System i and System p

iSCSI Host Bus Adapter for IBM BladeCenter, System x, or xSeries

System i and System p

iSCSI Host Bus Adapter for IBM BladeCenter, System x, or xSeries

Note

Before using this information and the product it supports, read the information in "Notices" on page 39 and the *IBM Systems Safety Information* manual, G229-9054.

Fourth Edition (September 2007)

Contents

Safety and environmental notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

World Trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the U.S. English source. Before using a U.S. English publication to install, operate, or service this product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the U.S. English publications.

Laser safety information

IBM® System i® models and System p® servers can use I/O cards or features that are fiber-optic based and that utilize lasers or LEDs.

Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
This product might contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.**

(C026)

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

CAUTION:
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

Power and cabling information for NEBS (Network Equipment-Building System) GR-1089-CORE

The following comments apply to the IBM System i models and IBM System p servers that have been designated as conforming to NEBS (Network Equipment-Building System) GR-1089-CORE:

The equipment is suitable for installation in the following:

- Network telecommunications facilities
- Locations where the NEC (National Electrical Code) applies

The intrabuilding ports of this equipment are suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding ports of this equipment *must not* be metallically connected to the interfaces that connect to the OSP (outside plant) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Note: All Ethernet cables must be shielded and grounded at both ends.

The ac-powered system does not require the use of an external surge protection device (SPD).

The dc-powered system employs an isolated DC return (DC-I) design. The DC battery return terminal *shall not* be connected to the chassis or frame ground.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http://www.ibm.com/ibm/environment/products/prp.shtml.

EU Only

Note: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

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.

For Taiwan: Please recycle batteries.

For the European Union:

Note: This mark applies only to countries within the European Union (EU).

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California: Perchlorate Material - special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product/part may include a lithium manganese dioxide battery which contains a perchlorate substance.

IBM Cryptographic Coprocessor Card Return Program

The following information applies only for systems originally sold prior to July 1, 2006:

This machine may contain an optional feature, the cryptographic coprocessor card, which includes a polyurethane material that contains mercury. Please follow local ordinances or regulations for disposal of this card. IBM has established a return program for certain IBM Cryptographic Coprocessor Cards. More information can be found at http://www.ibm.com/ibm/environment/products/prp.shtml.

About this topic

This topic describes how to install, remove and replace the iSCSI Host Bus Adapter (iSCSI HBA) for attachment of IBM System x®, xSeries®, or blade servers to a partition running the i5/OS® operating system.

For information about the accessibility features of this product, for users who have a physical disability, see "Accessibility features," on page 37.

iSCSI Host Bus Adapter for IBM BladeCenter, System x, or xSeries

Learn how to install and configure, or remove and replace an iSCSI Host Bus Adapter (HBA).

This is a customer task. You can perform this task yourself, or contact a service provider to perform the task for you. You might be charged a fee by the service provider for this service.

Important: If you came to these instructions from the *iSCSI install read me first* Web page continue with this procedure. The iSCSI HBA initial installation is one part of a larger installation procedure guided by the *iSCSI install read me first* Web page. For the installation to be successful, you must follow the full procedure in order. If you are not following the path in the *iSCSI install read me first* Web page see http://www.ibm.com/systems/i/systemx/iscsi/readme/. If you do not follow the full procedure the installation will not be successful.

During the iSCSI HBA installation procedure, you need to refer to the following documentation to complete several steps:

- The worksheets you completed as a part of the *iSCSI Network Planning Guide* procedure.
- The documentation, in either hardcopy or on compact disc that came with your IBM System x, xSeries, or IBM BladeCenter® server.
- The System i System i integration with BladeCenter and System x Web site. This site has the latest iSCSI HBA information, including information about i5/OS program temporary fixes (PTFs) that are required to run the iSCSI HBA environment.
- The *Troubleshooting* Web page for integrated server solutions for help troubleshooting the installation.

The iSCSI HBA environment requires that at least one System x, xSeries, or blade server iSCSI HBA (initiator) is installed in a System x, xSeries, or BladeCenter server and that at least one iSCSI HBA (target) is installed in the hosting system as shown in the following figure. Multiple iSCSI HBAs can be installed in either the System x, xSeries, or blade server, or the hosting system. You can perform these installation steps multiple times to install a multiple adapter environment.

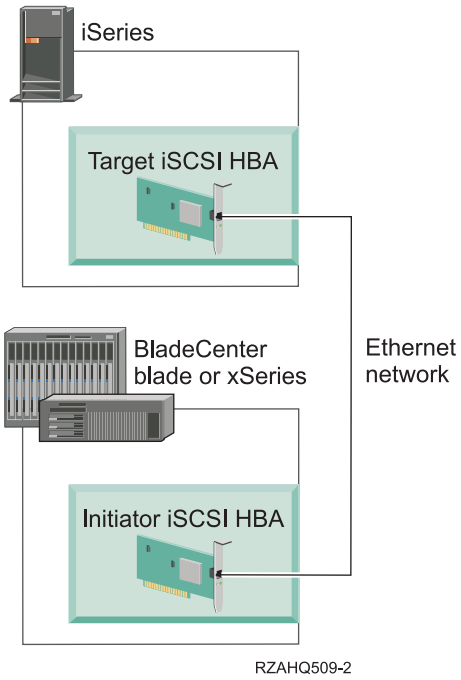

Figure 1. Simple iSCSI network

Related tasks

"Download BladeCenter or blade server firmware" on page 28
Learn how to locate, select, and download the needed firmware updates for your server. Use the instructions in this section to accomplish these tasks.

Related reference

"Download System x or xSeries firmware" on page 25
Learn how to download the latest firmware for your System x or xSeries server.

"Remove and replace the System x, xSeries, or blade server iSCSI HBA" on page 35
Learn the hardware and software configuration tasks to remove and replace an iSCSI HBA. Use the instructions in this section to accomplish these tasks.

Integrated server links

- http://www.ibm.com/systems/i/systemx/
- http://www.ibm.com/systems/i/systemx/iscsi/readme/
- http://www.ibm.com/systems/i/systemx/pdf/iscsi_planning.pdf
- http://www.ibm.com/systems/i/systemx/troubleshooting.html

PDF file for iSCSI Host Bus Adapter for IBM BladeCenter, System x, or xSeries

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select iSCSI Host Bus Adapter for IBM® xSeries or BladeCenter.

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 the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

---

iSCSI prerequisites

Learn the minimum hardware requirements for setting up your iSCSI network.

Ensure that you have the required hosting system hardware:

- iSCSI Host Bus Adapter: CCIN 573B for copper cabling, CCIN 573C for fiber optic cabling.
- Network adapter

  Tip: The network adapter does not need to be dedicated to the iSCSI HBA and might already be installed.

Ensure that you have the required hardware for an iSCSI network:

- Gigabit Ethernet switch (if not using BladeCenter I/O module switch).
- Ethernet cables (category 5e or better) or fiber optic cables.
  - One from each System x, xSeries, or blade system iSCSI HBA to network.
  - One from each hosting system iSCSI HBA to network.
  - One from each service processor hardware Ethernet port to network.
  - One from hosting system network adapter to network.
  - Any additional cables you might need to connect the Ethernet ports on the System x or xSeries server or BladeCenter to network, if desired.

Ensure that you have additional equipment and supplies you might need:

- Additional computer with a network interface capable of running web browser software (used to update and configure service processor hardware on System x, xSeries, or blade system) .
- Writable media diskettes or compact discs.

iSCSI IBM System x or xSeries prerequisites

Learn the minimum requirements for installing an iSCSI in an System x or xSeries server.

Ensure that you have the following before starting your installation:

- Diskless System x or xSeries server.
- iSCSI Host Bus Adapter for System x or xSeries server.
- Service processor hardware. Refer to the System i integration with BladeCenter and System x Web page to determine which of the following type of service processor hardware are required:
  - One of three versions of Remote Supervisor Adapter II (RSA II,) depending on System x or xSeries type and model: RSA II, RSA II – EXA, RSA II SlimLine
  - Baseboard Management Controller for System x or xSeries models that do not require the RSA II

- Mouse, keyboard, and display that can be attached through a KVM switch
- USB diskette drive. Some System x or xSeries models do not have an integrated diskette drive and require a diskette drive for firmware updates
- The documentation that is included with your System x or xSeries server (hardcopy or compact disc)

iSCSI blade server prerequisites

Learn the minimum requirements for a blade server installation.

Ensure that you have the following items before starting your installation:

- Diskless blade server.
- BladeCenter for housing blade servers.
- iSCSI expansion card or cards (also referred to as iSCSI HBA). Use one of these for each blade server you plan to attach.
- Management module installed in the BladeCenter to function as service processor hardware.
- I/O module in the appropriate BladeCenter I/O bay to support the network connection for the xSeries or blade system iSCSI expansion card. This I/O module can be an integrated gigabit switch which can take the place of an external switch in the iSCSI network or a pass-through module which would require an external switch.
- Mouse, keyboard, and display, which can be attached using a KVM switch.
- The documentation that is included with your BladeCenter, blade server and options – hardcopy, CD, or both.

Prepare your system

If this is the first iSCSI Host Bus Adapter (HBA) to be installed in your xSeries or blade server, follow the appropriate xSeries or blade server procedure before you install the iSCSI HBA.

"Prepare your System x or xSeries server"

"Prepare your blade server" on page 10

Prepare your System x or xSeries server

You might need to perform assembly, firmware update, and other preparation tasks to ensure your server is ready for a successful installation. Find instructions in the following sections to accomplish these tasks.

Preparing the System x or xSeries hardware

Locate information to assemble your server hardware.

The first step in preparing a System x or xSeries server is to assemble the hardware. This might include installing the keyboard, mouse, display, additional processors, additional memory and can also include options that may be required for the iSCSI Host Bus Adapter (HBA) solution, such as RSA II and the iSCSI HBA. Refer to System x or xSeries options documentation for details on how to install the System x or xSeries components.

Important: Do not connect any cables until instructed to do so. Connecting cables at the wrong point in the installation process may cause problems later.

Update the System x or xSeries firmware and configure the server

Perform the updates on all System x or xSeries servers to be attached.

Update the System x or xSeries server with the latest version of system basic input/output system (BIOS), Baseboard Management Controller firmware and system processor firmware.

Remember: You might be directed by the installation process on the *iSCSI install read me first* Web site to download the updates and return later to this document to apply the updates. If you have not already downloaded the firmware updates see "Download System x or xSeries BIOS firmware" on page 25.

Update System x or xSeries system BIOS

Preform these updates on all System x or xSeries servers that are to be attached.

Refer to the file named README you printed during the BIOS update download procedure. Use the README file instructions along with the steps below to perform the update. The README file contains any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur.

If you have not downloaded the BIOS update or printed the readme file see "Download System x or xSeries BIOS firmware" on page 25.

Perform the following steps on the server:

1. Plug the System x or xSeries server ac power cords into a power source. Refer to System x or xSeries documentation to complete this step.

2. Turn on the System x or xSeries server and insert the Flash BIOS update media in the appropriate drive. Refer to the server documentation to complete this step.
3. The system will start off of the media and present a window where you select **1 - Update POST/BIOS**.
4. On the next panel select 'Y' to move the current POST/BIOS image to the backup ROM location. The current code is copied to the backup bank immediately.
5. Select N for the next several display prompts until the **Save current flash code to disk prompt** is displayed.
6. Select N for the prompt to **Save current flash code to disk**.
7. Select the appropriate language, if prompted, or select the **Update BIOS** option. The update begins.
8. When the update is complete, remove the update media and turn the System x or xSeries server power off. Refer to System x or xSeries server documentation to complete this step.

Update System x or xSeries Baseboard Management Controller firmware

Learn how to apply the Baseboard Management Controller firmware update using the procedure in this section.

Refer to the README file printed earlier during the Baseboard Management Controller firmware download. If you have not already downloaded the README file or the firmware see "Download the Baseboard Management Controller firmware update" on page 26. Use the README instructions along with the following steps to perform the update. The README file contains any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur. The Baseboard Management Controller firmware should be updated whether or not an RSA II is installed in the System x or xSeries server.

This procedure should be performed on the System x or xSeries server.

1. Turn on the System x or xSeries server's power and insert the Baseboard Management Controller firmware update media in the appropriate drive. Refer to System x or xSeries server documentation to complete this step.
2. The update will load and start automatically. It can take several minutes to complete.
3. When the update completes, remove the media from the drive and turn off the System x or xSeries server's power. Refer to the System x or xSeries server documentation to complete this step.

Update firmware and configure System x or xSeries Remote Supervisor Adapter II

Learn how to apply the Remote Supervisor Adapter II firmware update and configure the adapter using the procedures in this section.

You may skip this section If the System x or xSeries server does not have an RSA II installed. Refer to the *iSCSI Network Planning Worksheets*, item XSP1, to determine whether or not to continue with this section.

If the System x or xSeries server requires you to install a System x or xSeries Remote Supervisor Adapter II (RSA II) option, install it before updating the firmware. After the RSA II is installed, connect it using an Ethernet cable to the Ethernet port on the computer containing the RSA II firmware update. Refer to the RSA II documentation to complete this action.

Tip: You may need a switch or hub to complete these connections depending on the location of the System x or xSeries server and the computer containing the update.
If you have not already downloaded the RSA II update see "Download Remote Supervisor Adapter II (RSA II) firmware" on page 26.

The procedure below assumes the RSA II is set to its factory default values. If the RSA II IP address is no longer known, it can be set back to the defaults, using the Setup utility, by following the instructions in the section "Alternate method to update Remote Supervisor Adapter II network configuration to defaults" on page 27.

Refer to the README file printed earlier during the RSA II firmware download. Use the README file instructions along with the steps below to perform the firmware update. The README file will contain any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur.

Note: The following steps are performed on the computer containing the update package (not on the System x or xSeries console):

Update RSA II firmware

Learn how to apply the RSA II firmware update.

Refer to the README file printed earlier during the RSA II firmware download. Use the README file instructions along with the following steps to perform the firmware update. The README file can contain any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur.

Note: The following steps are performed on the computer containing the update package (not on the System x or xSeries console):

1. Set the IP address to a value in the same subnet as the RSA II default IP address of 192.168.70.125. For example you can set the IP address to 192.168.70.101 with a subnet mask of 255.255.255.0.
2. Extract the files from the .zip file that you downloaded earlier to unpack the firmware update files.
3. Ensure the System x or xSeries ac power cords are attached to a power source. Refer to System x or xSeries documentation to complete this step. Wait at least 30 seconds following this step to allow the RSA II hardware to start.
4. Open a Web browser. In the address field, type the IP address (192.168.70.125) of the RSA II to which you want to connect. The *Enter Password* window opens.
5. Type the user name and password on the *Enter Password* window. The RSA II has a default user name of `USERID` and password of `PASSW0RD` (where 0 is a zero not the letter O).
6. Select a timeout value on the next screen and click continue.
7. If the next window is the **System Status** window, on the navigation pane on the left, under **Tasks**, click **Firmware Update**. If the RSA II firmware does not support the server on which it is installed, a warning window stating that the RSA II does not have firmware that supports the server is displayed. Click **OK** to continue.
8. At the next display, select **Browse** and navigate to the files containing the firmware update. The files will have an extension of .PKT; and there might be multiple files with this extension.
9. Select one of these files, and then click **Open**. The full path of the selected file is displayed in the Browse field.
10. To start the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the Remote Supervisor Adapter II. A confirmation window is displayed when the file transfer is complete.
11. Verify that the file shown on the Confirm Firmware Update window is the one you want to update. If not, click **Cancel**.
12. To complete the update process, click **Continue**. A progress indicator opens as the firmware on the Remote Supervisor Adapter II is copied. A confirmation window is displayed when the update completes.
13. Repeat the update procedure for any other .PKT files.

Configure the RSA II

You must configure a number of parameters in the RSA II before proceeding with the installation process. Refer to section 3.2 in the *iSCSI Network Planning Guide* for detailed information required to configure the RSA II. This process picks up from any of the screens after signon on the RSA II web browser interface.

Before you begin: Be sure to have the *iSCSI Network Planning Worksheets* handy; you will need information from them as you complete this task.

1. Navigate to the RSA II Web browser interface.
2. Select **Login Profiles** from under **ASM Control** in the navigation pane on the left side of the screen.
3. From the list of login IDs, find the entry for the default login ID value of **USERID** and click that entry.
4. The Login Profile window is displayed do the following:
   a. Change the **Login ID** (worksheet item XSP7) and fill in the **Password** (worksheet item XSP8) and **Confirm password** fields based on the information entered in the *iSCSI Network Planning Worksheets*.
   b. Ensure the **Authority Level** is set to **Supervisor**.
   c. Click **Save**.
5. On the navigation pane on the left side of the window, select **Network Interfaces** under **ASM Control** to start the configuration.
6. Use the values in the *iSCSI Network Planning Worksheets* to complete the following steps:
   a. Select **Enabled** from the **Interface** list.
   b. From the **DHCP** list select and set one of the following (worksheet item XSP3):
      1) **Disabled - Use static IP configuration**.
      2) **Enabled - Obtain IP config from DHCP server**. This option requires an operating DHCP server when you install the operating system.
   c. Enter a name for this RSA II in the **Hostname** (worksheet item XSP2) field.
   d. Enter a value for the following fields under the **Static IP Configuration** heading need to be filled in if the **Disabled – Use static IP** configuration value was selected for the **DHCP** field above:
      - **IP address** – type in the IP address (worksheet item XSP4).
      - **Subnet mask** – type in the desired subnet mask (worksheet item XSP5).
      - **Gateway address** – type in the gateway address (worksheet item XSP6).
   e. Click **Save** to complete configuring the network interfaces.
7. Select **System Settings** under **ASM Control** on the navigation pane on the left side of the window.
8. On the next window under the **ASM Information** heading, use the **Host OS** list to select a value of **Other**.
9. On the same window, under the heading **ASM Date and Time**, click **Set ASM Date and Time**.
10. On the next window, set the current date and time (using a 24-hour clock) and use the **GMT offset** list to select the appropriate time zone. Also, select the box to automatically adjust for daylight savings time, if necessary. Click **Save** to complete.
11. When all the updates and configuration steps are complete, select **Restart ASM** on the navigation pane to restart the Remote Supervisor Adapter II.
12. Click **OK** to confirm that you want to restart the Remote Supervisor Adapter II. A window is displayed advising that the browser window will be closed. Click **OK** to continue.

Update the System x or xSeries iSCSI HBA firmware

If update media for the iSCSI HBA firmware was built during the download process, it should be applied at this time. Use the procedure in this section to accomplish this task.

1. Plug the ac power cords into a power source. Refer to System x or xSeries documentation to complete this step.

2. Turn on the System x or xSeries server power. Insert the media containing the iSCSI HBA update in the drive. Refer to the System x or xSeries documentation to complete this step.
3. Wait for the server to complete POST. It should then access the media drive with the update and proceed to start. It will take several minutes to complete this.
4. The System x or xSeries server should boot to the update utility, which will present a window informing about the contents of the update. Type y to continue with the update. Note that if multiple iSCSI HBAs are installed, the update will be performed on all.
5. When the update completes, the media can be removed and the server's power can be turned off Refer to System x or xSeries server documentation to complete this step.

Set the System x or xSeries start options

You will need to configure several Start Options before continuing with the installation. Use the procedure in this section to accomplish this task.

It is recommended that you disable the Pre-Boot Execution Environment (PXE) option for all integrated Ethernet ports. You must turn the boot fail counter and virus detection off.

1. Turn on the System x or xSeries server. Refer to the server documentation to complete this step.
2. Press F1 when prompted to enter setup. This will be shortly after the IBM eServer™ logo appears on the display.
3. Highlight **Start Options** using the up or down arrow keys and press Enter to select.
4. Highlight **Planar Ethernet PXE/DHCP** using the up or down arrow keys. Use the right or left arrow keys to change the value to **Disabled**.
5. Highlight **Boot Fail Count** using the up or down arrow keys and use the right or left arrow keys to change the value to **Disabled**.
6. Highlight **Virus Detection** using the up and down arrow keys and use the right or left arrow keys to change the value to **Disabled**.
7. Press the Escape (Esc) key to return to the main setup menu.

Configure the Baseboard Management Controller

Preform the configuration steps only on System x or xSeries servers without an RSA II. Refer to worksheet item XSP1 in the *iSCSI Network Planning Worksheets* to determine this.

Before you begin: Be sure to have the *iSCSI network planning worksheets* handy; you will need information from them as you complete this task.

1. From the main setup menu, highlight **Advanced Setup** using the up or down arrow keys and press Enter to select.
2. Look for **RSA II Settings**.
   - If **RSA II Settings** exist, this indicates RSA II hardware is installed and the Baseboard Management Controller does not need to be configured. In this case, skip to the last step of this procedure.
   - If there are no **RSA II Settings**, RSA II hardware is not installed and you must continue with this procedure to configure the Baseboard Management Controller.
3. Highlight **Baseboard Management Controller (BMC) Settings** using the up or down arrow keys and press Enter.
4. Highlight **BMC Network Configuration** using the up or down arrow keys and press Enter to select.
5. Highlight **Static IP Address** (worksheet item XSP4) using the up or down arrow keys and use the backspace key to position the cursor for entry of the IP address from the *iSCSI Network Planning Worksheets*.

6. Highlight **Subnet Mask** (worksheet item XSP5) using the up or down arrow keys and use the backspace key to position the cursor for entry of the subnet mask from the *iSCSI Network Planning Worksheets*.
7. Highlight **Gateway** (worksheet item XSP6) using the up or down arrow keys and use the backspace key to position the cursor for entry of the gateway address from the *iSCSI Network Planning Worksheets*.
8. Highlight **Save Network Settings in BMC** using the up or down arrow keys and press Enter to select and perform the action. This will bring up the **BMC Settings saved!** screen.
9. Press Enter to return to the **Baseboard Management Controller (BMC) Settings** menu.
10. Highlight **User Account Settings** using the up or down arrow keys and press Enter.
11. Highlight **UserID 2** using the up or down arrow keys and press Enter.
12. On the **UserID 2 Account Settings** screen, highlight **UserID 2** using the up or down arrow keys and use the left or right arrow keys to change the value to **Enabled**.
13. Highlight **Username** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the field using the information from worksheet item XSP7 in the *iSCSI Network Planning Worksheets*.
14. Highlight **Password** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the field using the information from worksheet item XSP8 in the *iSCSI Network Planning Worksheets*.
15. Highlight **Confirm Password** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the same password as above.
16. Highlight **Privileged Limit** using the up or down arrow keys and use the left or right arrow keys to change the value to **Administrator**.
17. Highlight **Save User Account Settings to BMC** using the up or down arrow keys and press Enter.
18. The **BMC User Account Settings Saved!** Screen will be displayed. Press Enter to return to the **User Account Settings** menu.
19. Press Esc to return to the **Baseboard Management Controller (BMC) Settings** menu.
20. Press Esc to return to the *Advanced Setup* menu.
21. Press Esc to return to the main setup menu.

Complete the xSeries configuration

Complete the configuration of the System x or xSeries server using the procedure in this section.

1. From the main setup menu, highlight **Save Settings** using the up or down arrow keys and press Enter.
2. From the *Save Settings* window, press Enter to save.
3. From the main setup menu, press Esc to exit setup.
4. From the *Exit Setup* window, use the up or down arrow keys to highlight **Yes, exit the Setup Utility** and press Enter.
5. The System x or xSeries power can now be turned off. Refer to the System x or xSeries documentation to complete this step.

Prepare your blade server

You might need to perform assembly, configuration, and other preparation tasks to ensure your server is ready for installation. Use the instructions in this section to accomplish these tasks.

Assemble the BladeCenter and blade server hardware

The blade server iSCSI HBA is installed in the blade server to be attached. Perform the procedures in this section on all blade servers to be attached.

The first step in preparing the BladeCenter is to install the BladeCenter and blade server hardware. This may include installing any management modules, power modules, and I/O modules in the BladeCenter. The BladeCenter might have these components already installed if an additional blade server is being added to an already functioning BladeCenter. Before installing the blade servers in the BladeCenter, any blade server options must be installed. This may include additional processors, additional memory and the iSCSI HBA expansion card. For a blade server, the initiator iSCSI HBA is an expansion card that installs in the blade server package itself. Refer to the blade server and expansion card documentation for details on installing the iSCSI HBA. Once the blade server options have been installed, the blade server can be installed in the BladeCenter. Refer to BladeCenter and blade server documentation for details on how to install the BladeCenter and blade server components.

Important: Do not connect any cables until instructed to do so; connecting cables at the wrong point in the installation process may cause problems later.

Update and configure BladeCenter chassis

The management module must be set to the factory default values to perform the procedure in this section. If the management module IP address is no longer known, it can be set back to the defaults, using the IP reset button on the management module. Refer to management module documentation to complete this task.

Refer to the README file printed earlier during the management module firmware download. Use the README instructions along with the steps below to perform the firmware update. The README will contain any changes necessary to the general instructions listed below. Follow the directions in the README wherever differences occur.

Also at this time, the management module must have an Ethernet cable plugged into its Ethernet port. Refer to BladeCenter or management module documentation to complete these tasks. Plug the other end of this cable into the Ethernet connector of the computer containing the downloaded management module update package. In some cases, a switch or hub may also be necessary to connect.

Note: The following steps are performed on the computer containing the update package and not on the BladeCenter console.

1. Set the IP address to something in the same subnet as the management module default IP address of 192.168.70.125 such as 192.168.70.101 and set the subnet mask to 255.255.255.0
2. Unpack the .zip file you downloaded earlier to extract the firmware update files.
3. Ensure the BladeCenter's AC power cords are plugged into an appropriate power source to provide power for the management module. Refer to BladeCenter documentation to complete this step. Allow about 30 seconds after performing this step for the management module to boot.
4. Open a Web browser. In the address or URL field, type the IP address (192.168.70.125) of the management module to which you want to connect. The Enter Password window will open.
5. Type the user name and password on the Enter Password window. The management module has a default user name of `USERID` and password of `PASSW0RD` (where 0 is a zero, not the letter O).
6. Select a timeout value on the next screen and click continue.

Update the BladeCenter management module firmware

Learn how to apply the management module firmware update using the procedure in this section.

You can being this procedure from any management module (MM) Web browser window.

1. Click **Firmware Update** on the navigation pane on the left, under **MM Control**.
2. On the Update MM Firmware window, select **Browse** and navigate to the files containing the firmware update. The files will have an extension of .PKT; and there might be multiple files with this extension.

3. Highlight one of these files and click the **Open** button. The README text may specify a particular order to select these files. If so, follow the README file instructions. The full path of the selected file is displayed in the Browse field.
4. To start the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the Management Module. A confirmation window will be displayed when the file transfer is complete.
5. Verify that the file shown on the *Confirm Firmware Update* window is the one you want to update. If not, click **Cancel**.
6. To complete the update process, click **Continue**. A progress indicator opens as the firmware on the Management Module is flashed. A confirmation window will be displayed when the update has successfully completed.
7. The README file text might direct you to restart the MM after completing the .PKT file update. If so, click **Restart** MM on the navigation pane on the left side of the window. Click **OK** to confirm the reset. The Web browser window will then close. A new Web browser window will have to be started and signed onto to continue.
8. Repeat the update procedure for any other .PKT files (steps 1 through 7).

Configure the management module

You will need to configure several settings on the management module to prepare it for iSCSI network use. Use the procedure in this section to accomplish task.

1. Select **Login Profiles** under **MM Control** in the navigation pane on the left side of the window.
2. On the next window will be a list of Login IDs, find the entry for the default login ID value of **USERID** and click on that entry.
3. A Login Profile window is displayed. Change the **Login ID** (worksheet item XSP7) and fill in the **Password** (worksheet item XSP8) and **Confirm password** fields based on the information entered in the *iSCSI Network Planning Worksheets* . Also, make sure the **Authority Level** is set to **Supervisor**. Click **Save** to complete this step
4. To configure the MM network settings, select **Network Interfaces** under **MM Control** in the navigation pane on the left side of the screen.
5. Use the values in the *iSCSI Network Planning Worksheets* to complete the following steps:
   a. Select **Enabled** from the **Interface** list.
   b. From the **DHCP** list select and set one of the following (worksheet item XSP3):
      1) **Disabled - Use static IP configuration**.
      2) **Enabled - Obtain IP config from DHCP server**. This option requires an operating DHCP server when you install the operating system.
   c. Enter a name for this MM in the **Hostname** (worksheet item XSP2) field.
   d. Enter a value for the following fields under the **Static IP Configuration** heading need to be filled in if the **Disabled – Use static IP** configuration value was selected for the **DHCP** field above:
      - **IP address** – type in the IP address (worksheet item XSP4).
      - **Subnet mask** – type in the desired subnet mask (worksheet item XSP5).
      - **Gateway address** – type in the gateway address (worksheet item XSP6).
   e. Click **Save** to complete configuring the network interfaces.

Update the blade server Baseboard Management Controller firmware

Learn how to apply the Baseboard Management Controller firmware update using the procedure in this section.

The blade server Baseboard Management Controller firmware was downloaded previously onto removable media and can be updated at this point. An alternate method of updating the blade server Baseboard Management Controller can be found in the related procedures section. The update media is

required to do the update and should be accessible from the computer that is running the management module (MM) Web browser interface. This procedure starts from any MM Web browser window.

1. Select **Firmware Update** under **Blade Tasks** on the navigation pane on the left of the window.
2. On the Update Blade Firmware window, first click the pull-down in the **Target** field and highlight the desired blade server to update. Next, click **Browse** and navigate to the media containing the firmware update.
3. There should be a file with a .PKT extension on one of the update media, highlight it and click **Open**. The full path of the selected file will be displayed in the **Browse** field.
4. To start the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the Management Module. A confirmation window will be displayed when the file transfer is complete.
5. To complete the update process, click **Continue**. A progress indicator opens as the firmware on the blade server is copied. The update can take several minutes. A confirmation window is displayed when the update has successfully completed.

Repeat steps 1-5, changing the update target each time until all the blades have been updated.

Verify blade server information

Learn how to confirm that all the blade server information matches the information you have in the planning worksheets. Use the procedure in this section to accomplish this task.

Before you begin: Be sure to have the *iSCSI network planning worksheets* available; you will need information from them as you complete this task.

You can begin this procedure from any management module (MM) Web browser window.

1. Select **Hardware VPD** under Monitors on the navigation pane on the left side of the screen.
2. Scroll down to find the BladeCenter Hardware VPD heading.
3. Find the row in the **Blade Servers** portion of the displayed table corresponding to the blade server bay or bays to be attached.
4. Verify the information in the **Machine Type/Model** (worksheet item RS5) and **Machine Serial No.** (worksheet item RS4) columns in the table with the information in the *iSCSI Network Planning Worksheets*. Correct any discrepancies on the worksheet and also in any i5/OS remote system configuration objects that may have been created. Refer toChange remote system configuration properties for information on how to make the configuration object corrections.
5. Scroll down the page to the **BladeCenter Server MAC Addresses** heading.
6. Find the row in the **Blade Servers** (worksheet item RS5) portion of the displayed table corresponding to the blade server bay(s) to be attached.
7. Look just below the **Blade Servers** row described above; it should say **Daughter Card or Exp Card** in the Name column.
8. Verify the information in this row with the *iSCSI Network Planning Worksheets*.
   - **MAC Address 1** corresponds to the iSCSI address for port 1 (worksheet item RS11)
   - **MAC Address 2** corresponds to the LAN address for port 1 (worksheet item RS15)
   - **MAC Address 3** corresponds to the iSCSI address for port 2 (worksheet item RS11)
   - **MAC Address 4** corresponds to the LAN address for port 2 (worksheet item RS15)

   Correct any discrepancies on the worksheet and also in any i5/OS remote system configuration objects that may have been created. Refer toChange remote system configuration properties for information on how to make the configuration object corrections.
9. Select **Restart MM** on the navigation pane on the left side of the screen to restart the Management Module.

10. Click **OK** to confirm that you want to restart the Management Module. A window is displayed advising that the browser window will be closed. Click **OK**.

Update and configure BladeCenter I/O module

Learn how to select and apply the appropriate I/O module settings and updates. Use the procedure in this section to accomplish this task.

1. Select **Admin/Power/Restart** under I/O Module Tasks on the navigation pane on the left side of the screen.
2. Scroll down the next page to find the **I/O Module Advanced Setup** heading. Use the **Select a module** pulldown to select the appropriate I/O module (**I/O module 3** for the first port on the iSCSI expansion card, **I/O module 4** for the second port on the card).

   Note: Make sure the pulldown for External ports has Enabled selected.
3. Click the **Save** button on the extreme lower right of the screen to save the values to the I/O module.
4. I/O module software may be updated at this time. The procedure varies depending on the manufacturer of the I/O module. Refer to the README text printed earlier along with the I/O module documentation to complete this task.

Update the blade server BIOS

You must perform these updates on all blade servers to be attached. Use the procedure in this section to accomplish this task.

Refer to the README file printed earlier during the BIOS update download. Use the README file instructions along with the following steps to perform the update. The README file will contain any changes necessary to the general instructions listed below. Follow the directions in the README file wherever differences occur.

1. Plug the BladeCenter's ac power cords into a power source. Refer to the BladeCenter documentation to complete this step.
2. Assign the KVM and Media Tray to the blade server to be updated. Refer to the blade server documentation to complete this step.
3. Insert the media containing the BIOS update in the drive and turn on the blade server. Refer to the blade server documentation to complete this step.
4. The server will boot off of the disk and present a window, choose **1 - Update POST/BIOS** from the list of options.
5. On the next window, you will be asked if you would like to move the current POST/BIOS image to the backup ROM location. If you select '**Y**, the current code will be copied in to the backup bank immediately.
6. Select **N** for the next several display prompts until the **Save current flash code to disk** prompt is displayed.
7. Select **N** for the prompt to Save current flash code to disk.
8. Select the appropriate language, if prompted, or select the **Update BIOS** option. The update begins.
9. When the update is complete, remove the media and turn off the blade server's power. Refer to the blade server documentation to complete this step.

Repeat the above steps for all blade servers to be attached.

Update the blade iSCSI HBA firmware

If an update for the iSCSI HBA firmware was built during the download process, it should be applied at this time. Perform he procedure in this section is on the BladeCenter to accomplish this task.

1. Select the KVM and Media Tray to point to the blade server to receive the update. Refer to BladeCenter documentation to complete this step.

2. Insert the media containing the iSCSI HBA update in the drive and turn on the blade server power. Refer to the blade server documentation to complete this step.
3. Wait for the server to complete POST. It should then access the drive with the update media loaded and proceed to boot off the media. It will take several minutes to complete this.
4. The blade server should boot to the update utility, which will present a screen informing about the contents of the update. Type y to continue with the update.
5. When the update completes, turn off the server's power. Refer to blade server documentation to complete this step.

Repeat steps 1-5 for any other blade servers to be updated.

Set the blade start options

Configure the start options before continuing with the installation. Use the procedure in this section to disable the Pre-Boot Execution Environment (PXE) option for all integrated Ethernet ports, turn off the boot fail counter, and turn off virus detection.

1. Turn on the blade server. Refer to the server documentation to complete this step.
2. Press F1 when prompted, after the IBM eServer logo appears on the display.
3. Highlight **Start Options** using the up or down arrow keys and press Enter.
4. Highlight **Planar Ethernet PXE/DHCP** using the up or down arrow keys. Use the right or left arrow keys to change the value to **Disabled**.
5. Highlight **Boot Fail Count** using the up or down arrow keys and use the right or left arrow keys to change the value to **Disabled**.
6. Highlight **Virus Detection** using the up and down arrow keys and use the right or left arrow keys to change the value to **Disabled**.
7. Press the Esc key to return to the main setup menu.

Complete the blade server configuration

Save all the configuration settings and exit the setup utility to complete the server configuration. Use the procedure in this section to accomplish this task.

1. From the main setup menu, highlight **Save Settings** using the up or down arrow keys and press Enter.
2. From the *Save Settings* window, press Enter to save.
3. From the main setup menu, press Esc to exit setup.
4. From the *Exit Setup* window, use the up or down arrow keys to highlight **Yes, exit the Setup Utility** and press Enter.
5. The server power can now be turned off. Refer to blade server documentation to complete this step.

Configure iSCSI HBA

There are several configuration tasks you must complete on the iSCSI HBA after you have installed it into your server. Use the instructions in these sections to complete these tasks.

Initial configuration of an iSCSI HBA

Complete these tasks if you are installing an iSCSI HBA into your xSeries or blade server for the first time.

These instructions describe the configuration of the iSCSI HBA as a boot device.

Start the iSCSI HBA configuration utility

You can use the iSCSI configuration utility to complete initial installation settings, make changes to the adapter settings, or to assist in diagnosing problems. Use the procedure in this section to access the configuration utility.

If you came to this procedure from the related procedures section skip the following paragraph, complete the procedure and then return to the procedure that you came from.

Some configuration needs to be done to the xSeries or blade server iSCSI HBA before continuing. The steps are performed from the xSeries or BladeCenter display and keyboard using the iSCSI HBA configuration utility.

Note: Blade server only: Select the appropriate blade server for the BladeCenter KVM and media tray. Refer to BladeCenter or blade server documentation to complete this step.

1. Turn the xSeries or blade server's power on. Refer to xSeries or blade server documentation to complete this step. This will start the power on system test (POST) on the xSeries or blade server.
2. Wait for the QLogic BIOS prompt on the xSeries or blade server's display. This will appear sometime after the eServer logo has been displayed.

   Important: If you have more than one adapter version installed the prompt will appear for each version. The screen will display `QLA405x` then `QLA406x`, you must respond to the prompt for the adapter version you want to configure.
   The prompt will read something like this:**Press CTRL-Q for Fast!UTIL**. Respond to this prompt by pressing Ctrl + Q. This will start the configuration utility.
3. Successful initiation of the utility is confirmed by a message that reads **CTRL-Q Detected, Initialization in progress, Please wait...**

   Note: It may take several minutes before the next screen is displayed.

   Tip: A red status bar may appear at the bottom of the screen at various times informing about status or errors.
4. If more than one iSCSI HBA port is available for use, either because the iSCSI HBA has multiple ports (as in a blade server) or there are multiple iSCSI HBAs plugged into the server (as can be done with xSeries), the **Select Host Adapter** menu will appear. Highlight the iSCSI HBA port you will be configuring as identified by its MAC address using the up or down arrow keys and press Enter. It might take several seconds for the next window to appear.
5. The next window will have two panes:
   - The Selected Adapter pane is at the top. This pane shows the iSCSI HBA port currently selected for configuration.

- On the lower pane is the **Fast!UTIL Options** pane.

Configure the boot iSCSI HBA

Some of the iSCSI HBA settings depend on what addressing mode is being used. These are described in the following sections.

Select one of the two procedures listed below, based on the boot parameter delivery method selected in worksheet item RS6

- When configuring a new iSCSI HBA (one that has not been previously configured) for dynamic parameter delivery via DHCP, complete the steps in "Configure a new iSCSI HBA for dynamic addressing."
- When the iSCSI HBA may have been previously used follow the directions for "Resetting the cached iSCSI initiator configuration information" on page 31 followed by "Restore the factory defaults" on page 31 before continuing with "Configure a new iSCSI HBA for dynamic addressing."
- To configure your iSCSI for manual addressing see, "Configure iSCSI HBA for manual addressing" on page 19.

Note: These procedures start from the **Configuration Settings** menu if you need to restore this menu see, "Start the iSCSI HBA configuration utility" on page 17 then return to this procedure.

Configure a new iSCSI HBA for dynamic addressing

Learn how to use the configuration utility to prepare the iSCSI HBA for dynamic addressing. Use the procedure in this section to accomplish this task.

Note: These procedures start from the **Configuration Settings** menu if you need to restore this menu see, "Start the iSCSI HBA configuration utility" on page 17 then return to this procedure.

1. Highlight **Host Adapter settings** using the up or down arrow keys and press Enter
2. Highlight **Initiator IP address by DHCP** using the up or down arrow keys and press Enter until the value shows **NO**.
3. Press Esc to return to the **Configuration Settings** menu.
4. Highlight **ISCSI Boot Settings** using the up or down arrow keys and press Enter.
5. The **iSCSI Boot Settings** menu will be displayed.
6. Highlight **Adapter Boot Mode** using the up or down arrow keys and press Enter.
7. Highlight **DHCP** using the up or down arrow keys and press Enter.
   - For adapter version 406x highlight **DHCP using vendor IP** using the up or down arrow keys and press Enter
8. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press Enter.
9. Highlight **Security Settings** using the up or down arrow keys and press Enter to select. The next menu displayed will be the **Primary Boot Security Settings** menu.
10. Highlight **Chap** using the up or down arrow keys and press Enter to change the value to **Enabled** or **Disabled**, depending on whether or not CHAP will be used. Refer to the *iSCSI Network Planning Worksheets* item CQ12 for this information. Skip to step 13 if CHAP has been disabled.
11. Highlight **Chap Name** using the up or down arrow keys and press Enter. This will bring up the **Enter Chap Name** pane. Type in the CHAP name from the *iSCSI Network Planning Worksheets* item CQ13 and press Enter.
12. Highlight **Chap Secret** using the up or down arrow keys and press Enter. This will bring up the **Enter New Secret** pane. Type in the CHAP secret from the *iSCSI Network Planning Worksheets* item CQ14 and press Enter. The **Confirm New Secret** pane is then displayed. Retype the same secret and press Enter.
13. Press Esc to return to the **Primary Boot Device Settings** menu.
14. Press Esc to return to the i**SCSI Boot Settings** menu.

15. Press Esc to return to the **Configuration Settings** menu.

Configure iSCSI HBA for manual addressing

Learn how to use the configuration utility to prepare the iSCSI HBA to use manual addressing. Use the procedure in this section to accomplish this task.

Note: These procedures start from the **Configuration Settings** menu if you need to restore this menu see, "Start the iSCSI HBA configuration utility" on page 17 then return to this procedure.

To configure the selected iSCSI HBA port for manual addressing, perform the following steps. The xSeries or blade system iSCSI HBA settings are configured first starting from the **Configuration Settings** menu.

1. Highlight **Host Adapter settings** using the up or down arrow keys and press Enter.
2. Highlight **LUNs per Target** using the up or down arrow keys and press Enter. Use the arrow keys to select the value **64** and press Enter. This option is not available in adapter version 406x.
3. Highlight **Initiator IP Address via DHCP** using the up or down arrow keys and press Enter until the value shows **NO**.

   Important: In adapter version 406x select only the **IPv4** options for the following steps.
4. Highlight **Initiator IP address** using the up or down arrow keys and press Enter. Type the Integrated Server HBA iSCSI Initiator IP address from the *iSCSI Network Planning Worksheets* item CQ3 and press Enter.
5. Highlight **Subnet mask** using the up or down arrow keys and press Enter to select. Type the iSCSI Initiator subnet mask from the *iSCSI Network Planning Worksheets* item CQ4 and press Enter.
6. Highlight **Gateway IP Address** using the up or down arrow keys and press Enter to select. Type the iSCSI Initiator gateway IP address from the *iSCSI Network Planning Worksheets* item CQ5 and press Enter.
7. Highlight **Initiator iSCSI Name** using the up or down arrow keys and press Enter to select. Type the name (`iqn.1924-02.com.ibm:...`) from the *iSCSI Network Planning Worksheets* item CQ6 and press Enter.
8. Clear the **Initiator Chap Name** and **Initiator Chap Secret** fields. Highlight each field and using the up or down arrow keys, press Enter, type in a single space and press Enter to clear each field.

   Note: Initiator Challenge Handshake Authentication Protocol (CHAP) is not supported, so these fields must be blank.
9. Press Esc to return to the **Configuration Settings** menu.
10. Highlight **iSCSI Boot Settings** using the up or down arrow keys and press Enter to display the iSCSI Boot Settings menu.
11. Highlight **Adapter Boot Mode** using the up or down arrow keys and press Enter.
12. Highlight **Manual** using the up or down arrow keys and press Enter.
13. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press Enter.
14. Highlight **Target IP** using the up or down arrow keys and press Enter to select. Type the iSeries® iSCSI HBA iSCSI IP address from the *iSCSI Network Planning Worksheets* item CQ10 and press Enter.
15. Highlight **iSCSI Name** using the up or down arrow keys and press Enter. i5/OS will generate the IQN for the target side and it must be matched here. Type the iSCSI name from the *iSCSI Network Planning Worksheets* item CQ11 and press Enter.
16. Highlight **Security Settings** using the up or down arrow keys and press Enter to display the **Primary Boot Security Settings** menu.
17. Highlight **Chap** using the up or down arrow keys and press Enter to change the value to **Enabled** or **Disabled**, based on whether or not CHAP will be used. Refer to the *iSCSI Network Planning Worksheets* item CQ12 for this information. Skip to step 21 if CHAP has been disabled.

18. Highlight **Chap Name** using the up or down arrow keys and press Enter to select. This will bring up the Enter Chap Name pane. Type in the CHAP name from the *iSCSI Network Planning Worksheets* item CQ13 and press Enter.
19. Highlight **Chap Secret** using the up or down arrow keys and press Enter to select. This will bring up the **Enter New Secret** pane. Type in the chap secret from the *iSCSI Network Planning Worksheets* item CQ14 and press Enter and confirm by retyping the same chap secret on the next pane and press Enter.
20. Highlight **Bidirectional Chap** using the up or down arrow keys and press Enter to change the value to **Disabled**, since this feature is not supported.
21. Press Esc to return to the Primary Boot Device Settings menu.
22. Press Esc to return to the iSCSI Boot Settings menu.
23. Press Esc to return to the Configuration Settings menu.

Configure iSCSI HBA port settings

After configuring for either manual or dynamic addressing, use the procedure in this section to complete the selected iSCSI HBAs port configuration.

1. Highlight **Advanced Adapter Settings** using the up or down arrow keys and press Enter.
2. Highlight **Delayed ACK** using the up or down arrow keys and press Enter until the value shows **Disabled**.
3. Highlight **MTU** (maximum transmission unit) using the up or down arrow keys and press Enter until the value shows the desired frame size setting from the *iSCSI Network Planning Worksheets* item CQ16 (either 1500 or 9000). Ensure the network the iSCSI HBA will be attached to supports the value selected here.
4. Press Esc to return Configuration Settings menu.
5. Press Esc. Highlight **Save changes** using the up or down arrow keys and press Enter to select.

   Note: This may take several minutes to complete and will remain with the same pane on the screen until completion. At completion of the save, the **Fast!UTIL Options** menu will be displayed.

Disable boot for additional iSCSI HBA ports

iSCSI HBA ports other than the boot device need to be configured with boot mode disabled. Use the procedure in this section to accomplish this task.

1. Press Esc Highlight **Return to Fast!UTIL** and press Enter.
2. From the Select Host Adapter menu, find any unused adapter ports and check to see if the **Adapter Boot Mode** is already set to **Disable**. If so, there is no need to continue. Otherwise, highlight the unused adapter port using the up or down arrow keys and press Enter to select. It may take several seconds for the next screen to appear.
3. On the *Fast!UTIL* Options menu, highlight **Configuration settings** using the up or down arrow keys and press Enter to select.
4. On the Configuration Settings menu , highlight **iSCSI Boot Settings** using the up and down arrow keys and press Enter to select.
5. Highlight **Adapter Boot Mode** using the up or down arrow keys and press Enter to select.
6. Highlight **Disable** using the up or down arrow keys and press Enter to select.
7. Press Esc to return to the Configuration Settings menu.
8. Highlight **Advanced Adapter Settings** using the up or down arrow keys and press Enter.
9. Highlight **MTU** (maximum transmission unit) using the up or down arrow keys and press Enter until the value shows the desired frame size setting from the *iSCSI Network Planning Worksheets* item CQ16 (either 1500 or 9000). Ensure the network the iSCSI HBA will be attached to supports the value selected here.
10. Press Esc to return Configuration Settings menu.

11. Press Esc. Highlight **Save changes** using the up or down arrow keys and press Enter to select.

    Note: This may take several minutes to complete and will end up at the **Fast!UTIL Options** menu.

End the configuration utility

When all iSCSI HBA configuration is complete, the configuration utility can be ended by using the procedure in this section.

1. Press Esc on the **Fast!UTIL Options** menu.
2. Highlight **Reboot system** using the up or down arrow keys and press Enter.

The xSeries or blade server will now start to reboot. The xSeries or blade server power should now be turned off. Refer to the xSeries or blade server documentation to complete this step

Cable the network

Use the information in this section to understand the basic concepts of cabling the network after you have installed and configured the iSCSI HBA.

Once the xSeries or blade system has been configured, the network needs to be cabled to complete the configuration. The first step is to locate the ports that need to be cabled into the network.

Before you cable the network locate each point or port that you will connect from the following:

- The i5/OS partition network interface; either a new adapter or an existing adapter being used for a TCP/IP connection.
- The xSeries or blade server service processor. Depending on which server you are attaching the location of the service processor will vary. You will need to refer to your xSeries or blade server documentation to complete this connection.
  - For xSeries the RSA II or the BMC might be used as the service processor.
  - For blade servers located in a BladeCenter the management module is used as a service processor.
- The iSCSI HBA connection is as follows:
  - In the i5/OS partition and the xSeries the port to connect to is located on the tailstock of the iSCSI adapter.
  - In the blade server the port to connect is located on the module plugged into I/O bay number 3. This might be an internally wired port on an integrated switch or a fan-out cable from a pass-through module. Refer to the I/O module documentation to complete this connection.

There are many different ways to cable the network – the iSCSI configuration could even be added to an existing Ethernet network. All the possibilities won't be covered here. There are a couple of important considerations that must be observed when cabling the iSCSI configuration:

- Ensure all iSCSI HBAs in both the System i5® model and any xSeries or blade systems are in the same network.
- Ensure the System i5 model network interface card and the service processor connection reside in the same network.

For help understanding different external switch considerations see Ethernet switches for iSCSI.

Related procedures

This section contains procedures that are used as alternatives, additions, or references to the basic installation instructions and should only be used if directed here as a part of your installation or as directed by troubleshooting.

Related System x or xSeries procedures

Locate instructions to download firmware, alternate update methods, and other procedures you might be directed to do as a part of the installation or trouble shooting tasks.

Download System x or xSeries firmware

Learn how to download the latest firmware for your System x or xSeries server.

Download System x or xSeries BIOS firmware

Learn how to locate, select, and download the required firmware updates using the procedure in this section.

The following procedure is performed on a computer using a common web browser, while accessing the following web page http://www.ibm.com/systems/i/systemx/iscsi/servermodels/. Start by locating the System x or xSeries server type and model in the System x or xSeries models supported with iSCSI table. Click on the **download firmware** link. The *Software and device drivers* page for the selected server is displayed.

The BIOS firmware updates may be available in a number of formats, employing different bootable media:

- .exe file(s): create a bootable update diskette.
- .img file(s): create a bootable update diskette.
- .iso file: create a bootable update CD.

Download the system BIOS update by following these steps:

1. Find the **BIOS** heading and column for the appropriate hardware, if necessary and select the link for **Flash BIOS Update (DOS Version)** or **Flash BIOS Update (Diskette image)**. Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.
2. Click on the link for the README text file and print a copy for use as a reference when actually performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Click on the link to download one of the update versions on the page for the BIOS update.
5. Create the update media by performing the appropriate action for the file type from the following methods:
   - .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
   - .img file(s): Use an image-to-disk utility such as EMT4W32 to create a bootable update diskette from the file.
   - .iso file: Use a CD burning utility to create a bootable update CD.
6. Click on the browser's Back button to return to the *Software and drivers* page.

Download the Baseboard Management Controller firmware update

The Baseboard Management Controller should be updated in all xSeries servers even those with remote supervisor adapter II (RSAII) installed. Use the procedure in this section to accomplish this task.

The following procedure is performed on a computer using a common web browser, while accessing the following web page http://www.ibm.com/systems/i/systemx/iscsi/servermodels/. Start by locating the xSeries server type and model in the xSeries models supported with iSCSI table. Click on the **download firmware** link. The *Software and device drivers* page for the selected server will then be displayed.

The Baseboard Management Controller firmware updates may be available in a number of formats, employing different bootable media:

- .exe file(s): create a bootable update diskette.
- .img file(s): create a bootable update diskette.
- .iso file: create a bootable update CD.

Download the system Baseboard Management Controller update by following these steps:

1. Find the **BMC** heading. If there is no **BMC** heading, look for the **Advanced Systems Management** heading. Select the link for **Baseboard Management Controller Update** from the appropriate hardware column.

   Note: Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.
2. Click on the link for the README text file on the next page, and print a copy for use as a reference when actually performing the update.
3. Click Back, on the browser, to return to the previous page.
4. Click on the link to download one of the update versions on the page for the Baseboard Management Controller update. There may be multiple links for a single update version.
5. Create the update media by performing the appropriate action for the file type from the following methods:
   - .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
   - .img file(s): Use an image-to-disk utility such as EMT4W32 to create a bootable update diskette from the file.
   - .iso file: Use a CD burning utility to create a bootable update CD.
6. Click Back, on the browser, to return to the *Software and drivers* page.

Download Remote Supervisor Adapter II (RSA II) firmware

If you have the RSA II, use the procedure in this section to locate, select, and download the required firmware update. You will not need to update the RSA II firmware if it is not installed on your xSeries server.

The RSA II firmware update will reside in a .zip file.

The following procedure is performed on a computer using a common web browser, while accessing the following web page http://www.ibm.com/systems/i/systemx/iscsi/servermodels/. Start by locating the xSeries server type and model in the xSeries models supported with iSCSI table. Click on the **download firmware** link. The *Software and device drivers* page for the selected server will then be displayed.

Download the RSA II firmware update by following these steps:

1. Find the **Remote Supervisor Adapter II** heading. Select the link that is not associated with an operating system. You will complete the update before an operating system is installed on your server.

Note: If a DOS update is listed select that link.

2. On the **firmware update** page, click on the link for the readme text file and print a copy for use as a reference when actually performing the update.
3. Click Back on your browser to return to the **firmware update** page.
4. Click on the link for the .zip file containing the firmware updates to download the file. You will use this file to update the RSA II firmware.

Download iSCSI HBA update for System x or xSeries

Learn when and how to update the iSCSI HBA firmware during the installation process.

You must download the update to ensure you have the exact level of BIOS and firmware specified in theSystem i documentation. Do this regardless of what BIOS version is currently present on the iSCSI HBA.

Once the iSCSI HBA is installed and the operating system is installed and running on the System x or xSeries server, updates are applied through i5/OS integration service pack PTFs.

Restriction: The following procedure is only for use during the installation of the iSCSI HBA. Unpredictable results might occur if you attempt this procedure on an installed and running iSCSI HBA.

1. Using a computer and Web browser access http://www.ibm.com/systems/i/systemx/iscsi/servermodels/.
2. Click the **Download iSCSI HBA firmware** link.
3. Click the README text file link on the next page, and print a copy for use as a reference when actually performing the update.
4. Click **Back** on the browser to return to the previous page.
5. Click on the link to download the iSCSI HBA update. This will be in the form of a .iso file.
6. Create a compact disc (CD) containing the update using a CD burning utility.

Alternate method to update Remote Supervisor Adapter II network configuration to defaults

This method should be used to set RSA II network settings when the defaults are no longer set. This method will not work if the RSA II does not have firmware compatible with the xSeries server it is installed in. This procedure is performed on the xSeries console.

1. Turn on the xSeries server. Refer to the server documentation to complete this step.
2. When the IBM eServer logo appears on the display, press F1 to go to setup.
3. Highlight **Advanced Setup** using the up or down arrow keys and press **Enter** to select.
4. Highlight **RSA II Settings** (will only be present with RSA II hardware installed) using the up or down arrow keys and press **Enter** to select.
5. Highlight **DHCP Control** using the up or down arrow keys and use the left or right arrow keys to change the value to **Use Static IP**.
6. Highlight **Static IP Address** using the up or down arrow keys and use the backspace key to position the cursor and enter the IP address 192.168.070.125
7. Highlight **Subnet Mask** using the up or down arrow keys and use the backspace key to position the cursor and enter 255.255.255.000.
8. Highlight **Gateway** using the up or down arrow keys and use the backspace key to position the cursor and enter 192.168.070.001
9. Highlight **OS USB Selection** using the up or down arrow keys and use the right or left arrow keys to change the value to **Other OS**.
10. Highlight **Save Values and Reboot RSA II** using the up or down arrow keys and press **Enter** to select and perform the action. A screen will display confirming the action.

11. Press **Esc** two times to return to the main setup menu.

If you downloaded an available update to the iSCSI HBA installed in your xSeries go to "Update the System x or xSeries iSCSI HBA firmware" on page 8.

Related BladeCenter and blade server procedures

Locate instructions to download firmware, alternate update methods, and other procedures to assist with installation or troubleshooting.

Download BladeCenter or blade server firmware

Learn how to locate, select, and download the needed firmware updates for your server. Use the instructions in this section to accomplish these tasks.

The following procedure is performed on a computer using a common web browser, while accessing the webpage: http://www.ibm.com/systems/i/systemx/iscsi/servermodels/. Start by locating the blade server type or model in the BladeCenter blade models supported with iSCSI table. Click on the **download firmware** link. The Software and device drivers page for the selected blade server will then be displayed.

The BIOS and Baseboard Management Controller firmware updates may be available in a number of formats, employing different bootable media.

- .exe file(s): create a bootable update diskette.
- .img file(s): create a bootable update diskette.
- .iso file: create a bootable update CD.

Other firmware will have a single file type.

Download the blade server BIOS

Learn how to locate, select, and download the BIOS updates for your blade server using the procedure in this section.

1. On the next page, find the **BIOS** heading and column for the appropriate hardware, if necessary and select the link for **Flash BIOS Update (DOS Version)** or **Flash BIOS Update (Diskette image)**. Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.
2. On the next page, click on the link for the README text file and print a copy for use as a reference when actually performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Again, on the page for the BIOS update, click on the link to download one of the update versions.
5. Perform the appropriate action to create the update media
   a. .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
   b. .img file(s): Use an image-to-disk utility such as EMT4W32 to create the update diskette from the file.
   c. .iso file: Use a CD burning utility to create the update CD.
6. Click on the browser's Back button to return to the Software and drivers page.

Download the BladeCenter Baseboard Management Controller firmware update

The BMC should be updated even though the BladeCenter has a Management Module.

1. From the blade server *Sofware and device drivers* page, find the BMC heading. If there is no BMC heading, look for the Advanced Systems Management heading. Select the link for Baseboard

Management Controller Update from the appropriate hardware column, if multiple columns are present. Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.

2. On the next page, click on the link for the README text file and print a copy for use as a reference when actually performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Again, on the page for the BMC update, click on the link to download one of the update versions. There may be multiple links for a single update version.
5. Click your browser's back button until you are at the software and device drivers page.
6. Create the update media by performing the appropriate action for the file type from the following methods:
   - .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
   - .img file(s): Use an image-to-disk utility such as EMT4W32 to create a bootable update diskette from the file.
   - .iso file: Use a CD burning utility to create a bootable update CD.
7. Click on the browser's Back button to return to the Software and drivers page.

Download BladeCenter management module firmware

Learn how to locate, select, and download the management module firmware update using the procedure in this section.

This procedure is started by accessing the *BladeCenter and System x models supported with iSCSI* Web page. Locate the BladeCenter chassis model in the table under the **BladeCenter chassis models supported by iSCSI** heading. Click on the **Download firmware** link. The software and device drivers page for the selected BladeCenter will is displayed.

1. Find the **Management Module** heading and select the link for the update, making sure you don't select a link for an update version based on an operating system, since the update will be done prior to installing the operating system.
2. On the firmware update page, click on the link for the README text file and print a copy for use as a reference when actually performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Click on the link for the .zip file containing the firmware updates to download the file. This file will be used to later update the firmware.

Download the BladeCenter I/O module firmware update

Learn how to locate, select, and download BladeCenter I/O module firmware updates using the procedure in this section.

1. From the BladeCenter software and device drivers page find the **Networking** heading and select the appropriate link for the I/O module installed in the BladeCenter chassis.
2. On the firmware update page, click on the link for the README text file and print a copy for use as a reference when performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Next, click on the link of the firmware update to download the file. This file will be used later to update the firmware.

Download the iSCSI HBA update for blade servers

Learn when and how to update the iSCSI HBA basic input/output system (BIOS) and firmware.

If your iSCSI HBA BIOS level is version 1.08 or higher, and the iSCSI firmware is version 2.0.0.29 or higher you do not need to download the update. If the BIOS or firmware versions are lower than the

above numbers, or if the version is unknown, you should download the update to ensure you have the minimum BIOS and firmware versions for a successful installation.

Once the iSCSI HBA is installed and the operating system is installed and running on the blade server, updates are applied through i5/OS integration service pack PTFs.

Restriction: The following procedure is only for use during the installation of the iSCSI HBA. Unpredictable results might occur if you attempt this procedure on an installed and running iSCSI HBA.

1. Using a computer and Web browser access http://www.ibm.com/systems/i/systemx/iscsi/servermodels/.
2. Click the **Download iSCSI HBA firmware** link.
3. Click the README text file link on the next page, and print a copy for use as a reference when actually performing the update.
4. Click **Back** on the browser to return to the previous page.
5. Click on the link to download the iSCSI HBA update. This will be in the form of a .iso file.
6. Create a compact disc (CD) containing the update using a CD burning utility.

Alternate method to update the blade server Baseboard Management Controller

You might need an alternative method to update the Baseboard Management Controller on a blade server. Use the procedure in this section to accomplish this task.

Refer to the README file printed earlier during the Baseboard Management Controller firmware download"Download the Baseboard Management Controller firmware update" on page 26. Use the README file instructions, along with the following steps to perform the update. The README file contains any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur. You can use the following procedure to update Baseboard Management Controller firmware for blade servers.

1. On a blade server assign the KVM and Media Tray to the blade server to be updated. Refer to the blade server documentation to complete this step.
2. Turn on the blade server's power and insert the media containing the Baseboard Management Controller firmware update in the appropriate drive. Refer to the blade server documentation to complete this step.
3. The update will load and start automatically. It will take several minutes to complete.
4. When the update completes, remove the media from the drive and turn off the blade server's power. Refer to the blade server documentation to complete this step.

Repeat the above steps for all blade servers to be attached.

Related iSCSI HBA configuration procedures

Locate procedures, for use as directed during the install or as part of a troubleshooting process. These procedures are designed to be performed independently of each other (with the exception of the Start the configuration utility and End the configuration utility sections).

The procedures in this section are performed on the xSeries or BladeCenter console. The BladeCenter KVM must be assigned to the appropriate blade server before starting.

Start the iSCSI HBA configuration utility

You can use the configuration utility to make changes to the iSCSI HBA settings. Use the procedure in this section to access the configuration utility.

Preform the following steps from the xSeries or BladeCenter display and keyboard using the iSCSI HBA configuration utility.

Note: Blade server only: Select the appropriate blade server for the BladeCenter KVM and media tray. Refer to BladeCenter or blade server documentation to complete this step.

1. Turn the xSeries or blade server's power on. Refer to xSeries or blade server documentation to complete this step. This will start the power on system test (POST) on the xSeries or blade server.
2. Wait for the QLogic BIOS prompt on the xSeries or blade server's display. This will appear sometime after the eServer logo has been displayed. The prompt will read something like this:**Press CTRL-Q for Fast!UTIL**. Respond to this prompt by pressing Ctrl + Q. This will start the configuration utility.
3. Successful initiation of the utility is confirmed by a message that reads **CTRL-Q Detected, Initialization in progress, Please wait...**

   Note: It may take several minutes before the next screen is displayed.

   Note: A red status bar may appear at the bottom of the screen at various times informing about status or errors.
4. If more than one iSCSI HBA port is available for use, either because the iSCSI HBA has multiple ports (as in a blade server) or there are multiple iSCSI HBAs plugged into the server (as can be done with xSeries), the **Select Host Adapter** menu will appear. Highlight the iSCSI HBA port you will be configuring as identified by its MAC address using the up or down arrow keys and press Enter. It might take several seconds for the next window to appear.
5. The next window will have two panes:
   - The Selected Adapter pane is at the top. This pane shows the iSCSI HBA port currently selected for configuration.
   - On the lower pane is the **Fast!UTIL Options** pane.

Restore the factory defaults

If the iSCSI HBA was previously used in another environment, it may be desirable to restore the factory defaults before proceeding with any configuration. This can be done starting at the *Fast!UTIL Options* menu.

To start the utility see "Start the iSCSI HBA configuration utility" on page 30 and then return to these instructions.

1. Highlight **Configuration Settings** using the up or down arrow keys and press Enter.
2. Highlight **Restore Adapter Defaults** using the up or down arrow keys and press Enter.
3. Press Esc. The Configuration settings modified pane is displayed.
4. On the **Restore Adapter Defaults** menu, highlight **Restore Adapter Defaults** using the up or down arrow keys and press Enter to restore the default settings.
5. Highlight **Save changes** using the up or down arrow keys and press Enter. This may take several minutes to complete after which the *Fast!UTIL Options* menu is displayed.

Resetting the cached iSCSI initiator configuration information

You might want to clear any cached information from other iSCSI HBAs your adapter communicated with in the past. Use the procedure in this section to accomplish this task.

Important: performing this procedure will likely erase iSCSI boot information, making it necessary to reconfigure the boot iSCSI HBA settings.

1. Start the configuration utility if it is not already running. For instructions see, "Start the iSCSI HBA configuration utility" on page 30.

   Note: The procedure below starts at the *Fast!UTIL Options* menu.

2. Highlight **Configuration Settings** using the up or down arrow keys and press Enter.
3. Highlight **Clear persistent targets** using the up or down arrow keys and press Enter.
4. On the next screen, highlight **Clear persistent targets** using the up or down arrow keys and press Enter. The text in the Clear Persistent Targets pane will change to Clearing Persistent Targets while the clear is in progress. It might take several minutes to complete.
5. Once the clear is complete, the text in the Clear Persistent Targets pane will change to Persistent Targets Cleared; hit any key to return to the *Configuration Settings* menu.
6. Press Esc to return to the *Fast!UTIL Options* menu.

Using the ping utility

Learn how to use the ping utility to debug connection problems during the installation process.

Before you can use the ping utility the iSCSI HBA must have an IP address. If you have already configured and know the IP address of the adapter continue with the rest of the procedure. To set the IP address choose one of the two following options:

- If you have configured the iSCSI HBA to use DHCP, the network server description must be started. This enables the integrated DHCP server to provide the IP address. For instructions see "Configure a new iSCSI HBA for dynamic addressing" on page 18.
- If you are configuring the iSCSI HBA with manual addressing see "Configure iSCSI HBA for manual addressing" on page 19 to set the IP address.

Use the following steps to access the ping utility to verify the physical connection of the xSeries or blade server to the i5/OS partition.

1. "Start the iSCSI HBA configuration utility" on page 30.
2. Highlight **Ping Utility** and press Enter.
3. Highlight the values for **Target IP** and press Enter to select. A red **Enter IP Address** pane is displayed.
4. Type the IP address of the iSCSI HBA in the i5/OS partition into the **Enter IP Address** pane and press Enter. The Enter IP Address pane will disappear and the address just entered will be displayed in the **Target IP** field on the Ping Utility pane.
5. Highlight **Ping Target** and press Enter to perform the ping. A small pane will open with the results of the ping:
   - Ping successful: verifies the path from the xSeries or blade server iSCSI HBA to the i5/OS iSCSI HBA
   - Ping unsuccessful: means the path from the xSeries or blade server iSCSI HBA cannot be verified. This may occur when the Ping Target is an iSCSI HBA LAN IP address in a different subnet, but on the same switched network as the xSeries or blade server iSCSI HBA used to send the Ping.
6. Press Enter to close the ping utility pane.
7. Press Esc to return to the options menu.

Change CHAP secret

Learn how to set the CHAP secret within the iSCSI HBA configuration settings. Use the procedure in this section to accomplish this task.

Note: If you have previously set the challenge handshake authentication protocol (CHAP) secret and are going to change it you must know the original CHAP secret. If you do not know the original CHAP secret, you will need to restore the factory defaults and reconfigure the iSCSI HBA. Refer to "Restore the factory defaults" on page 31, then refer to "Configure the boot iSCSI HBA" on page 18 in this case.

The generation of a CHAP secret can be deferred to when the i5/OS remote system configuration object is created. This can be done when using either dynamic or manual addressing. This section provides a

procedure for updating the CHAP secret once the initial configuration has already been done. These settings are configured starting from the *Fast!UTIL Options* menu. For information about accessing this menu see, the "Start the iSCSI HBA configuration utility" on page 30 section and then return to this procedure.

1. Highlight **Configuration Settings** using the up or down arrow keys and press Enter.
2. Highlight **iSCSI Boot Settings** using the up or down arrow keys and press Enter to display the *iSCSI Boot Settings* menu.
3. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press Enter.
4. Highlight **Security Settings** using the up or down arrow keys and press Enter to select. The next menu displayed will be the *Primary Boot Security Settings* menu
5. Highlight **Chap** using the up or down arrow keys and press Enter to change the value to **Enabled**, if necessary.
6. Highlight **Chap Name** using the up or down arrow keys and press Enter to select. This will bring up the **Enter Chap Name** pane. Type in the CHAP name if this hasn't been previously done, using the *iSCSI Network Planning Worksheets* (item CQ13) and press Enter.
7. Highlight **Chap Secret** using the up or down arrow keys and press Enter. If CHAP was previously configured, the *Enter Old Secret* pane will be displayed. Type in the original CHAP secret and press Enter. At this point, in either case the *Enter New Secret* pane is displayed. Type in the chap secret from the *iSCSI Network Planning Worksheets* (item CQ14) and press Enter. The *Confirm New Secret* pane is then displayed. Retype the same secret and press Enter.

   Remember: the chap secret is case sensitive.
8. Highlight **Bidirectional Chap** using the up or down arrow keys and press Enter to change the value to **Disabled**, since this feature is not supported.
9. Press Esc to return to the *Primary Boot Device Settings* menu.
10. Press Esc to return to the *Configuration Settings* menu.
11. Press Esc. The *Configuration settings modified* pane is displayed.
12. Highlight **Save changes** using the up or down arrow keys and press Enter. It might take several minutes to complete the save process. When complete, the *Fast!UTIL Options* menu is displayed.

Change the maximum transmission unit (MTU)

The MTU might need to be changed after the original configuration of the iSCSI HBA. Use the procedure in this section, which starts from the Fast!UTIL Options menu of the configuration utility, to accomplish this task.

See "Start the iSCSI HBA configuration utility" on page 30 for information on accessing the configuration menu.

1. Highlight **Configuration Settings** using the up or down arrow keys and press Enter.
2. Highlight **Advanced Adapter Settings** using the up or down arrow keys and press Enter.
3. Highlight **MTU** using the up or down arrow keys and press Enter until the value shows the desired frame size setting (refer to the *iSCSI Network Planning Worksheets* item CQ16).
4. Press Esc to return *Configuration Settings* menu.
5. Press Esc. The *Configuration settings modified* pane is displayed.
6. Highlight Save changes using the up or down arrow keys and press Enter. It might take several minutes it will take to complete the save process. When complete, the *Fast!UTIL Options* menu is displayed.

End the configuration utility

When all iSCSI HBA configuration is complete, the configuration utility can be ended by using the procedure in this section.

1. Press Esc on the **Fast!UTIL Options** menu.
2. Highlight **Reboot system** using the up or down arrow keys and press Enter.

The xSeries or blade server will now start to reboot. The xSeries or blade server power should now be turned off. Refer to the xSeries or blade server documentation to complete this step

Remove and replace the System x, xSeries, or blade server iSCSI HBA

Learn the hardware and software configuration tasks to remove and replace an iSCSI HBA. Use the instructions in this section to accomplish these tasks.

Stop the iSCSI integrated System x, xSeries, or blade server

Locate instructions to stop your integrated server.

To stop the iSCSI HBA integrated server, refer to the Start and stop an integrated server topic in the web site http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzahq/rzahqntspo.htm. Successfully stopping an iSCSI HBA integrated server will turn off the power to the integrated server.

Remove the System x, xSeries, or blade server iSCSI HBA

Locate instructions to remove the adapter.

Once the iSCSI HBA integrated server has been stopped, removing the iSCSI HBA from a System x, xSeries, or blade server is not any different from removing any other adapter from either server. See the documentation for your System x, xSeries, or blade server and return to these instructions to complete configuration.

Note: Any Ethernet cables plugged into the System x or xSeries iSCSI HBA should be labeled and disconnected prior to removing the iSCSI HBA. You will not have to disconnect any Ethernet cables from the blade server as these connections are made through the BladeCenter midplane.

Replace the System x, xSeries, or blade server iSCSI HBA

Before you continue with this procedure print the *iSCSI Network Planning Worksheets* in the *iSCSI Network Planning Guide*.

Select System x, xSeries, or blade server replacement from the following list:

Important: In either procedure make a note of the MAC addresses from the sticker on the iSCSI HBA in the *iSCSI Network Planning Worksheets*.

- System x or xSeries: Refer to the System x or xSeries server documentation to perform this task. Any Ethernet cables connected to the original iSCSI HBA will need to be reconnected after the replacement iSCSI HBA is installed.
- blade server: Refer to the blade server documentation to perform this task.

Configure the replacement iSCSI HBA

The new iSCSI HBA will need to be configured to match the replaced iSCSI HBA. Also, the remote system network server configuration object associated with the xSeries or blade server this iSCSI HBA is installed in will need to be updated to reflect the new iSCSI HBA hardware.

Obtain and update remote system network server configuration object information

You will need to update the remote system network server configuration object information after you reinstall the adapter. Use the procedure in this section to accomplish this task.

To complete the following procedure you will need the *iSCSI Network Planning Worksheets* you filled in during the initial installation of this iSCSI Host Bus Adapter. If you are not able to locate these worksheets you will have to print and fill in a new set. For instructions see iSCSI Network Planning Guide.

Remember: Ensure that you record the Media Access Control (MAC) address from the new iSCSI adapter in items RS11 and RS15 of the planning worksheets.

1. Open iSeries Navigator.
2. Select **Integrated Server Administration** → **iSCSI Connections** → **Remote Systems**.
3. Right-click on the appropriate remote system configuration in the list and select **Properties**.
4. Click the **Boot Parameters** tab.
5. Record in the *iSCSI Network Planning Worksheets* (item RS6) if either **Dynamically delivered to remote system via DHCP** or **Manually configured on remote system options** is indicated.
6. Click the **CHAP Authentication** tab.
7. Record in the *iSCSI Network Planning Worksheets* (item RS7) if either **Do not use CHAP** or **Use the following values for CHAP authentication** is indicated.
8. Record the **CHAP** name (item RS8) and **CHAP secret** (item RS9) values in the *iSCSI Network Planning Worksheets* if CHAP is being used.
9. Click the **Network Interfaces** tab.
10. Select the interface you are configuring and click the **Properties** tab.
11. Change the value for **Remote SCSI interface: Local adapter (MAC) address** to the value copied from the adapter and entered in the *iSCSI Network Planning Worksheets* (item RS11).
12. If the **Manually configured on remote system** option was selected, note the values for **Remote SCSI interface: Internet address** (item RS12), **Remote SCSI interface: Subnet mask** (item RS13) and **Specific iSCSI qualified name** (item CQ6) in the *iSCSI Network Planning Worksheets*.
13. Change the value for **Remote LAN interface: Local adapter (MAC) address** to the value copied from the sticker (TOE) on the adapter and entered in the *iSCSI Network Planning Worksheets* (item RS15).
14. If the **Manually configured on remote system** option was selected, note the values for **Remote LAN interface: Internet address** (item RS16) and **Remote SCSI interface: Subnet mask** (item RS17) in the *iSCSI Network Planning Worksheets*.
15. Click **OK** to complete the update.
16. Click **OK** to close the window.
17. Click the **Storage Paths** tab on the network server description properties window.
18. Select the storage path with the desired NWSH name and click the **Properties** button.
19. If the **Manually configured on remote system** option was selected, note the value for **iSCSI qualified name (IQN)** in the iSCSI Network Planning Worksheets (item CQ6).

Complete the replacement iSCSI HBA configuration

Locate instructions to complete the configuration of your iSCSI HBA.

Once you have updated the *iSCSI Network Planning Worksheets* with the new information from the previous procedures, "Replace the System x, xSeries, or blade server iSCSI HBA" on page 35 and "Obtain and update remote system network server configuration object information," you can complete the configuration of the iSCSI HBA by following the procedure in "Configure iSCSI HBA" on page 17.

Appendix. Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are tactilely discernible and do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

IBM and accessibility

See the IBM Accessibility Center at http://www.ibm.com/able/ for more information about the commitment that IBM has to accessibility.

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.

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®
BladeCenter
eServer
i5/OS
IBM
iSeries
System i
System i5
System p
System x
xSeries

Microsoft®, Windows®, Windows NT®, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Electronic emission notices

Class A Notices

The following Class A statements apply to the IBM System i models and IBM System p servers with the exception of those that are specifically identified as Class B.

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.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A respecte est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC 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 A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
E-mail: tjahn@de.ibm.com

Warning: 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、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス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。

The following is a summary of the VCCI Japanese statement in the box above.

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Electromagnetic Interference (EMI) Statement - People's Republic of China

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.

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Please note that this equipment has obtained EMC registration for commercial use. In the event that it has been mistakenly sold or purchased, please exchange it for equipment certified for home use.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Class B Notices

The following Class B statements apply to model 9111-520 (stand-alone version), 9131-52A (stand-alone version), 7047-185 and the 9111-285.

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.

Industry Canada Compliance Statement

This Class B digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B respecte est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EC Council Directive 2004/108/EC 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 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.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
E-mail: tjahn@de.ibm.com

VCCI Statement - Japan

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

The following is a summary of the VCCI Japanese statement in the box above.

This is a Class B 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.

IBM Taiwan Product Service Contact Information

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거 지역에서는 물론 모든 지역에서 사용할 수 있습니다.

Radio Protection for Germany

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse B.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse B.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of the manufacturer.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications 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 publications 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 publications 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 THESE PUBLICATIONS. THESE PUBLICATIONS ARE 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.

Printed in USA