disk array on your system.
- Display information of physical drives and disk arrays.
- Run recovery options on the RAID (which needs to be done at the end of a service call in which you replaced the RAID adapter cache card or changed the RAID configuration)

Other RAID functions are available using this service aid; they should only be used by the system administrator who is familiar with the RAID configuration. These functions are normally done when booting AIX by running **smitty pdam** from the command line. Without knowledge of how the RAID was set up, these functions can cause loss of data stored on the RAID.

Process Supplemental Media

Process 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, run diagnostics 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 depend on the state of the diagnostics run-time options. See "Display or Change Diagnostic Run-Time Options" on page 57.

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, 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 the **/tmp** directory 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 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 the **/tmp** directory 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 the following options:

- **Option 1 - Short Exercise.** Exercises the resources within a relatively short time and exits.
- **Option 2 - Extended Exercise.** 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 fill out 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 exercises are exited)

For information about using other available options, see the help text.

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 displays.

If miscompare errors were encountered, run diagnostics on the resource. If the problem is not reported, contact your service support structure. If any other error 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.

Acronym	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 exerciser is labeled `mem0`. The exerciser requests as many memory buffers as possible from AIX. The exerciser fills these buffers with specific bit patterns and then compares them to the original bit patterns. If memory is removed as a result of processors being reconfigured dynamically, the exerciser terminates.

On systems with multiple processors, a process is started for each processor. The free memory space is split evenly among 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 **/etc/lpp/diagnostics/data**.

Tape Exerciser

The tape exerciser is labeled `rmtx`, 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 diagnostic test cartridge are required to run this exerciser. The actual diagnostics test cartridge depends upon the specific tape device being tested. The exerciser automatically rewinds the tape. Test requirements are:
- Tape device
- Diagnostic test cartridge (the part number depends upon tape device)

Diskette Exerciser

The diskette exerciser is labeled `fdx`, 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 `cdx`, 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 P/N 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.

Save or Restore Hardware Management Policies

Use this service aid to save or restore the settings from ring indicate power-on policy, surveillance policy, remote maintenance policy and reboot policy. The following options are available:
- Save Hardware Management Policies

  This selection writes all of the settings for the hardware-management policies to the following file: **/etc/lpp/diagnostics/data/hmpolicies**
- Restore Hardware Management Policies

  This selection restores all of the settings for the hardware-management policies from the contents of the following file: **/etc/lpp/diagnostics/data/hmpolicies**

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

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, then start adding additional devices and cables to the bus, ensuring that each one works. 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. If the device is in use by another process, AIX does not send the command.

SCSI RAID Physical Disk Status and Vital Product Data

Note: This task was previously known as the PCI RAID physical disk identify task.

Use this service aid when you want to look at the vital product data for a specific disk attached to a RAID adapter.This service aid displays all disks that are recognized by the PCI RAID adapter, along with their status, physical location, microde level, and other vital product data. The physical location of a disk consists of the channel number of the RAID adapter and the SCSI ID number of the position in the enclosure. The microde level is listed next to the physical location of the disk.

You can run this task directly from the command line with the following command syntax:

```
diag -c -d < device name > -T "identify"
```

Flags	Description
-c	Run the task without displaying menus. Only command line prompts are used.
-d	RAID adapter device name (for example, `scraid0`).
-T	Task to run.

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 must 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. The command syntax is: `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 Component and attention LEDs.

System Identify Indicator

For a description of the system fault indicator task, see Component and attention LEDs.

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 and Manage System Flash

Note: For detailed firmware update scenarios, see Getting Fixes.

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 a service partition has been designated, 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 in a file on the system, reboot the system in a full system partition and use the following normal firmware update procedures.

If the system is already in a full system partition, use the following normal firmware update procedures.

This selection validates a new system firmware flash image and uses it to update the system temporary flash image. This selection can also be used to validate a new system firmware flash image without performing an update, commit the temporary flash image, and reject the temporary flash image.

Look for additional update and recovery instructions with the update kit. You need to 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 or optical media, the service aid can list the files on the diskette or optical media for selection. The diskette must be a valid backup format diskette.

Refer to the update instructions with the kit, or the service guide for the system unit to determine the current level of the system unit or service processor flash memory.

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, optical media, 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 one 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 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. You may 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 | -v] -f file_name
update_flash [-q | -v] -D device_name -f file_name
update_flash [-q | -v] -D update_flash [-l]
update_flash -c
update_flash -r
```

Attention: The **update_flash** command reboots the entire system. Do not use this command if more than one user is logged in to the system.

Flag	Description
-D	Specifies that the flash update image file is on diskette. The *device_name* variable specifies the device. 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.
-v	Validates the flash update image. No update will occur. This flag is not supported on all systems.
-c	Commits the temporary flash image when booted from the temporary image. This overwrites the permanent image with the temporary image. This flag is not supported on all systems.
-r	Rejects the temporary image when booted from the permanent image. This overwrites the temporary image with the permanent image. This flag is not supported on all systems.

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

To download the adapter microcode, use this command syntax: `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)

To download physical disk microcode, use this command syntax : `diag -c -d` *deviceName* `-T "download -l` *ChId* `[-D][-P]"`

Flag	Description
-D	Microcode is on diskette (default to /etc/microcode directory)
-l	Physical disk channel/ID (for example, 27)
-P	Download the previous level of microcode (default to latest level)

To format a physical disk, use this command syntax: `diag -c -d` *deviceName* `-T "format -l` *ChId"*

Flag	Description
-l	Physical disk channel/ID (for example, 27)

To certify a physical disk, use this command syntax: `diag -c -d` *deviceName* `-T "certify -l` *ChId"*

Flag	Description
-l	Physical disk channel/ID (for example, 23)

To identify a physical disk, use this command syntax: `diag -c -d` *deviceName* `-T "identify"`

Powering on and powering off

The following procedures may be performed by customers, and are located outside this topic:

Powering on the system

Powering off the system

Powering on the partition

Powering off the partition

These procedures are for authorized service providers only and are found in this topic:

"Powering off an expansion unit" on page 83

"Using the control panel power button to power off" on page 87

Powering off an expansion unit

Attention: Use the HSM options only for systems that are not managed by an HMC. If the server is HMC-managed, the power off and power on functions must be performed from the HMC (**Service Focal Point** > **Service Utilities** > **Power On/Off Unit**).

Attention: **Do not** use this procedure on the system unit or the system unit's integrated expansion unit. For system units and system unit integrated expansion units see "Powering on and powering off" on page 82.

Attention: **Do not** use this procedure to replace disk units that are supported under device concurrent maintenance. Use device concurrent maintenance instead.

Note: If the system has logical partitions, then all operations on the console refer to the console of the logical partition in which you are working.

Note: Throughout this procedure, the term *HSL I/O bridge* is interchangeable with *RIO adapter*.

Use this procedure only to power off an expansion unit when you are performing one of the following:

- Removing or replacing a failing part within an expansion unit.
- Adding, moving, removing, or replacing a failing item within an expansion unit.

Perform the following with the assistance of the customer:

1. Determine if the system is managed by an HMC. Is the system managed by an HMC?

   No: Continue with the next step.

   Yes: Use the HMC to power off the expansion unit (**Service Focal Point** > **Service Utilities** > **Power On/Off Unit**).
2. Determine if the system is running i5/OS. Is the system running i5/OS?

   Yes: Continue with the next step.

   No: Power down the system (see Stop the system).
3. Determine if a tower on the HSL OptiConnect Loop is configured as a switchable tower, either by asking the customer or referring to Determining if a tower is configured as switchable under iSeries OptiConnect.

   Is the tower configured as a switchable tower?

   Yes: Continue with the next step.

   No: The expansion tower is privately owned by this system or partition. Go to step 10 on page 84.
4. Determine if the system that controls the SPCN for this tower also owns the tower's HSL I/O bridge resource. See IASP/Clustering Service Reference Procedures for details.

   Is the tower's SPCN (power) controlling system the same as the tower's HSL I/O bridge owner?

   No: Continue with the next step.

   Yes: Go to step 8 on page 84.
5. Is the tower's SPCN controlling system already IPL'd?

   Yes: Continue with the next step.

   No: You cannot power off the tower at this time because the SPCN controlling system must be IPL'd. Correct that problem first, then perform this procedure again. **This ends the procedure.**
6. Work with the customer to switch ownership of the tower's HSL I/O bridge resource to the tower's SPCN controlling system. Were you able to switch ownership of the tower's HSL I/O bridge resource to the tower's SPCN controlling system?

   No: Continue with the next step.

   Yes: Go to step 8 on page 84.

7. Working with the customer, use Hardware Service Manager (HSM) to switch ownership of the tower's switchable resources to the tower's SPCN controlling system. See Switching ownership of a tower's switchable resources.

   Were you able to switch ownership of the tower's switchable resources to the tower's SPCN controlling system?

   Yes: Continue with the next step.

   No: Contact your next level of support. **This ends the procedure.**
8. Perform this procedure from the SPCN controlling system. Work with the customer to end the Cluster Resource Group (CRG) containing disk units configured as independent ASPs (IASP) under the tower's HSL I/O bridge resource. Refer to the OptiConnect for i5/OS manual.

   Were you able to end the CRG?

   No: Continue with the next step.

   Yes: Go to step 10.
9. Working with the customer, use HSM to switch the tower's mode to *private* using Switching the mode of a tower's switchable resources.

   Were you able to switch the tower's mode?

   Yes: Continue with the next step.

   No: Contact your next level of support. **This ends the procedure.**
10. Check to see that no other towers controlled by this system's SPCN are powered off at this time. Then continue with the next step of this procedure.

    Attention: During this procedure, only one expansion tower per system can be powered off at any given time.
11. Were you directed to power off the tower to set the SPCN configuration ID?

    No: Continue with the next step.

    Yes: Go to step 14.
12. Verify that the "type numbers" (for example, IOPs and IOAs) contained in the expansion tower that you are powering off matches what is shown on the system by performing the following:
    a. From the SST or DST menu, select **Start a service tool** > **Hardware service manager** > **Packaging Hardware Resources** > **Concurrent Maintenance**.
    b. Select the "Toggle LED blink off/on" option for the unit you are working on. Physically locate the unit with the flashing LED in the display panel. Record its Unit value that is displayed on the top line in the display panel.
13. Work with the customer to end all bus activity in the tower by performing one of the following:
    - If the expansion tower does not contain disk unit IOPs, work with the customer to end all jobs and vary off all devices, lines, and controllers for that expansion tower.
    - If the expansion tower contains disk unit IOPs and the disk units are not mirrored to disk units in other expansion towers, work with the customer to end all communications activities to these disk units by ending all subsystems.
    - If the expansion tower contains disk unit IOPs and these disk units are mirrored to disk units in other expansion towers, you do not need to end all subsystems. Mirroring will assist during the service action.
14. Ensure that any external DVD-RAM storage device (containing its own power supply) is powered off prior to powering off the expansion tower. Then, power off the expansion tower by performing the following:

    Note: If the server is HMC-managed, the power off and power on functions must be performed from the HMC (**Service Focal Point** > **Service Utilities** > **Power On/Off Unit**).

    Attention: If any console resides on the bus that you are powering off, then powering off the bus will result in the loss of that console.

a. Use the system console and get to the SST or DST menu. Select **Start a service tool** > **Hardware service manager** > **Packaging Hardware Resources**.

b. From the Packaging Hardware Resources display, specify the **Concurrent Maintenance** option for the expansion tower that you are powering off, then press the power off PF key.

   Note: If resources on the bus or buses are active, you will receive a message indicating which resources are in use and the expansion tower will not power off. Return to step 13 on page 84 of this procedure and ensure that all resources on the bus are varied off. Follow the instructions on the screen for locating the active resources and varying them off.

c. The Confirm Power Off display appears. Follow the instructions on the display. You may be directed to perform a function 68 to power the tower down and a function 69 to power the tower back on, or you may be directed to do only a function 69 to power the tower back on.

   Attention: Make a note of what you were instructed to do at this time. You will need this information to complete the repair. Ensure that the location displayed is correct for the expansion tower that you intend to power off, and press Enter.

d. Wait for the expansion tower to power off. This may take up to 15 minutes depending on the I/O configuration and number of buses in the system power control network.

   When the power off action is initiated, DST will report that the expansion tower has powered off successfully. However, to ensure that the expansion tower is actually powered off, verify that one of the two air moving devices (AMDs) in the expansion tower has stopped and that the power LED indicator on the expansion tower control panel is off.

   Note: If the expansion tower contains disk IOPs, an attention reference code may appear on the control panel. Note the following:

   - Ignore the reference codes if the expansion tower completes the power off procedure.
   - If the expansion tower does not power off in the maximum time allowed, the system may be hung. You must power off the entire system from the control panel to do the repair.

15. Were you directed to power off the tower to set the SPCN configuration ID?

    No: Continue with the next step.

    Yes: You can now return to the procedure that sent you here to set the configuration ID in the tower card. When you are instructed to power on the tower, go to step 21b on page 86.

16. Is this an expansion tower with ac power cords connected from this tower's ac input/charger to an SPCN controlled expansion unit (for example: a 5088 expansion I/O unit)?

    Yes: Servicing this expansion tower may affect an SPCN controlled expansion unit that is receiving ac power from this tower. Continue with the next step.

    No: This expansion tower can be serviced without affecting an SPCN controlled expansion unit. Go to step 19 on page 86.

17. You may be able to maintain ac power to the expansion tower and remove power from this expansion tower so that you can service this tower. The following steps will help you to determine what you can do. Are you here to exchange the ac input/charger, any of the device boards, or the power board?

    Yes: You must search for an alternate ac power source for the expansion unit. Continue with the next step.

    No: You can maintain ac power to the expansion unit while you are servicing this tower. When the expansion tower is powered off, open the rear cover and trace the ac jumper cords from the three power supplies to the ac input charger. Then disconnect them at the ac charger. Power is now removed from the components that you will be working with or near. Go to step 20 on page 86.

18. Can you find an alternate ac power source for the expansion unit?

No: You must power off the system to service this tower. Do **not** attempt to power off the expansion unit. You must power on this expansion unit and then use dedicated service to power off the system for the FRU that you are exchanging. Go to step 21 to power on this expansion unit.

Yes: Move each of the expansion unit's ac power cords one at a time to the alternate ac power source to prevent the expansion unit from losing ac power. Go to step 19.

19. When the expansion unit is powered off, disconnect the power cord(s).
20. Remove or install the part using the procedure that sent you here. Then continue with the next step in this procedure.

    Notes:

    a. Ensure that you replace the failing IOP, IOA, or feature card with the same type and model.
    b. When IOPs and feature cards are moved or removed, ensure that the configuration rules are followed.

21. Perform the following:
    a. Reconnect the power cord(s) that you disconnected in step 19 or the power supply cords that you disconnected in step 17 on page 85.

       Note: The tower will automatically power on.

    b. Were you instructed to perform a function 69 to power the tower on?

       Yes: Continue with the next step.

       No: Go to step 21d.

    c. Perform function 69 (with the control panel set to *manual* mode) from the control panel. See Control panel functions. Then go to step 22.
    d. If the Packaging Hardware Resources display is available, specify the **Power on** option for the expansion tower you **were** working on and press **Enter**.

       Note: In some cases, FRU replacement may generate a new location in **both** the expansion tower control panel and in HSM. If this occurs, use the new location to complete the power on procedure.

    e. If the Packaging Hardware Resources display is not available, select (with the control panel set to *manual* mode) the SPCN control panel function to power on the expansion unit (see Control panel functions).
       1) Select function `07` and press **Enter**.
       2) Increment to `A1` and press **Enter**. This will send out a Rack Power On command on the SPCN which will restore power to the expansion unit, which has become powered off.

22. Were you sent here from a tower card exchange procedure?

    No: Continue with the next step.

    Yes: Choose from the following options:

    – If you have not set the configuration ID and the type, model, and serial number, return to the tower card exchange procedure to set it.
    – If you have already set the configuration ID and type, model, and serial number, then continue with the next step of this procedure.

23. Perform the following:
    a. From the Packaging Hardware Resources display, select **Associated Logical Resource(s)** for the expansion unit.
    b. The Logical Hardware Resources Associated a Packaging Resource display shows the status of devices and IOPs. When all expected resources appear with an operational status, work with the customer to bring the system to the operational state.

       Note: A resource that has been removed will show a status of ″Not Connected″.

c. Work with the customer to restart all bus activity:
   1) Start all subsystems that were ended.
   2) Vary on all devices, lines, and controllers for the expansion unit that was powered off.
   3) Start customer applications.

Was the tower configured as a switchable tower when you entered this procedure?

Yes: Continue with the next step.

No: If you moved the ac power cords of an expansion unit from this tower to an alternate ac power source during this procedure, then move them back to this expansion tower. Move only one of the expansion unit's ac power cords at a time to this tower to prevent the expansion unit from losing ac power. **This ends the procedure.**

24. Did you change the tower's mode to *private* using HSM?

    No: Continue with the next step.

    Yes: Work with the customer to restore the mode of the tower to *Switchable* using Switching the mode of a tower's switchable resources. Then continue with the next step.

25. Work with the customer to start the CRG that you ended during this procedure. Refer to the OptiConnect for i5/OS manual.

    Were you able to start the CRG?

    Yes: Continue with the next step.

    No: Contact your next level of support. **This ends the procedure.**

26. Work with the customer to restore ownership of the tower's HSL I/O bridge resource to the system that the customer prefers. Refer to the OptiConnect for i5/OS manual.

    Were you able to restore the ownership of the tower's HSL I/O bridge resource to the system that the customer prefers?

    Yes: This ends the procedure.

    No: Contact your next level of support. **This ends the procedure.**

Powering off a system with multiple logical partitions

Using the control panel power button to power off

Attention: Using the control panel power button to power off the system may cause unpredictable results in the data files, and the next IPL will take longer to complete.

1. Select **Manual** mode, if it is not already selected (see Function 02–Select IPL type, IPL speed override, and system operating mode).
2. Press and hold the (white) power button on the control panel. The Data-Function display will show the international power-off symbol (0?) and the countdown time (x), as follows:

   ```
   ____0?____x
   ___________
   ```

   Note: The default countdown time is 4 seconds, although the customer may have changed this setting.

   To power off the system, depress the power button until countdown time reaches zero (0).

   Note: If the power button is depressed for less than one second, no countdown time will be displayed and the power off function will not be initiated. To cancel the power-off operation, release the power button prior to the countdown reaching zero (0).

   Does the system power off successfully?

   Yes: This ends the procedure.

   No: Contact your next level of support. **This ends the procedure.**

Hardware Management Console Maintenance

The hardware management console (HMC) system is delivered with its machine code preinstalled on the disk drive. After the system is installed and connected to a managed system, system management tasks can begin.

The HMC connects to one or more managed systems to perform various functions. The HMC's main functions include the following:

- Providing a console for system administrators and service representatives to manage server hardware
- Creating and maintaining a multiple partitioned environment on a managed system
- Detecting, reporting, and storing changes in hardware conditions.
- Acting as a service focal point for service representatives to determine an appropriate service strategy
- Displaying operating system session terminals for each partition

The HMC machine code does not have provisions for loading or running additional applications that are not related to hardware management or service. All the tasks you need to maintain the managed system, the underlying operating system, and the HMC's machine code are available by using the HMC's management interface.

Managed System Operation

The HMC's graphical user interface provides the functions needed to create and maintain a partitioned environment on a managed system. Using the interface allows for direct manipulation of HMC-defined objects and increased information regarding detected changes in hardware conditions.

The managed system can be run as a partitioned system, sometimes referred to as *logically partitioned* (LPAR). This means that the managed system can run multiple operating systems simultaneously. The system can also run as a large single partition, which is known as the *manufacturing default configuration* when the system is delivered. If the system has been partitioned, then a the single partition that uses all the system resources is referred to as a *full system partition*.

Partitioning provides users with the ability to divide a single managed system into several systems. Each of these systems, running in a partition, is capable of running applications in multiple, independent environments simultaneously. Logical partitioning makes it possible for a user to run a single application using different sets of data on separate partitions, as if that application were running independently on separate physical systems. By creating partitions, for example, a company can test its programs in one partition while developing the same program in another, at the same time, all using the same system. This "same system" partitioning method is more cost-effective, potentially eliminating the need for a separate test system.

The full system partition is no different from the traditional way of using a system. The single server uses all of its resources as one system.

Powering On and Off

During the process of powering on, the HMC checks to see which managed systems are available and communicating with the console. To ensure that each managed system is available before you power on the HMC, managed systems must be in "standby mode" or actively operating. Standby mode is indicated by the `OK` shown in the operator panel after the managed system has the power connected and the initial tests are complete.

Note: If the managed system is in an emergency power off (EPOW) condition, the managed system must be brought to "standby mode" before the HMC can be used to power on the system.

To power on the HMC, do the following:

1. Press the Power button once to turn on the power.
2. When the system has finished the power-on self-test (POST), log in to the HMC by using your service representative name and password.

To power off the HMC, do the following:

1. Log in to the HMC and select **Power Off**.
2. The HMC shuts down any applications that are running, and then turns off the HMC.

Power-On Self-Test

After power is turned on and before the operating system is loaded, the system 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, codes indicating the progress of the POST might appear on the display. After the POST is complete, the HMC operating machine code loads and a login prompt appears.

Specifications and system unit locations

For information about system specifications and system unit locations, use the following procedure to go to the PC hardware maintenance manuals:

1. Go to the Personal computing support Web site (http://www.pc.ibm.com) .
2. In the left navigation bar, select **Support**.
3. Select **Search PC support**.
4. Search on the machine type for the PC server on which your HMC is based. The following table contains a cross reference to help you match your HMC machine type and model number to the equivalent PC server machine type and model number.

Your HMC machine type and model number (available on the serial number plate of your HMC)	Equivalent PC server machine type and model number	Supporting hardware maintenance
7310 Model CR2	8676 Model 22X	48P9908
7310 Model C03	8187 Model F4U	74P2661

HMC external AC power cable

To avoid electrical shock, a power cable with a grounded attachment plug is provided. Use only properly grounded outlets.

Power cables used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA). These power cords consist of the following:

- Electrical cables, type ST
- Attachment plugs complying with National Electrical Manufacturers Association (NEMA) L6-30P
- Appliance couplers complying with International Electrotechnical Commission (IEC) Standard 320, Sheet C13 and C14

Power cables used in other countries consist of the following:

- Electrical cables, type HD21 or HD22
- Attachment plugs approved by the appropriate testing organization for the specific countries where they are used
- Appliance couplers complying with the International Electrotechnical Commission (IEC) Standard 320, Sheet C13 and C14

Using System Management Services (SMS)

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.

Notes:

1. If the firmware console is a graphics terminal, you will be asked to enter the password for the service processor's admin user that was set using the Advanced System Management Interface (ASMI).
2. On some of the system management services (or service processor) screens, you will see the term *LPAR*. LPAR is equivalent to the term *logically partitioned server* or *partitioned server*.
3. In a partitioned server, only those devices that are assigned to the partition that is being booted display in the SMS menus. In a partition that uses all the resources in a server, all devices in the system display in the SMS menus.
4. In some of the following example screens, U*n* is used in place of U*feature_code.model.serial number* for legibility.

To start the system management services, do the following:

1. For a server that is connected to an HMC, use the HMC to restart the server or partition.

   If the server is not connected to an HMC, stop the system, and then restart the server by pressing the power button on the control panel.
2. For a partitioned server, watch the virtual terminal window on the HMC.

   For a full server partition, watch the firmware console.
3. Look for the POST indicators **memory, keyboard, network, scsi, speaker**, which appear across the bottom of the screen. Press the numeric 1 key after the word **keyboard** appears, and before the word **speaker** appears.

After the system management services starts, the following screen displays:

```
Main Menu

 1   Select Language
 2   Setup Remote IPL (Initial Program Load)
 3   Change SCSI Settings
 4   Select Console
 5   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: _
```

Note: The system management services can also be started using the Service Processor Boot Mode Menu.

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 previous 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** returns you 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 TTY 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: _
```

Setup remote IPL (Initial Program Load)

This option allows you to enable and set up the remote startup capability of your server or partition. A list of NIC (network interface card) adapters in the server displays first. An example of this screen follows:

Attention: In a partitioned server, only those network adapters that have been assigned to the partition being booted display in the IP Parameters menu. In a full system partition, all network adapters in the system are listed in the adapter parameters menu.

```
NIC Adapters
         Device                       Slot                 Hardware Address
1.    Port 1 - 2 PORT Gigabit Et       Un-P1-T9                 00096bff616b
2.    Port 2 - 2 PORT Gigabit Et       Un-P1-T10                00096bff616a
3.    10/100/1000 Base-TX PCI-X        Un-CB1-C03-T1            000295e3814f



-------------------------------------------------------------------------------------------------
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 an adapter is selected, the Network Parameters menu displays:

```
Network Parameters
Port 1 - 2 PORT Gigabit Et    Un-P1-T9     00096bff616b
 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
Port 1 - 2 PORT Gigabit Et    Un-P1-T9     00096bff616b
 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. Entering IP parameters on this screen will automatically update the parameters on the ping test screen.

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

Selecting **Adapter Configuration** allows the setting of the network speed, enabling or disabling spanning tree, and setting the protocol as shown in the following example menu:

```
Adapter Configuration
Port 1 - 2 PORT Gigabit Et    Un-P1-T9     00096bff616b
1.  Speed, Duplex
2.  Spanning Tree Enabled
3.  Protocol




-------------------------------------------------------------------------------------------------
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 **Speed, Duplex** option allows you to set the interface speed at which the card will run and half versus full duplex. The current setting is indicated by "<===".

```
Adapter Configuration
Port 1 - 2 PORT Gigabit Et    Un-P1-T9     00096bff616b

1.  auto, auto
2.  10,half
3.  10,full
4.  100,half
5.  100,full




-------------------------------------------------------------------------------------------------
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 **Spanning Tree Enabled** menu allows you to enable or disable the spanning tree flag. If this flag is enabled (because the network the system is being attached to supports spanning trees), the firmware will impose a waiting period of 60 seconds before the adapter is allowed to communicate with the network. If this flag is disabled, the network adapter will be able to access the network immediately after the system is connected.

The **Protocol** option allows you to set the appropriate protocol for your network as shown below.

```
Protocol
Port 1 - 2 PORT Gigabit Et    Un-P1-T9     00096bff616b

 1. Standard  <===
 2. IEEE802.3




-------------------------------------------------------------------------------------------------
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 the **ping test** option from the network parameters menu to test an adapter's network connection to a remote system. After the ping test option is selected, the same series of screens will take you through setting up the IP parameters and the adapter configuration before attempting the ping test.

Notes:

1. Once the ping test is initiated, it may take 60 seconds or longer 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 allows 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 option is not available on partitioned systems.

The Select Console utility allows the user to select which console 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 automatically returns 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: _
```

Select Install or Boot Device

Allows you to select a device from which to boot or install the operating system. This option is for the current boot only.

Select Boot Devices
Allows you to set the boot list.

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

If **Select Install or Boot Device** 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 is not 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, a menu similar to the following 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 **SCSI** is selected, for example, all of the SCSI adapters that are in the system, or assigned to the partition, are shown on the next screen. Depending on the devices that are installed in your system, a menu similar to the following displays:

```
Version SF220_014
SMS 1.5 (c)  Copyright IBM Corp. 2000, 2003 All rights reserved.
-------------------------------------------------------------------------------------------------

Select Media Adapter
1.  Un-P1-T14 /pci@800000020000000d/pci@2/pci1069,b166@1/scsi@0
2.  Un-P1-T12 /pci@800000020000000f/pci@2,2/pci1069,b166@1/scsi@0
3.  Un-P1-T13 /pci@800000020000000f/pci@2,2/pci1069,b166@1/scsi@1
4.  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 an adapter is selected, the next screen displays the devices of the requested type that are attached to that adapter. In the following example, all of the SCSI hardfiles that are attached to the first adapter are listed:

```
Version SF220_014
SMS 1.5 (c)  Copyright IBM Corp. 2000, 2003 All rights reserved.
-------------------------------------------------------------------------------------------------
Select    Device
Device    Current      Device
Number    Position     Name

1           1         SCSI 73407 MB Harddisk Un-P1-T14 /pci@800000020000000d/pci@2/
                       pci1069,b166@1/scsi@0




-------------------------------------------------------------------------------------------------
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 installation or boot.

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 73407 MB Harddisk Un-P1-T14 /pci@80000002000000d/pci@2/pci1069,b166@1/scsi@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

Attention: In a partitioned system, only those devices from which an operating system can be booted that are assigned to the partition that is being booted display on the select boot devices menu. In a full system partition, devices from which an operating system can be booted display on the Select Boot Devices menu.

Note: To keep the search time for bootable devices down, these menus follow a hierarchy of:

`device type -> bus type -> adapter -> devices attached to the adapter`

To view all of the potentially bootable devices at one time rather than traversing down the hierarchy with the submenus, go to the ″Select Device Type″ menu or the ″Select Media Type″ menu and select the last option, ″List All Devices″.

The ″List All Devices″ function may take a long time on a large system with many I/O adapters and devices, such as large disk arrays.

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 will be displayed, which is 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, such as item 5, a Select Media Type menu is displayed. The following is an example of that menu.

```
 Select Media Type
 1.  SCSI
 2.  SSA
 3.  SAN
 4.  IDE
 5.  ISA
 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 the media type is selected, all adapters of that type are displayed on the Select Media Adapter menu. The following is an example of that menu for a SCSI media type.

```
Version SF220_014
SMS 1.5 (c)  Copyright IBM Corp. 2000, 2003 All rights reserved.
-------------------------------------------------------------------------------

Select Media Adapter
1.  Un-P1-T14 /pci@800000020000000d/pci@2/pci1069,b166@1/scsi@0
2.  Un-P1-T12 /pci@800000020000000f/pci@2,2/pci1069,b166@1/scsi@0
3.  Un-P1-T13 /pci@800000020000000f/pci@2,2/pci1069,b166@1/scsi@1
4.  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: _
```

Each adapter must then be selected individually to see the devices that are attached to it. An example of this menu for the first adapter in the previous example is as follows:

```
Version SF220_014
SMS 1.5 (c)  Copyright IBM Corp. 2000, 2003 All rights reserved.
-------------------------------------------------------------------------------------------------
Select    Device
Device    Current      Device
Number    Position     Name

1           1         SCSI 73407 MB Harddisk Un-P1-T14 /pci@80000002000000d/pci@2/
                       pci1069,b166@1/scsi@0




-------------------------------------------------------------------------------------------------
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 there are no devices of the type chosen earlier (on the Select Device Type menu) attached to the adapter that is specified, a message similar to the following displays:

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

When a device type is selected, the Select Task menu allows you to see detailed information about the device or set the device's location in the boot list as shown below in the example menu. The following is an example of the menu for a hard disk.

```
 Select Task

SCSI 73407 MB Harddisk Un-P1-T14 /pci@80000002000000d/pci@2/pci1069,b166@1/scsi@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@8000000200000dd/pci@2/pci1069,b166@1/scsi@1/sd@5,0
                    :  (Bootable)
DEVICE              : SCSI 73407 MB Harddisk Un-P1-T14 /pci@80000002000000d/pci@2/
                      pci1069,b166@1/scsi@0
NAME                : sd
DEVICE-TYPE         : block

Parent Information
IBM,FW-ADAPTER-NAME: Ultra-320
NAME                : scsi
DEVICE-TYPE         : scsi-2



-------------------------------------------------------------------------------------------------
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 73407 MB Harddisk Un-P1-T14 /pci@80000002000000d/pci@2/pci1069,b166@1/scsi@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 as follows:

1. Primary diskette drive (if installed)
2. Optical drive (if installed)
3. Tape drive (if installed)
4. Hard disk drive (if installed)
5. Network adapter

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.

Component and attention LEDs

This topic contains information about component and attention LEDs, which assist in identifying failing components in your server. If a failing component is detected in your system, an amber-colored attention LED on the operator panel is turned on solid (not blinking). To further identify the failing FRU, the service processor menus (available from the Advanced System Management Interface) or AIX Service Aid menu can be used to blink the FRU LED for the failing FRU. For details about each LED, chose the server from the list below to go to the appropriate section:

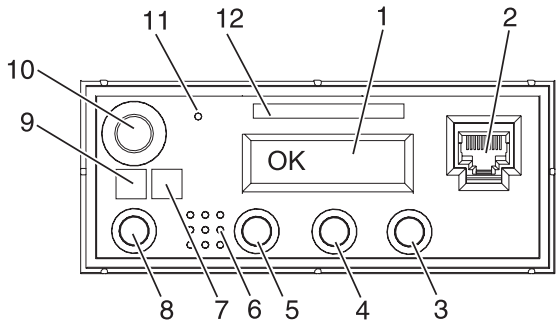
520 component and attention LEDs

570 component and attention LEDs

520 component and attention LEDs

This section contains information regarding the component LED indicators, such as the operator panel, power supplies, PCI adapters and so on for the 520 server.

520 operator panel display



Number	Name	Description
1	Display	Displays current status of system startup, or diagnostic information in the event of a hardware problem.
2	Front serial connector (FS1)	Serial port uses RJ-45 connector. Use to plug in external devices at the front of the system unit.
3	Increment up	Scrolls the information in the display up.
4	Enter	Enter
5	Increment down	Scrolls the information in the display down.
6		
7	Attention LED	Normal State - LED is off
8	System reset button	Resets the system

Number	Name	Description
9	Power LED	Blinking - When connected to the power source (System is in standby mode). Solid - When power button has been pressed. **Note:** There is approximately a 30-second transition period from the time the power-on button is pressed to when the power LED goes from blinking to on solid. During the transition period, you may observe the blinking intervals speed up.
10	Power-on button	Turns the system power on and off.
11	Service processor reset switch (pinhole)	Service Personnel Use
12	Serial number label	Displays the system serial number

520 Component LEDs

Individual LEDs are located on or near the failing field replaceable unit (FRU). The LEDs are located either on the component itself or on the carrier of the component (for example, memory card, fan, memory module, CPU). LEDs are either green or amber.

Green LEDs indicate either of the following:

- Electrical power is present.
- Activity is occurring on a link. (The system could be sending or receiving information.)

Amber LEDs indicate a fault or identify condition. If your system or one of the components in your system has an amber LED turned on or blinking, identify the problem and take the appropriate action to restore the system to normal.

The following table identifies the location, color and status of your system component LEDs.

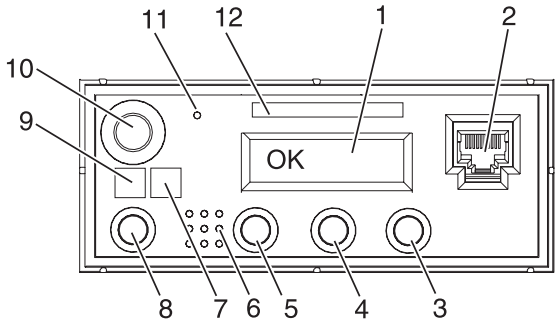
Unit (FRU)	LED Function	Location	Viewable Location	LED Color	OFF	ON	Blink
Power and Packaging LEDs							
System	Attention	Operator panel and rear	External front and rear	Amber	Normal	Fault	Identify
	Power			Green	No ac	System on	Standby
Fan	Identify	Part	Internal	Amber	Normal	n/a	Identify
Power supply	AC input good	Part	Internal	Green	No Input	Input good	n/a
	Identify	Part	Internal	Amber	Normal	Fault	Identify
	DC output good	Part	Internal	Green	All power supply outputs off	All power supply outputs on	Control voltage good
Disk drives	Activity	Disk drive carrier	Front of system unit	Green	No disk activity	Disk being accessed	n/a

Unit (FRU)	LED Function	Location	Viewable Location	LED Color	OFF	ON	Blink
CARD LEDs							
PCI slots	Power	Socket	External	Green	No power	Power on	n/a
	Identify	Socket	External	Amber	Normal	n/a	Identify
RIO-G	Identify	Socket	External	Amber	Normal	n/a	Identify
Memory DIMMs	Identify	Memory Connector	Internal	Amber	Normal	n/a	Identify
System backplane	Identify	Planar	Internal	Amber	Normal	n/a	Identify
Disk drive backplane	Identify	Card	Internal	Amber	Normal	n/a	Identify
Media backplane	Identify	Card	Internal	Amber	Normal	n/a	Identify
Service processor card	Identify	Card	Internal	Amber	Normal	n/a	Identify
Voltage regulator module	Identify	Card	Internal	Amber	Normal	n/a	Identify
RAID adapter card	Identify	Card	External	Amber	Normal	n/a	Identify
HMC port	Link	Service processor card	External	Green	No link	Link	n/a
	Activity	Service processor card	External	Green	No activity	n/a	Activity
Imbedded Ethernet	Link	Service processor card	External	Green	No link	Link	n/a
	Activity	Service processor card	External	Green	No activity	n/a	Activity

570 component and attention LEDs

This section contains information regarding the component LED indicators, such as the operator panel, power supplies, PCI adapters and so on for the 520 server.

570 operator panel display



Number	Name	Description
1	Display	Displays current status of system startup, or diagnostic information in the event of a hardware problem.
2	Front serial connector (FS1)	Serial port uses RJ-45 connector. Use to plug in external devices at the front of the system unit.
3	Increment up	Scrolls the information in the display up.
4	Enter	Enter
5	Increment down	Scrolls the information in the display down.
6		
7	Attention LED	Normal State - LED is off
8	System reset button	Resets the system
9	Power LED	Blinking - When connected to the power source (System is in standby mode). Solid - When power button has been pressed. **Note:** There is approximately a 30-second transition period from the time the power-on button is pressed to when the power LED goes from blinking to on solid. During the transition period, you may observe the blinking intervals speed up.
10	Power-on button	Turns the system power on and off.
11	Service processor reset switch (pinhole)	Service Personnel Use
12	Serial number label	Displays the system serial number

570 Component LEDs

Individual LEDs are located on or near the failing field replaceable unit (FRU). The LEDs are located either on the component itself or on the carrier of the component (for example, memory card, fan, memory module, CPU). LEDs are either green or amber.

Green LEDs indicate either of the following:

- Electrical power is present.
- Activity is occurring on a link. (The system could be sending or receiving information.)

Amber LEDs indicate a fault or identify condition. If your system or one of the components in your system has an amber LED turned on or blinking, identify the problem and take the appropriate action to restore the system to normal.

The following table identifies the location, color and status of your system component LEDs.

Unit (FRU)	LED Function	Location	Viewable Location	LED Color	OFF	ON	Blink
Power and Packaging LEDs							
System	Attention	Operator panel and rear	External front and rear	Amber	Normal	Fault	Identify
	Power			Green	No ac	System on	Standby
Fans	Identify	Part	Internal	Amber	Normal	n/a	Identify

Unit (FRU)	LED Function	Location	Viewable Location	LED Color	OFF	ON	Blink
Power and Packaging LEDs							
Power supply	AC input good	Part	External rear	Green	No Input	Input good	n/a
	Identify	Part	External rear	Amber	Normal	Fault	Identify
	DC output good	Part	External rear	Green	All power supply outputs off	All power supply outputs on	Control voltage good
Media device	Identify	Card	Internal	Amber	Normal	n/a	Identify
Disk drives	Activity	Disk drive carrier	Front of system unit	Green	No disk activity	Disk being accessed	n/a

Unit (FRU)	LED Function	Location	Viewable Location	LED Color	OFF	ON	Blink
CARD LEDs							
PCI slots	Power	Socket	External	Green	No power	Power on	n/a
	Identify	Socket	External	Amber	Normal	n/a	Identify
RIO-G expansion card	Identify	Card	External	Amber	Normal	n/a	Identify
RIO-G connector on expansion card	Identify	Card connector	External	Amber	Normal	n/a	Identify
RIO-G connector on expansion card	Identify	Card connector	External	Amber	Normal	n/a	Identify
Memory DIMMs	Identify	Memory Connector	Internal	Amber	Normal	n/a	Identify
System backplane (processor and regulator assembly)	Identify	Planar and cage assembly	Internal	Amber	Normal	n/a	Identify
Processor card	Identify	Card	Internal	Amber	Normal	n/a	Identify
Processor regulator card	Identify	Card	Internal	Amber	Normal	n/a	Identify
I/O backplane	Identify	Planar	Internal	Amber	Normal	n/a	Identify
Mid-plane backplane	Identify	Planar	Internal	Amber	Normal	n/a	Identify
Disk drive backplane	Identify	backplane mounted to disk drive cage	Internal	Amber	Normal	n/a	Identify
Media backplane	Identify	Card	Internal	Amber	Normal	n/a	Identify
Service processor card	Identify	Card	Internal	Amber	Normal	n/a	Identify

Unit (FRU)	LED Function	Location	Viewable Location	LED Color	OFF	ON	Blink
CARD LEDs							
Voltage regulator and card	Identify	Card	Internal	Amber	Normal	n/a	Identify
RAID adapter card	Identify	Card	Internal	Amber	Normal	n/a	Identify
HMC port	Link	Service processor card	External	Green	No link	Link	n/a
	Activity	Service processor card	External	Green	No activity	n/a	Activity
Imbedded Ethernet	Link	Service processor card	External	Green	No link	Link	n/a
	Activity	Service processor card	External	Green	No activity	n/a	Activity

Setting expansion unit configuration ID and MTMS value

The preferred method for setting the configuration ID is through the Advanced System Management Interface (ASMI), but it can also be performed using the physical control panel if the ASMI is unavailable.

The MTMS value for the unit should also be set to match the original value (located on the label or frame). Updating the MTMS value keeps the configuration and error information in sync, and is used by the system when creating the location codes. This must be done using the ASMI, **not** with the control panel. However, if you do not have access to the ASMI, the system will still operate without updating this information

Note: Refer to Accessing the Advanced System Management Interface for information on setting up the ASMI, and Managing your server using the Advanced System Management Interface for information on using the ASMI, including updating the system configuration settings.

Choose from the following:

- Using the ASMI to set the configuration ID
- Using the control panel to set the configuration ID

Using the ASMI to set the configuration ID

To perform this operation, the server must be powered on and your authority level must be one of the following:

- Administrator
- Authorized service provider

1. If the ac power is not applied, then apply it now.

   Note: The tower may power up automatically.

2. In some cases, FRU replacement will generate a new temporary unit value in both the expansion unit control panel and in HSM. Use this new value to power down the expansion tower without removing the power cord using “Powering off an expansion unit” on page 83. Then return here and continue with the next step.
3. On the ASMI welcome pane, specify your user ID and password, and click **Log In**.
4. In the navigation area, expand System Configuration and click **Configure I/O Enclosures**.
5. Select the unit identified by the new value in the panel of the unit you are working on. In most cases it will appear as ″TMPx.yyy.yyyyyyy″ where x is a hex digit, and the y’s are any value.
6. Select **change settings**.
7. Enter the Power Control Network Identifier:
   - 81 for 5074 and 5079 expansion units
   - 89 for 5088 and 0588 expansion units
   - 8A for 5094 and 5294 expansion units
   - 8B for 5095 and 0595 expansion units
   - 88 for 7311-D10, 7311-D11, and 5790 expansion units
   - 8C for 7311-D20 expansion units
8. Enter the type-model from the label on the I/O unit
9. Enter the serial number (also called sequence number) from the label on the I/O unit.
10. Click **Save Setting** to complete the operation.

    Attention: Do not use the browser back button or the values will not be saved.
11. Verify the correct value is now displayed in the panel of the unit you are working on.
12. Disconnect all ac power to the unit, wait for the display panel to go off, and then reconnect the ac power.

    Note: The tower will automatically power on.
13. Log off and close the ASMI and return to the procedure that sent you here.

Using the control panel to set the configuration ID

To perform this operation, the server must be powered on.

Control panel function 07 is used to query and set the configuration ID and to display the frame address of any tower connected to the SPCN network. Since the tower display panel will have the MTMS and not frame address displayed, a function is provided to display the frame address.

1. If the ac power is not applied, then apply it now.

   Note: The tower may power up automatically.
2. In some cases, FRU replacement will generate a new temporary unit value in both the expansion unit control panel and in HSM. Use this new value to power down the expansion tower **without** removing the power cord. See “Powering off an expansion unit” on page 83, then return here and continue with the next step.
3. Select function **07** on the control panel and press **Enter**.
4. Select sub function A6 to display the address of all units. The frame address is displayed on all units for 30 seconds.
5. Note the frame address on the unit that you are working on for use in the next steps.
6. Select sub function A9 to set the ID of a tower.
7. Use the arrow keys to increment/decrement to the first two digits of the frame address noted above.
8. Press enter
9. Use the arrow keys to increment/decrement to the last two digits of the frame address noted above.

10. Press enter
11. Use the arrow keys to increment/decrement to a configuration ID for the type of unit you are working on:
    - 81 for 5074 and 5079 expansion units
    - 89 for 5088 and 0588 expansion units
    - 8A for 5094 and 5294 expansion units
    - 8B for 5095 and 0595 expansion units
    - 88 for 7311-D10, 7311-D11, and 5790 expansion units
    - 8C for 7311-D20 expansion units
12. Press **Enter** (078x 00 will be displayed).
13. Use the arrow keys to increment/decrement until 07** is shown.
14. Press **Enter** to return the panel to 07.
15. Disconnect all ac power to the unit, wait for the display panel to go off and then reconnect the ac power.

    Note: The tower will automatically power on.
16. Continue with the next step to update the MTMS value using the ASMI. If you do not have access to the ASMI, then return to the procedure that sent you here.
17. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
18. In the navigation area, expand System Configuration and click **Configure I/O Enclosures**.
19. Select the unit identified by the new value in the panel of the unit you are working on. In most cases it will appear as "TMPx.yyy.yyyyyyy" where x is a hex digit, and the y's are any value.
20. Select **change settings**.
21. Enter the type-model from the label on the I/O unit
22. Enter the serial number (also called sequence number) from the label on the I/O unit.
23. Click **Save Setting** to complete the operation.

    Attention: Do not use the browser back button or the values will not be saved.
24. Verify the correct value is now displayed in the panel of the unit you are working on.
25. Log off and close the ASMI. Then return to the procedure that sent you here.

Updating the world-wide port name for a new 2766 or 2787 IOA

If you have exchanged a 2766 or 2787 Fibre Channel IOA, the IBM external storage subsystem must be updated to use the world-wide port name of the new 2766 or 2787 IOA. This name can be found on using the Hardware Service Manager in SST or DST. Display detail on the 2766 or 2787 IOA Logical Hardware Resource information, and use the port worldwide name field.

The 16-digit world-wide port name can also be determined by appending the digits "1000" to the beginning of the 12-digit IEEE address found on the tailstock label of the Fibre Channel IOA. For the IBM 2105 external storage subsystem, use the IBM TotalStorage Enterprise Storage Server User's Guide (SC26-7445) to update the world-wide port name in the host configuration. This guide can be found at the IBM TotalStorage Web site (http://www.storage.ibm.com/disk/ess/index.html) . In the Resources column select **Technical documentation** under Service and support.

System safety inspection

A safety inspection for the system should be performed:

- when it is inspected for an IBM maintenance agreement,
- when IBM service is requested and no service has recently been performed by IBM,
- when an alterations and attachments review is performed, or
- when changes have been made to the equipment that might affect its safety.

If the inspection indicates safety conditions that are not acceptable, the conditions must be corrected before IBM services the machine.

Note: The correction of any unsafe condition is the responsibility of the system owner.

While performing this inspection, special attention must be given to these areas:

- Feature and model changes and engineering change (EC) upgrades
- Additions of non-IBM power supplies or attachments
- Missing safety covers
- Removed, faded, or painted-over safety labels
- Replacement requirements concerning parts for primary power
- Any other items relating to the product's safety

Before you start, you must have completed the *Electrical Safety Education Course for IBM Service Representatives* (self-study course 77170 or equivalent).

You will need these items:

- An IBM service representative tool kit (or equivalent)
- A copy of Service Memorandums (SMs), which include engineering change announcements (ECAs) and service aids (SAs) documents for the system
- Latest machine history, if possible
- *Electrical Safety for IBM Service Representatives*, S229-8124
- A Fluke** 8060A digital voltmeter (part 8496278) or equivalent

Perform the following safety checks:

Covers

1. Check for any missing or damaged covers.
2. Check the covers for any sharp edges.

AC power cords

1. With the machine powered off, remove the power cord from the electrical outlet.
2. Check the power cord and power plug for visible cracks, wear, or damage.
3. Check for 1.0 ohm or less of resistance between the power cord ground and the power supply frame.
4. Ensure that the power cord is fully inserted and secured into position on the machine end.
5. Ensure that the power cord required for your country or region, and system, is installed. See Determine power cord, plug, and receptacle type) in the Planning topic.

AC safety grounds

1. Ensure that all power supply mounting screws are tight.
2. Ensure that the mounting screws of the ac module or internal uninterruptible power supply are tight.

Safety labels

Ensure that all the safety labels are visible and readable:

- Main power rating attached to the right side frame at the back of the machine.
- 240 V AC attached to each 23 pin connector (J2 and J3) on AC modules that have SPCN connectors (J15 and J16) (46G3576).
- Danger up to 240 V AC attached to the bottom frame under the power supplies (46G3575).
- Weight restriction label attached under the handle on the cover of the External Battery Backup Unit (74F9976).
- Main power rating attached to the left side frame at the back of the machine.
- Danger up to 240 V AC attached to the bottom frame under each power supply (90H6275).
- Caution Lead Acid battery attached to side of internal battery unit (21H7089).
- Weight restriction label attached to top of internal battery (74F9976).
- Weight restriction label attached to top of power sub-frame assembly (74F9976).
- Models 640, 730 and S30 only: Two weight restriction labels attached to SPD/DASD cage sub-frame assembly (74F9976).
- Two weight restriction labels attached to active back plane assembly (74F9976).
- Main power rating attached to back plate on external battery unit.
- Caution lead Acid battery label attached to back plate on external battery unit (21H7089).
- Weight restriction label attached to base at rear of external battery unit (74F9978).

Power off and on (system unit)

1. Ensure that the system powers off correctly.
2. Ensure that the system powers on correctly.

Internal mechanical inspection

1. Ensure that air moving device (AMD) shields are installed on the AC module AMD assembly.
2. Ensure that the electromagnetic compatibility (EMC) access plate is installed over the power supplies.
3. Ensure that the card retainers are installed on the front and back of the card enclosure.
4. Ensure that the latch to lock the bottom adapter card is installed on all Magnetic Storage IOP (2624) cards with part number 86G8317.
5. Ensure that the safety shield is installed over the left side of the expansion unit AMD assembly.
6. Check the external battery backup power supply cable (if present) for visible cracks, wear, or damage.

Models 640, 730, and S30 only:

1. Ensure that the retainer that holds the vertical SPD card separators is in place.
2. Ensure that the vertical rods between DASD units are in place (model 640, 730 and S30 only).
3. Ensure that the EMC access plate is installed over the charger and internal battery unit.
4. Ensure that the EMC access plates are installed over all cages.

Forms

"Problem reporting forms" on page 111

"Work with electrostatic discharge-sensitive parts" on page 113

"Service log" on page 114

"HSL cable location form" on page 116

Problem reporting forms

Use this form to record information displayed on the control panel or in the HMC when a problem occurs on the system.

Use one of the following forms, depending on whether you have a system in its manufacturing default configuration or a system with multiple logical partitions:

- System in its manufacturing default configuration
- System with multiple logical partitions

Problem reporting form for a system in its manufacturing default configuration

Collect as much of the following information as possible. If necessary, you can use both the control panel and the HMC to gather the information.

Required information	Your answers
Date and time that the problem occurred	
Describe the problem	
Machine type	
Model	
Serial number	
Operating system, version, and release	
IPL type	
IPL mode	
Message ID	
Message text	
From/send program	
Instruction number	
To/receive program	
Instruction number	
Service request number (SRN)	

Go to the HMC or the control panel and indicate whether the following lights are on:

Control panel light	Place a check if light is on
Power On	
System Attention	
Processor active	

Go to the HMC or control panel to find and record the values for functions 11 through 20. See Collecting reference codes and system information for step-by-step instructions on collecting reference codes. Use the following grid to record the characters shown on the HMC or Function/Data display.

11	__ __
12	__ __

13	__ __
14	__ __
15	__ __
16	__ __
17	__ __
18	__ __
19	__ __
20 (if you use the control panel)	__ __
20 (if you use the HMC)	Machine type: Model: Processor feature code: IPL type:

Problem reporting form for a system with multiple logical partitions

Collect as much of the following information as possible. For partitions, you must use the HMC to gather the information.

Required information	Your answers
Date and time that the problem occurred	
Describe the problem	
Machine type	
Model	
Serial number	
Logical partition state	
Logical partition ID	
Logical partition operating system, version, and release	
IPL type	
IPL mode	
Message ID	
Message text	
From/send program	
Instruction number	
To/receive program	
Instruction number	
Service request number (SRN)	

Go to the HMC or control panel and indicate whether the following lights are on:

Control panel light	Place a check if light is on
Power On	
System Attention	
Processor active	

Go to the HMC to find and record the values for functions 11 through 20. See Collecting reference codes and system information for step-by-step instructions on finding reference codes. Use the following grid to record the characters shown on the HMC.

11	__ __
12	__ __
13	__ __
14	__ __
15	__ __
16	__ __
17	__ __
18	__ __
19	__ __
20 (if you use the control panel)	__ __
20 (if you use the HMC)	Machine type: Model: Processor feature code: IPL type:

Work with electrostatic discharge-sensitive parts

When holding or installing electrostatic discharge-sensitive (ESD) parts, use the ESD handling kit (IBM part 6428316) or similar. Read the instructions inside the top cover of the carrying case.

All system logic cards are sensitive to electrostatic discharge. To prevent damage to ESD-sensitive logic cards, follow these instructions:

- Switch off power to the system or device before removing logic cards.
- Keep the ESD-sensitive card in the original shipping container until you install the card in the machine.
- When holding logic cards, move your body as little as possible to prevent an increase of static electricity from clothing fibers, carpet fibers, and furniture.

- Just before touching the ESD-sensitive card, discharge any static electricity in your body by touching the metal frame or cover of the machine. If possible, keep one hand on the frame when, for example, you are installing or removing a logic card.
- Hold the ESD-sensitive card by the edge or connector shroud cover. Do not touch the pins. If you are removing a field-replaceable module, use the correct tool.
- Return the card to the special container when it is not being used. Do not place the ESD-sensitive card on the machine cover or on a metal table. Machine covers and metal tables are electrical grounds. They make a discharge path from the ESD-sensitive card through your body to ground, increasing the risk of damage to the card. Large metal objects can be discharge paths without being grounded.
- Prevent ESD-sensitive cards from being touched accidentally by other persons. Reinstall machine covers when you are not working on the machine. Do not place unprotected ESD-sensitive cards on a table.
- Be careful when working with ESD-sensitive cards during cold weather heating. Cold weather heating causes low humidity and increases the risk of static electricity.

Service log

Machine type _____

Serial number _____

Logical partition _____

Date	Description of problem/action taken (do not record hours or part numbers.)	Service representative

Date	Description of problem/action taken (do not record hours or part numbers.)	Service representative

Date	Description of problem/action taken (do not record hours or part numbers.)	Service representative

HSL cable location form

Use this worksheet to determine the loop number, frame ID, and HSL port label for an HSL cable that you will be replacing. Record information in the table below when you are directed to do so.

Note: You may copy this form as necessary.

Table 1. HSL cable location form

Loop number	From frame ID	From HSL port label	To frame ID	To HSL port label
Hexadecimal loop number _____	Hexadecimal frame ID _____		Hexadecimal frame ID _____	
Decimal loop number _____	Decimal frame ID _____		Decimal frame ID _____	
Cable type (optical or copper) _____				

Chapter 2. Related information for service provider information

Listed below are the Web sites and Information Center topics that relate to the service provider information topic. You can view or print any of the PDFs.

Web sites

- iSeries Information Center
  (http://www.ibm.com/eserver/iseries/infocenter)
  The iSeries Information Center is a source for technical information about the iSeries server. The information center is your starting point for all iSeries technical information.

Other information

- Accessing the Advanced System Management Interface
- Installing features
- Managing your server using the Hardware Management Console
- Managing your server using the Advanced System Management Interface
- Troubleshooting

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

You need Adobe Acrobat Reader to view or print these PDFs. You can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

© Copyright IBM Corp. 2004

Appendix. 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 other country where such provisions are inconsistent with local law: THIS INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS 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.

Any references in this information to Web sites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this product and use of those Web sites is at your own risk.

The manufacturer may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning products not produced by this manufacturer was obtained from the suppliers of those products, their published announcements or other publicly available sources. This manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products not produced by this manufacturer. Questions on the capabilities of products not produced by this manufacturer should be addressed to the suppliers of those products.

All statements regarding the manufacturer's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

© Copyright IBM Corp. 2004

The manufacturer's prices shown are the manufacturer's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of the manufacturer.

The manufacturer has prepared this information for use with the specific machines indicated. The manufacturer makes no representations that it is suitable for any other purpose.

The manufacturer's 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 manufacturer's support websites for updated information and fixes applicable to the system and related software.

Trademarks

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

AIX
AIX 5L
e(logo)server
eServer
i5/OS
IBM
iSeries
pSeries

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Communications statements

The following Class A statements apply to these models:

5790
5791
5794
7311-D10
7311-D11
7311-D20
9111-520 (rack-mounted version)
9113-550
9117-570
9119-590
9119-595
9124-720
9405-520
9406-520
9406-550
9406-570
9406-595
9411-100

The following Class B statements apply to model 9111-520 (stand-alone version).

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504

Telephone: 1-919-543-2193

Industry Canada Compliance Statement

This Class A digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI Statement - Japan

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　ＶＣＣＩ－Ａ

The following is a summary of the VCCI Japanese statement in the box above.

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Electromagnetic Interference (EMI) Statement - People's Republic of China

Per GB 9254–1998, the user manual for a Class A product must carry the following warning message (English translation from the Chinese standard) about use in a residential environment in Chinese (*Simplified Chinese*):

声　明

此为Ａ级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

The following is a summary of the EMI Taiwan statement above.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user will be required to take adequate measures.

Radio Protection for Germany

Dieses Gerät ist berechtigt in Übereinstimmung mit Dem deutschen EMVG vom 9.Nov.92 das EG–Konformitätszeichen zu führen.

Der Aussteller der Konformitätserklärung ist die IBM Germany.

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse A. Für diese von Geräten gilt folgende Bestimmung nach dem EMVG:

Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.

(Auszug aus dem EMVG vom 9.Nov.92, Para.3, Abs.4)

Hinweis

Dieses Genehmigungsverfahren ist von der Deutschen Bundespost noch nicht veröffentlicht worden.

The following Statement applies to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables or connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interferences, and (2) this device must accept any interferences received, including interference that may cause undesired operation.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504

Telephone: 1-919-543-2193

Industry Canada Compliance Statement

This Class B digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to CISPR 22 / European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Properly shielded and grounded cables and connectors (IBM part number 75G5958 or its equivalent) must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for an interference caused by using other than recommended cables and connectors.

Terms and conditions for downloading and printing information

Permissions for the use of the information you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.

Personal Use: You may reproduce this information for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of this information, or any portion thereof, without the express consent of the manufacturer.

Commercial Use: You may reproduce, distribute and display this information solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of this information, or reproduce, distribute or display this information or any portion thereof outside your enterprise, without the express consent of the manufacturer.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the information or any data, software or other intellectual property contained therein.

The manufacturer reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the information is detrimental to its interest or, as determined by the manufacturer, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations. THE MANUFACTURER MAKES NO GUARANTEE ABOUT THE CONTENT OF THIS INFORMATION. THE INFORMATION IS PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

All material copyrighted by IBM Corporation.

By downloading or printing information from this site, you have indicated your agreement with these terms and conditions.

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. Information on product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

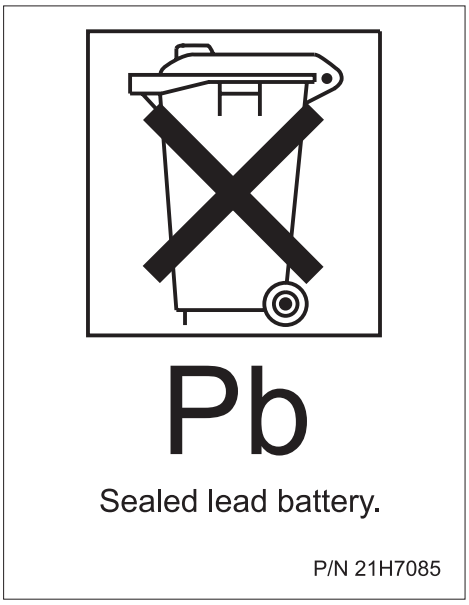
IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of programs and services to assist equipment owners in recycling their IT products. Information on product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

In the Netherlands, the following applies:



In Taiwan, the following applies. Please recycle batteries.

IBM Cryptographic Adapter Card Return Program

This machine may contain an optional feature, the cryptographic coprocessor card, which includes a polyurethane material that contains mercury. Follow local ordinances or regulations for disposal of this card. IBM has established a return program for certain IBM Cryptographic Adapter Cards. More information can be found at: http://www.ibm.com/ibm/environment/products/prp.shtml

Printed in USA