



System i and System p

Managing the Hardware Management Console (HMC)





System i and System p

Managing the Hardware Management Console (HMC)

Note

Before using this information and the product it supports, read the information in “Notices,” on page 93 and the manual *IBM Systems Safety Information*, G229-9054.

Tenth Edition (August 2006)

© Copyright International Business Machines Corporation 2004, 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Managing the Hardware Management

Console (HMC). 1

Printable PDF	1
HMC concepts.	1
Implementations of HMCs.	1
HMC user interface	3
Navigation area	4
Contents area	4
Menu bar	4
Toolbar	5
Status bar	5
HMC applications	5
Tasks and roles	6
Definitions of HMC roles	6
HMC configuration tasks	7
HMC user management tasks.	9
Predefined passwords for hscroot and root user IDs	11
HMC network connections	11
Types of HMC network connections	11
Private and open networks in the HMC environment	12
HMC as a DHCP server	16
Web-based System Manager Remote Client.	17
Installation requirements for the remote client	17
Remote client comparison	18
System Manager Security.	18
When should I back up the HMC?	21
Setting up the HMC	21
Cabling the HMC	22
Installing the HMC into a rack	28
Installing the external modem into a rack	34
Check the power source on the rack	34
Install the modem into the modem tray	35
Install the modem tray into the rack	36
Complete the installation.	40
Identifying the Ethernet port defined as eth0	42
Gathering information for configuration settings	43
Configuring the HMC	48
Configuring the HMC using the fast path through the Guided Setup wizard	49
Prerequisites	49
Start the fast path through the Guided Setup Wizard.	49
Starting the HMC and passwords	49
Configuring network settings	50
Configuring connectivity to your service provider	50
Monitoring your configuration	51
Configuring the HMC using the Guided Setup wizard	51
Prerequisites	51
Run the Guided Setup Wizard	51
After you have completed the Guided Setup Wizard.	51

Accessing the Guided Setup wizard using the HMC interface	53
Configuring the HMC using the HMC configuration checklist.	53
Changing the predefined passwords for hscroot and root user IDs.	54
Configuring network connections	54
Setting identification information	59
Configuring a routing entry as the default gateway	59
Configuring domain name services	60
Configuring domain suffixes.	60
Testing the connection between the HMC and the managed system	60
Postconfiguration steps for the HMC	60
Replacing an HMC	61
Installing and securing the remote client.	62
Configuring one HMC as a certificate authority	62
Generating private key ring files for the servers	63
Installing private key ring files on the servers	63
Distributing the certificate authority's public key with Web-based System Manager Remote Client for Java Web Start	64
Distributing the certificate authority's public key with Web-based System Manager Remote Client	64
Viewing configuration properties	65
Configuring HMC object manager security	66
Installing the Web-based System Manager Remote Client	66
Uninstalling the Web-based System Manager Remote Client	67
Installing the Web-based System Manager Remote Client for Java Web Start	67
Uninstalling the Web-based System Manager Remote Client for Java Web Start	68
Working with the HMC	69
Basic operations	69
Starting the HMC	69
Shutting down, rebooting, and logging off the HMC	69
Setting the date and time.	69
Changing the HMC interface language	70
Configuring the HMC keyboard layout	70
Viewing recent HMC activity	71
Working with partition profile information	71
Backing up partition profile data	72
Initializing profile data	72
Restoring profile data	72
Removing profile data.	73
Collecting and viewing resource utilization data	73
Setting the HMC to collect resource utilization data for managed systems	73
Viewing resource utilization data for a managed system.	74
Backing up and restoring the HMC	74

Setting up the network interface as a startup device	75	Editing HMC user information and roles	84
Setting up a remote system for HMC installation, backup, or restoration over the network	76	Changing HMC user passwords	84
Backing up the entire HMC hard drive to a remote system	77	Using the HMC remote command line	84
Backing up critical HMC data	78	Viewing HMC remote command information	84
Restoring the entire HMC hard drive using the network	79	Setting up secure script execution between SSH clients and the HMC	84
Restoring critical HMC data	80	Enabling and disabling HMC remote commands.	86
Restoring from DVD	80	Troubleshooting HMC setup.	86
Restoring from a remote server.	81	Related information	91
Scheduling and reviewing HMC backups	81		
Saving HMC upgrade data	81	Appendix. Notices 93	
Reinstalling the HMC machine code	82	Trademarks	94
Working with users, roles, and passwords	82	Regulatory notices	95
Creating an HMC user	83	Class A Notices	95
Viewing an HMC user description.	83	Class B Notices	97
Copying HMC user information	83	Terms and conditions	99
Deleting an HMC user.	83	Product recycling and disposal	99
Creating a customized HMC role	83	Battery return program	100
		IBM Cryptographic Coprocessor Card Return Program	100

Managing the Hardware Management Console (HMC)


Understand how to manage your Hardware Management Console.

You can manage your servers, logical partitions, and Capacity on Demand with the Hardware Management Console (HMC). The HMC communicates with systems using service applications to detect, consolidate, and send information to IBM® for analysis.

Attention: To avoid potential problems, if you plan to install an earlier version of your server or the HMC, from one release to an earlier release, contact IBM service and support before you perform any installation procedures of this type.

Printable PDF

Use this to view and print a PDF of this information.


To view or download the PDF version of this document, select Managing the Hardware Management Console  (about 1628 KB).

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/readstep2.html) .

HMC concepts

Learn about the different types of HMCs, predefined passwords, installation methods for the remote client, installation requirements for the remote client, and System Manager Security.

The following topics provide essential supporting information to the tasks of setting up the Hardware Management Console (HMC) and installing the remote client:

Implementations of HMCs

Learn about the local HMC, the remote HMC, and the Web-based System Manager Remote Client.

The Hardware Management Console (HMC) is a system that controls managed systems, including IBM eServer™ hardware, logical partitions, and Capacity on Demand. To provide flexibility and availability, there are different ways to implement HMCs, including the local HMC, remote HMC, redundant HMC, and the Web-based System Manager Remote Client. Figure 1 on page 3 illustrates how HMCs might be implemented in your network.

Local HMC

A local HMC is one that is physically located close to the system it manages and is connected by either a private or public network. An HMC in a private network is a DHCP server for the service processors of the systems it manages. An HMC may also manage a system over an open network, where the managed system's service processor IP address has been assigned manually using the Advanced System Management Interface (ASMI). For convenience of service personnel, an HMC should be close in proximity to the servers it manages.

Remote HMC

A remote HMC is one that is network-connected to a distant managed server or HMC.

Redundant HMC

A redundant HMC manages a system that is already managed by another HMC. When two HMCs manage one system, they are peers, and each can be used to control the managed system. One HMC can manage multiple managed systems, and each managed system can have two HMCs. If both HMCs are connected to the server using private networks, each HMC must be a DHCP server set up to provide IP addresses on two unique, nonroutable IP ranges.

Web-based System Manager Remote Client

The Web-based System Manager Remote Client is an application that is usually installed on a PC. You can then use this PC to access other HMCs remotely. Web-based System Manager Remote Clients can be present in private and open networks. You can perform most management tasks using the Web-based System Manager Remote Client.

The remote HMC and the Web-based System Manager Remote Client allow you the flexibility to access your managed systems (including HMCs) from multiple locations.

For more information about how you can plan for and implement HMCs, see *Solutions with the Hardware Management Console (HMC)*.

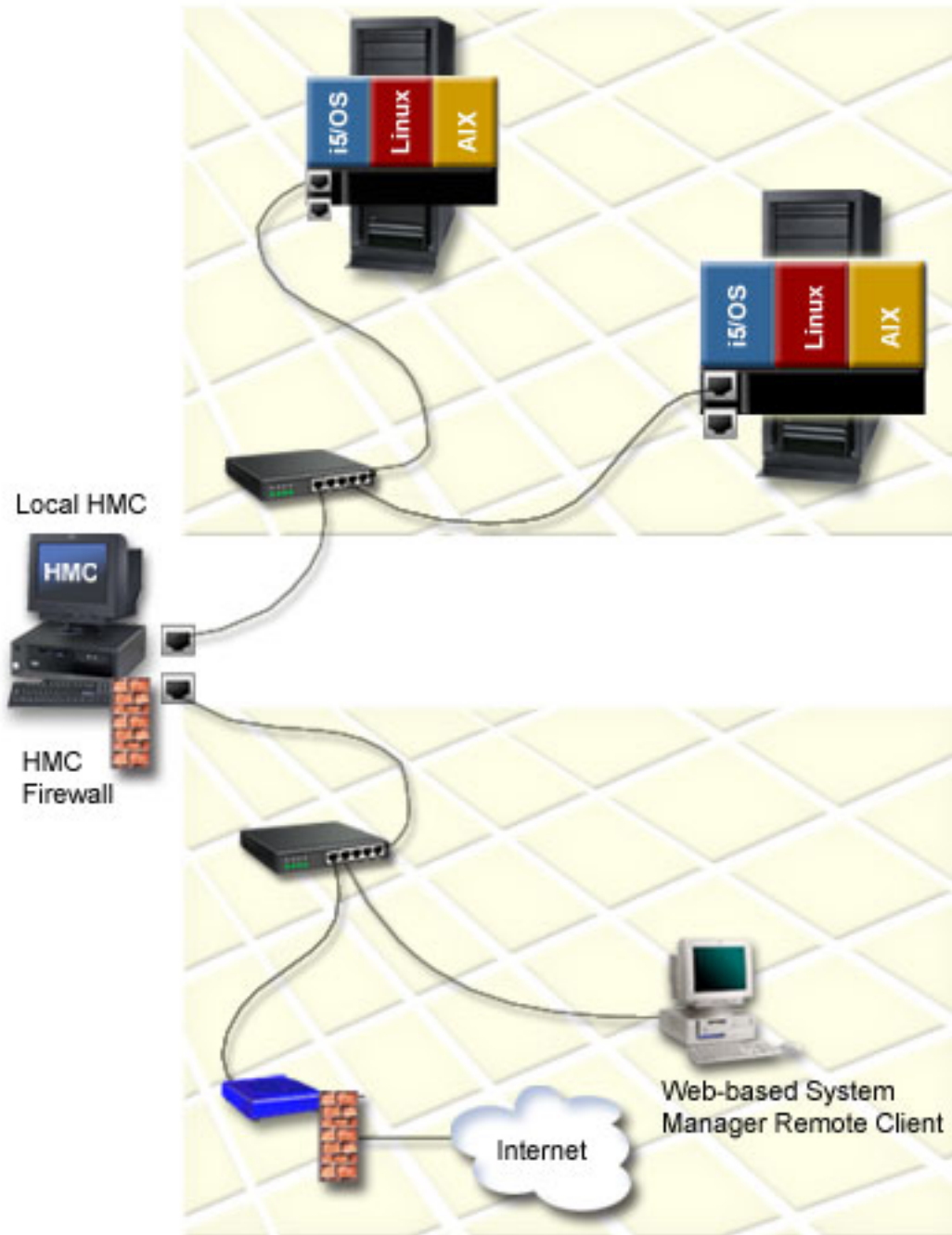


Figure 1. Implementations of HMCs

HMC user interface

Learn about the HMC graphical user interface.

The HMC provides a menu (also called the *context* menu) for quick access to menu choices. The menu lists the actions found in the Selected and Object menus for the current object or objects.

The following components make up the HMC graphical user interface (GUI):

Navigation area

Learn about the navigation area of the HMC GUI.

The left side of the HMC GUI is the Navigation area. It displays a hierarchy of items ordered in a tree structure. The root of the tree is the Management Environment, which contains the name of the HMC into which you are currently logged. This name is the same as the host name that you have given the HMC.

The Management Environment is a set of host systems that can be managed from the HMC. The host systems can be the HMC into which you are currently logged and other remote HMCs.

Each folder in the Navigation area contains different HMC applications used in the specific management task, such as the Server and Partition folder. If you select one of these HMC applications, it provides appropriate submenus and objects in the Contents area.

Contents area

Learn about the contents area of the HMC GUI.

The right side of the HMC GUI is called the Contents area. It displays managed objects and related tasks. You can select different views in the Contents area: large icons, small icons, or details in the form of a list.

Menu bar

Understand the menu bar on the HMC GUI.

The following menu items are provided in the menu bar of the HMC GUI:

Console

The Console menu contains choices that control the console. It enables you to add and remove managed systems, other HMCs, or other systems from the management environment. It also enables you to change themes on the desktop, change font sizes, open an outbound Telnet terminal session using an IP address or a host name, and exit the console.

Object

The title of the Object menu changes to indicate the type of resource managed by the current HMC application. For example, when the Server Management application is selected, the Object menu title becomes Server Management. The Object menu contains general choices and actions for an HMC application that do not require the selection of specific objects to act on. The find function is also located in the Object menu. The contents of the Object menu are updated when a new HMC application is selected.

Selected

The Selected menu contains the set of actions that are applicable to the object selected in the Contents pane. The contents of the Selected menu are updated based on which object you select. The Selected menu is disabled when Overview and Launch applications are loaded. The open tab in the Selected menu expands the view of a managed system in the Navigation area.

View The View menu contains choices for navigating. It also includes choices for customizing the console in the Show submenu. For example, you can select to show or hide the toolbar and status bar. This menu also includes options that control how objects are presented. For example, if the Contents area content provides a choice of views, such as Large Icon, Small Icon, Details, and Tree, these choices are listed here. If the content has only a single view, no view choices are listed. When the content displays an icon or details view, the View menu includes choices for sorting and filtering the container.

Window

The Window menu contains actions for managing subpanels in the console workspace. The new virtual terminal creates a new console subpanel in the workspace. Other choices control how all console subpanels are presented.

Help The Help menu lists user assistance choices. Different options enable you to view help contents, search for help on a particular topic, and view help information about shortcut keys.

Toolbar

Learn about the toolbar on the HMC interface.

The toolbar of the HMC GUI lists commonly used actions that are available when the current plug-in application is loaded. It includes navigation controls, Find and View choices (if available), and a refresh option of the HMC GUI. The toolbar also provides tool tip help when the pointer remains over a toolbar icon for a few seconds.

Status bar

Learn about the status bar on the HMC GUI.

The status bar of the HMC GUI displays at the lower edge of a console panel. It can be hidden or shown by clearing or checking the Status Bar option in the Show submenu under View. The status bar has the following fields ordered from left to right for displaying status information:

Padlock icon

The padlock icon is open when secure communications are not active.

Application loading status

When an HMC application is loaded, the text Ready displays. When an application is in the process of loading, a graphical bar is displayed.

Number of objects visible in the Contents area

Objects can be present on the managed system but hidden from the view by the view filter.

Number of objects selected in the Contents area

This field displays the number of objects that you have selected in the Contents area.

Security context

This field displays the administrator user name and the HMC host name for the currently active HMC.

HMC applications

Understand the HMC folders and applications.

Application folders and application icons are provided in the Navigation area in the HMC GUI. The folders and icons contain several applications to be used for different system management tasks on the HMC and managed systems.

Server and Partition

The Server and Partition folder contains the Server and Frame Management applications. The Server Management application provides all logical partition-related tasks. It is used to create, maintain, activate, and delete logical partitions. This application also provides a focal point for all managed-system related tasks, such as powering the managed system on and off. The Frame Management application provides frame Bulk Power Assembly (BPA)-related tasks. It can be used to update managed frame passwords. This application can also be used to add, initialize, reset, remove, and view properties of managed frames. For more information about logical partitions, see Partitioning the server. For more information about working with the managed system and frame, see Working with managed systems and frames.

System Plans

This folder contains the system plan applications. A system plan is a specification of the logical partition configuration of a single managed system. Use the System plans applications to import, deploy, and manage system plans.

For more information about system plans, see Creating partitions from a system plan.

Licensed Internal Code Maintenance

The Licensed Internal Code Maintenance application folder contains the HMC Code Update and Licensed Internal Code Updates applications. For more information about using these applications to maintain the code on your systems, see [Getting fixes](#).

HMC Management

This folder contains the HMC configuration and HMC Users applications. Use the HMC configuration application to do the following:

- Set the HMC date and time. For more information about setting the HMC date and time, see [“Setting the date and time”](#) on page 69.
- Configure and test network settings For more information about configuring network settings, see [“Configuring the HMC using the HMC configuration checklist”](#) on page 53.
- View console events For more information about viewing console events, see [“Viewing recent HMC activity”](#) on page 71.
- Schedule routine backups For more information about scheduling backups, see [“Backing up and restoring the HMC”](#) on page 74.
- Enable and disable remote commands and virtual terminals.

Use the HMC Users application to manage HMC users. For more information about managing users, see [“Basic operations”](#) on page 69.

Service Applications

This folder contains several applications to be used for service-related tasks. For more information about using these applications, see [Customer service and support](#).

Information Center and Setup Wizard

The Information Center and Setup Wizard application allows you to open the technical documentation for your server. The Setup Wizard helps you configure the HMC to work with the managed system. For more information about configuring the HMC using the Setup Wizard, see [“Configuring the HMC using the Guided Setup wizard”](#) on page 51.

Switch Management

The Switch Management folder contains applications used to manage switches in cluster environment.

Tasks and roles

Understand the user roles that can be assigned to each HMC user. Learn about the tasks that each HMC user role can perform and the commands associated with each task.

The following topics provide essential information regarding HMC roles and various configuration and user management tasks that can be performed:

Definitions of HMC roles

This section describes the HMC roles that can perform various tasks.

Each HMC user can be a member of a different role. Each of these roles allows the user to access different parts of the HMC and perform different tasks on the managed system. HMC roles are either *predefined* or *customized*.

The roles discussed in this section refer to HMC users; operating systems running on logical partitions have their own set of users and roles.

When you create an HMC user, you must assign that user a task role. Each task role allows the user varying levels of access to tasks available on the HMC interface.

For more information about the tasks each HMC user role can perform and the commands associated with each task, see [Overview of HMC tasks](#).

You can assign managed systems and logical partitions to individual HMC users. This allows you to create a user that has access to managed system A but not to managed system B. Each grouping of managed resource access is called a *managed resource role*.

To learn more about managed resource roles and how to create them, refer to the HMC interface help.

Predefined HMC roles

The predefined HMC roles, which are the default on the HMC, are as follows:

super administrator

The super administrator acts as the root user, or manager, of the HMC system. The super administrator has unrestricted authority to access and modify most of the HMC system.

service representative

A service representative is an employee who is at your location to install, configure, or repair the system.

operator

An operator is responsible for daily system operation.

product engineer

A product engineer assists in support situations, but cannot access HMC user management functions. To provide support access for your system, you must create and administer user IDs with the product engineer role.

viewer

A viewer can view HMC information, but cannot change any configuration information.

Customized HMC roles

You can create customized HMC roles by modifying predefined HMC roles. Creating customized HMC roles is useful for restricting or granting specific task privileges to a certain user.

For more information about creating customized HMC roles, see “Creating a customized HMC role” on page 83.

HMC configuration tasks

Describes HMC configuration tasks and the roles that can perform them.

Use the following table for descriptions of the HMC configuration tasks, the associated commands, and the user roles necessary to perform them.

Table 1. HMC configuration tasks, commands, and user roles

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Add or remove an entry in the HMC syslog configuration file	chhmc	X	X	X	X	
Add or remove an entry in the HMC network time protocol configuration file	chhmc	X	X	X	X	

Table 1. HMC configuration tasks, commands, and user roles (continued)

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Back up critical console data	bkconsdata	X	X	X	X	
Configure whether keyboard mapping configuration will occur during the next HMC reboot	chhmc	X	X	X	X	
Display HMC locale information	lshmc	X	X	X	X	X
Display the HMC BIOS level	lshmc	X	X	X	X	X
Display the HMC configuration	lshmc	X	X	X	X	X
Display the HMC network settings	lshmc	X	X	X	X	X
Display the HMC remote access settings	lshmc	X	X	X	X	X
Display the HMC VPD information	lshmc	X	X	X	X	X
Display the HMC version information	lshmc	X	X	X	X	X
Display the status of prompting for the Terms and Conditions agreement at user login	lsusrtca	X	X	X	X	X
Display the storage media devices on the HMC	lsmediadev	X	X	X	X	X
Enable or disable displaying the Terms and Conditions agreement at user login	chusrtca	X				

Table 1. HMC configuration tasks, commands, and user roles (continued)

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Enable or disable HMC boot from the alternate hard disk partition	chhmc	X	X	X	X	
Enable or disable HMC network boot	chhmc	X	X	X	X	
Get HMC upgrade files	getupgfiles	X	X	X	X	
Install corrective service on the HMC	updhmc	X	X		X	
Modify the HMC configuration	chhmc	X	X	X	X	
Modify the HMC locale	chhmc	X	X	X	X	
Modify the HMC network settings	chhmc	X	X	X	X	
Modify the HMC remote access settings	chhmc	X	X	X	X	
Reboot the HMC	hmcshutdown	X	X	X	X	
Save upgrade data	saveupgdata	X	X	X	X	
Shut down the HMC	hmcshutdown	X	X	X	X	
Update code on the HMC	updhmc	X	X		X	
View console events logged by the HMC	lssvcevents	X	X	X	X	X

For more information about how to perform HMC configuration tasks, see “Working with the HMC” on page 69. For more information on using commands, see “Using the HMC remote command line” on page 84.

HMC user management tasks

Describes HMC user management tasks and the roles that can perform them.

Use the following table for descriptions of the HMC user management tasks, the associated commands, and the user roles necessary to perform them.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Create a user for the HMC	mkhmcusr	X				
Create an access control roles	mkaccfg	X				
Display a user's access control resource instances	lshmcusr	X	X	X	X	X
Display a user's access control roles	lshmcusr	X	X	X	X	X
Display a user's properties	lshmcusr	X	X	X	X	X
Modify a user's access control resource instances	chhmcusr	X	X	X	X	X
Modify a user's access control roles	chhmcusr	X	X	X	X	X
Modify a user's password	chhmcusr	X	X	X	X	X
Modify a user's properties	chhmcusr	X	X	X	X	X
Modify an access control role	chaccfg	X				
Remove an access control role.	rmaccfg	X				
Remove inactive access control resource instances assigned to a user	rmaccfg	X				
Remove a user from the HMC	rmhmcusr	X				
View an access control resource instance	lsaccfg	X	X	X	X	X

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
View an access control role	lsaccfg	X	X	X	X	X

Predefined passwords for hscroot and root user IDs

Learn about the user IDs and passwords included with the HMC.

Predefined user IDs and passwords are included with the HMC. It is imperative to your system's security that you change all predefined passwords immediately.

The following predefined user IDs and passwords are included with the HMC:

User ID	Password	Purpose
hscroot	abc123	The hscroot user ID and password are used to log in to the HMC for the first time. They are case-sensitive and can only be used by a member of the super administrator role.
root	passw0rd	The root user ID and password are used by the service provider to perform maintenance procedures. They cannot be used to log in to the HMC.

HMC network connections

This section describes how the HMC can be used in a network.

You can use different types of network connections to connect your HMC to managed systems.

For more information about configuring the HMC to connect to a network, see "Configuring the HMC using the HMC configuration checklist" on page 53.

For more information about using the HMC on a network, see the following:

Types of HMC network connections

Describes how to utilize HMC remote management and service functions using your network.

The HMC supports the following types of logical communications:

- **HMC to managed system:** This type of communications is used to perform most of the hardware management functions, in which HMC issues control function requests through the service processor of the managed system.
- **HMC to logical partition:** This type of communications is used to collect platform-related information (hardware error events, hardware inventory) from the operating systems running in the logical partitions, as well as to coordinate certain platform activities (dynamic LPAR, concurrent repair) with those operating systems. If you want to use service and error notification features, it is important that you make this connection.
- **HMC to remote users:** This type of communications provides remote users with access to HMC functionality. Remote users can access the HMC in the following ways:
 - By using the remote client to access all the HMC GUI functions remotely
 - By using SSH to access the HMC command line functions remotely
 - By using a virtual terminal server for remote access to virtual logical partition consoles
- **HMC to service provider:** This type of communications is used to transmit data, such as hardware error reports, inventory data, and microcode updates, to and from your service provider. You can use this communications path to make automatic service calls.

The HMC supports up to three separate physical Ethernet interfaces. In the desktop version of the HMC, this consists of one integrated Ethernet and up to two plug-in adapters. In the rack-mounted version, this consists of two integrated Ethernet adapters and up to one plug-in adapter. Use each of these interfaces in the following ways:

- One network interface can be used exclusively for HMC-to-managed system communications, which means that only the HMC and service processors of the managed systems would be on that network. Even though the network interfaces into the service processors are encrypted for the Secure Sockets Layer (SSL) protocol and password-protected, having a separate dedicated network can provide a higher level of security for these interfaces.
- Another network interface would typically be used for the network connection between the HMC and the logical partitions on the managed systems, for the HMC-to-logical partition communications. For more information about configuring the HMC to connect to a network, see “Configuring the HMC using the HMC configuration checklist” on page 53. For more information about the communications options you have for logical partitions, see Communications options for logical partitions.
- The third interface is an optional additional Ethernet connection that can be used for remote management of the HMC. This third interface can also be used to have a separate HMC connection to different groups of logical partitions. For example, you might want to have an administrative LAN that is separate from the LAN on which all the usual business transactions are running. Remote administrators could access HMCs and other managed units using this method. Sometimes the logical partitions are in different network security domains, perhaps behind a firewall, and you might want to have different HMC network connections into each of those two domains.

For more information about physically cabling the HMC to the managed system, see Cabling your server.

Private and open networks in the HMC environment

Explains how a private and open network are used in relation to the HMC.

This topic describes when you might want to use a private network, and when you might want to use an open network.

Note: If you are connecting the HMC to the model 9118-575 server or the 590 or 0595 managed servers, you must configure the HMC in a private DHCP network.

The connection between the HMC and its managed systems can be implemented either as a private or open network. The term *open* refers to any general, public network that contains elements other than HMCs and service processors that is not isolated behind an HMC. The other network connections on the HMC are considered open, which means that they are configured in a way that you would expect when attaching any standard network device to an open network.

In a private service network, however, the only elements on the physical network are the HMC and the service processors of the managed systems. In addition, the HMC provides Dynamic Host Configuration Protocol (DHCP) services on that network, which allow it to automatically discover and assign IP configuration parameters to those service processors. You can configure the HMC to select one of several different address ranges to use for this DHCP service, so that the addresses provided to the service processors do not conflict with addresses used on the other networks to which the HMC is connected. The DHCP services allow the elements on the private service network to be automatically configured and detected by the HMC, while at the same time preventing address conflicts on the network.

On a private network, therefore, all of the elements are controlled and managed by the HMC. The HMC also acts as a functional firewall, isolating that private network from any of the open networks to which the HMC is also attached. The HMC does not allow any IP forwarding; clients on one network interface of the HMC cannot directly access elements on any other network interface.

To take advantage of the additional security and ease of setup, implement service network communications through a private network. However, in some environments, this is not feasible because

of physical wiring, floor planning, or control center considerations. In this case, the service network communications can be implemented through an open network. The same functionality is available on both types of networks, although the initial setup and configuration on an open network require more manual steps.

The following figures show representations of private and open networks:

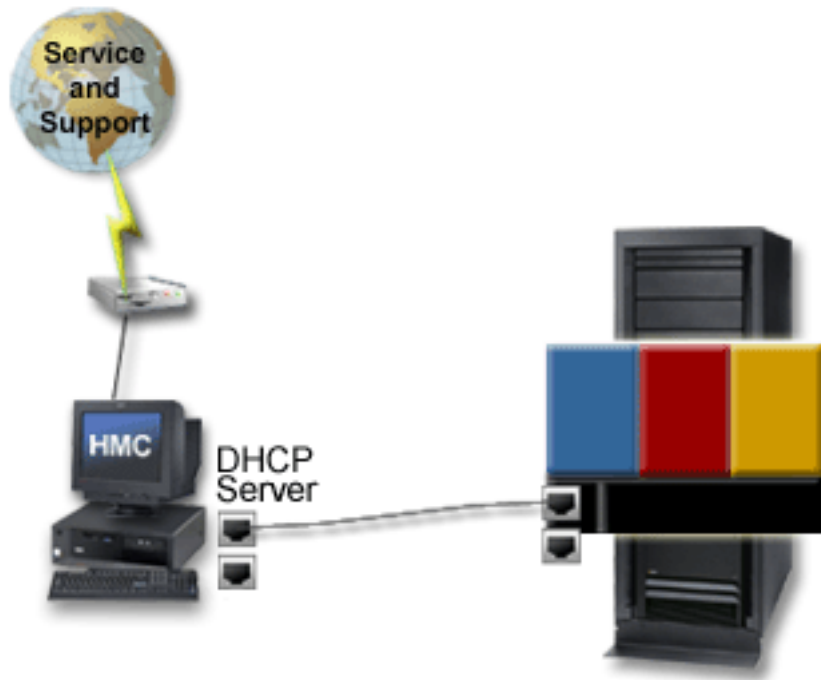


Figure 2. Private network: direct connection

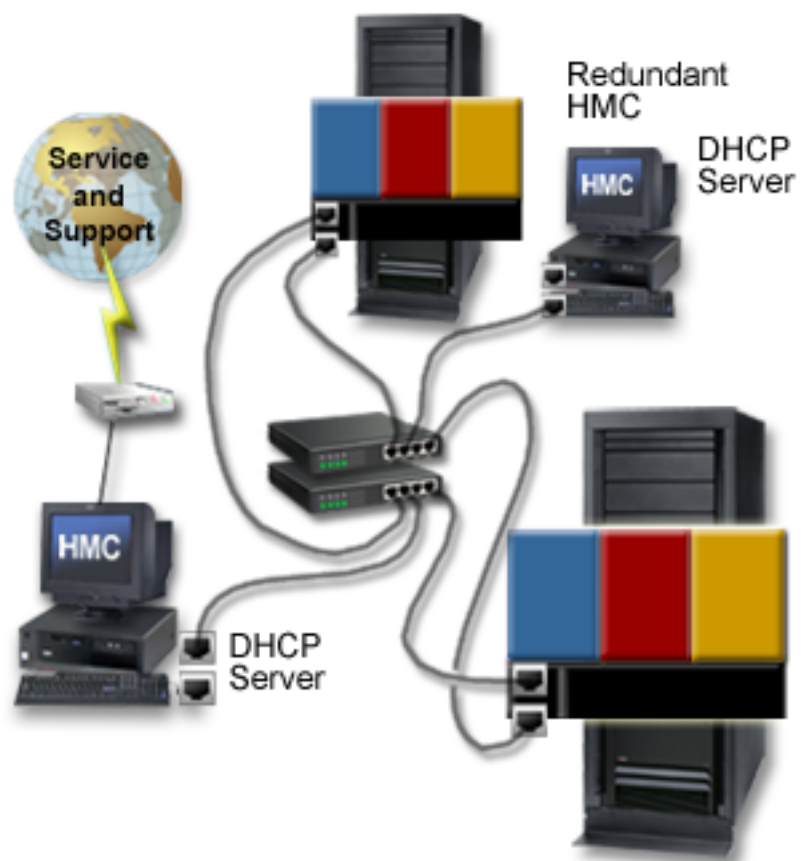


Figure 3. Private network: indirect connection

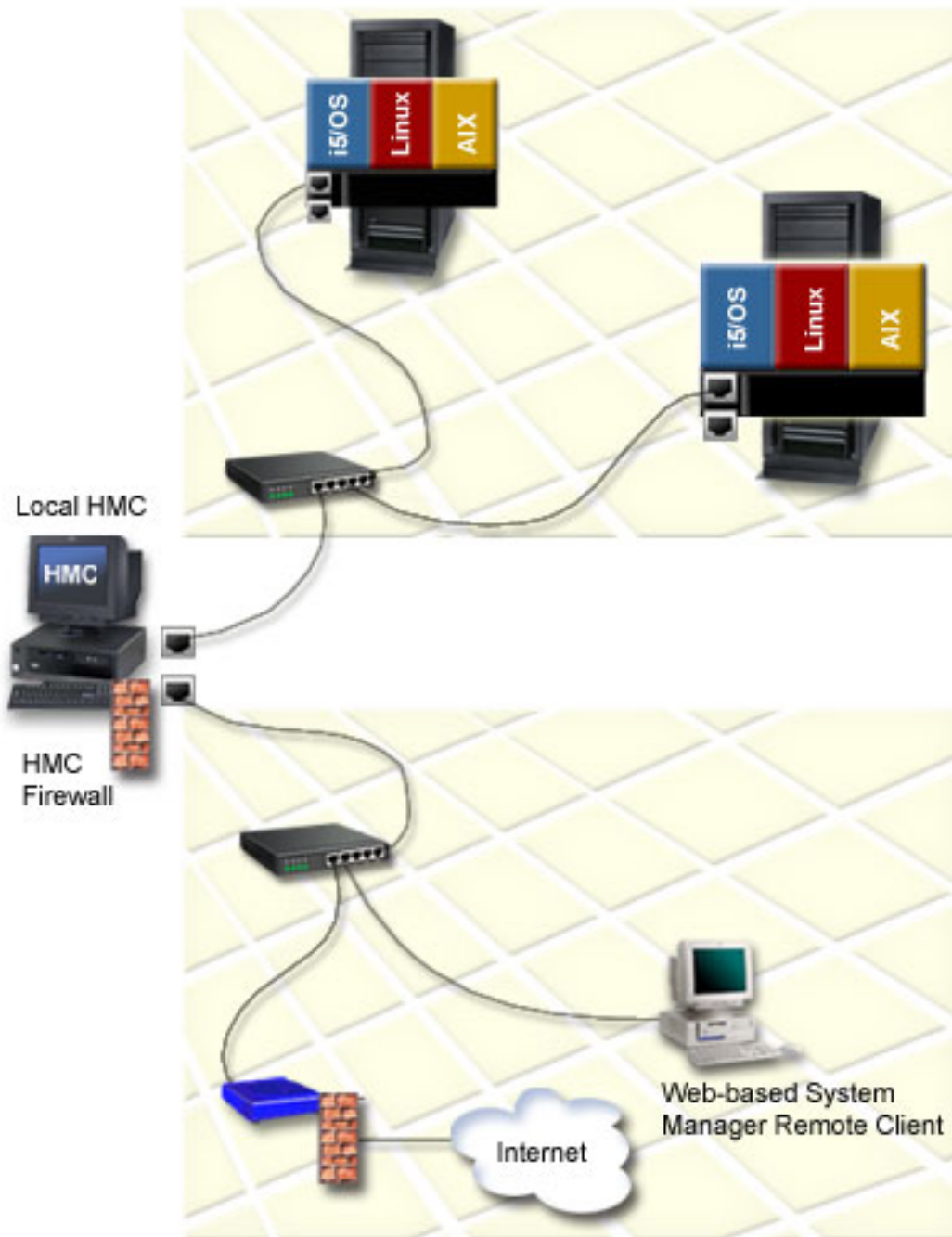


Figure 4. Open network

Choosing a private network

Designate the first HMC network interface as private if any of the following is true:

- Only the HMC and service processors will be endpoints on that network.
- All elements will be connected in a single subnet, and you will not be routing or switching.
- You want the HMC to automatically configure and detect the managed systems associated with those service processors.
- You want to keep the service network isolated behind the HMC.

Choosing an open network

Designate the first network interface as open if you want to run the communications between the HMC and the service processors across an open network that crosses multiple subnets or has other devices on the network.

For more information about choosing a network type, see “Selecting the network type” on page 55.

HMC as a DHCP server

Explains the basics of DHCP and how to use the HMC as a DHCP server.

If you want to configure the first network interface as a private network, you can select from a range of IP addresses for the DHCP server to assign to its clients. The selectable address ranges include segments from the standard nonroutable IP address ranges.

In addition to these standard ranges, a special range of IP addresses is reserved for IP addresses. This special range can be used to avoid conflicts in cases where the HMC-attached open networks are using one of the nonroutable address ranges. Based on the range selected, the HMC network interface on the private network will be automatically assigned the first IP address of that range, and the service processors will then be assigned addresses from the rest of the range.

The DHCP server in the HMC uses automatic allocation, which means that each unique service processor Ethernet interface will be reassigned exactly the same IP address each time it is started. Each Ethernet interface has a unique identifier based upon a built-in Media Access Control (MAC) address, which allows the DHCP server to reassign the same IP parameters.

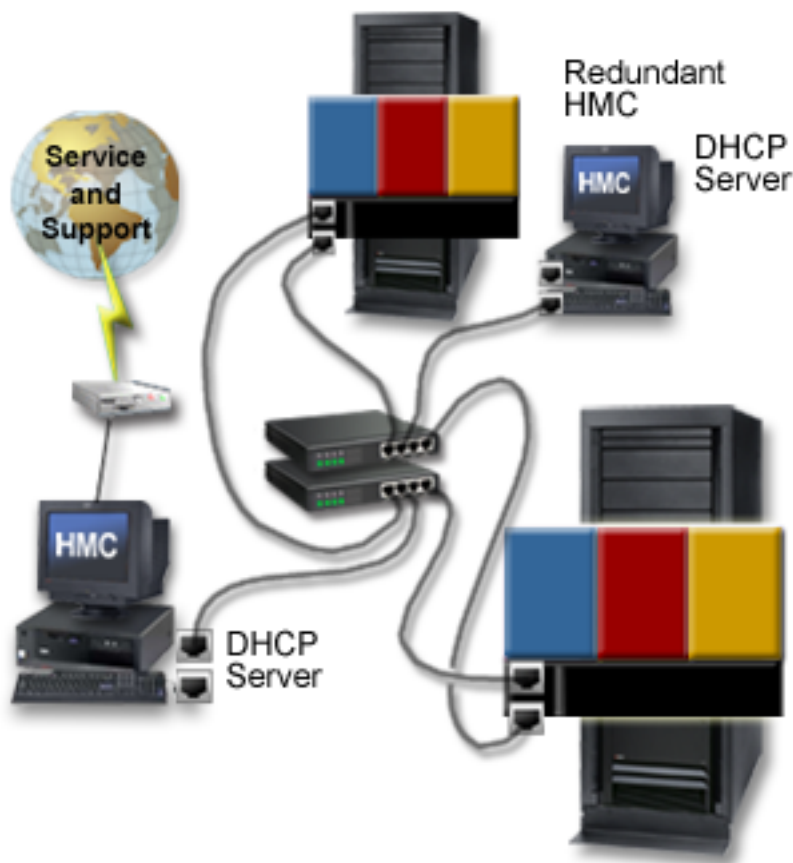


Figure 5. Private network with one HMC as a DHCP server

For more information about how to configure the HMC as a DHCP server, see “Configuring the HMC as a DHCP server” on page 56.

Web-based System Manager Remote Client

Learn about the prerequisites needed for installing the remote client, differences between remote clients, and ways to secure the remote client in your environment.

The following topics provide essential information regarding installing and securing the remote client:

Installation requirements for the remote client

Ensure that your PC is compatible with the remote client.

To install the remote client on a PC, your computer must meet the following requirements:

- Either Microsoft® Windows® (supported versions include Windows 2000, Windows XP, and Windows Server 2003) or the Linux® operating systems (supported versions include Red Hat® Enterprise Linux version 3, (SLES) 8, SLES9, and SUSE Linux Enterprise Server 9.)
- 150 MB of free disk space on the default drive for temporary use during the installation procedure
- 150 MB of free disk space on the drive that you plan to use to install the remote client
- Minimum PC processor speed of 1 GHz
- Minimum of 512 MB of memory (1 GB of memory is recommended for optimum performance)

Remote client comparison

Determine whether to install the Web-based System Manager Remote Client or the Web-based System Manager Remote Client for Java™ Web Start on your PC.

You can access your HMC remotely by installing the Web-based System Manager remote client on your PC. The remote client provides great flexibility by allowing you to manage your system from virtually anywhere you have a PC. You can use either one of these clients: the Web-based System Manager Remote Client and the Web-based System Manager Remote Client for Java Web Start. After you start the remote client, there is no difference between the two.

The following table lists the similarities and differences between the remote clients:

Table 2. Comparisons between the Web-based System Manager Remote Client for Java Web Start and the Web-based System Manager Remote Client

Web-based System Manager Remote Client for Java Web Start	Web-based System Manager Remote Client
<ul style="list-style-type: none">• Available for Linux and Windows platforms• Checks for updates every time it opens, and if updates are available, downloads them automatically• Launches from the Java Web Start console• Automatic update downloads might impact performance if you are using a cable modem or DSL connection• Requires an HTTP server	<ul style="list-style-type: none">• Available for Linux and Windows platforms• Updates require that you uninstall the previous version and install the current version• Installs through an InstallShield wizard• You can select the installation location

System Manager Security

Understand how to secure the HMCs in your environment.

System Manager Security ensures that the HMC can operate securely in client/server mode. Servers and clients communicate over the Secure Sockets Layer (SSL) protocol, which provides server authentication, data encryption, and data integrity. Each System Manager server has its own private key and a certificate of its public key signed by a certificate authority (CA) that is trusted by the System Manager clients. The private key and the server certificate are stored in the server's private key ring file. Each client must have a public key that contains the certificate of the trusted CA.

A **Certificate Authority (CA)** is a trusted central administrative entity (a local HMC in this situation) that can issue digital certificates to clients and servers (HMC4 in Figure 6 on page 20). The trust in the CA is the foundation of trust in the certificate as a valid credential. A CA uses its private key to create a digital signature on the certificate that it issues to validate the certificate's origin. Others, such as System Manager clients, can use the CA certificate's public key to verify the authenticity of the certificates that the CA issues and signs.

Every digital certificate has a pair of associated cryptographic keys. This pair of keys consists of a public key and a private key. A **public key** is part of the owner's digital certificate and is available for anyone to use. A **private key**, however, is protected by and available only to the owner of the key. This limited access ensures that communications that use the key are kept secure. The owner of a certificate can use these keys to take advantage of the cryptographic security features that the keys provide. For example, the certificate owner can use a certificate's private key to "sign" and encrypt data sent between clients and servers, such as messages, documents, and code objects. The recipient of the signed object can then use the public key contained in the signer's certificate to decrypt the signature. Such digital signatures ensure the reliability of an object's origin and provide a means of checking the integrity of the object.

A **server** is a an HMC you want to access remotely. In Figure 6 on page 20, HMCs 1, 3, and 4 are servers. A **client** is a system from which you want to access other HMCs remotely. In Figure 6 on page 20,

Web-based System Manager Remote Clients A, B, and C, and HMCs 1, 2, and 5 are clients. As shown in Figure 6 on page 20, you can configure multiple servers and clients in your private and open networks.

An HMC can be multiple roles simultaneously. For example, an HMC can be a client and a server such as HMC1 in Figure 6 on page 20. An HMC can also be a CA, server, and client at the same time.

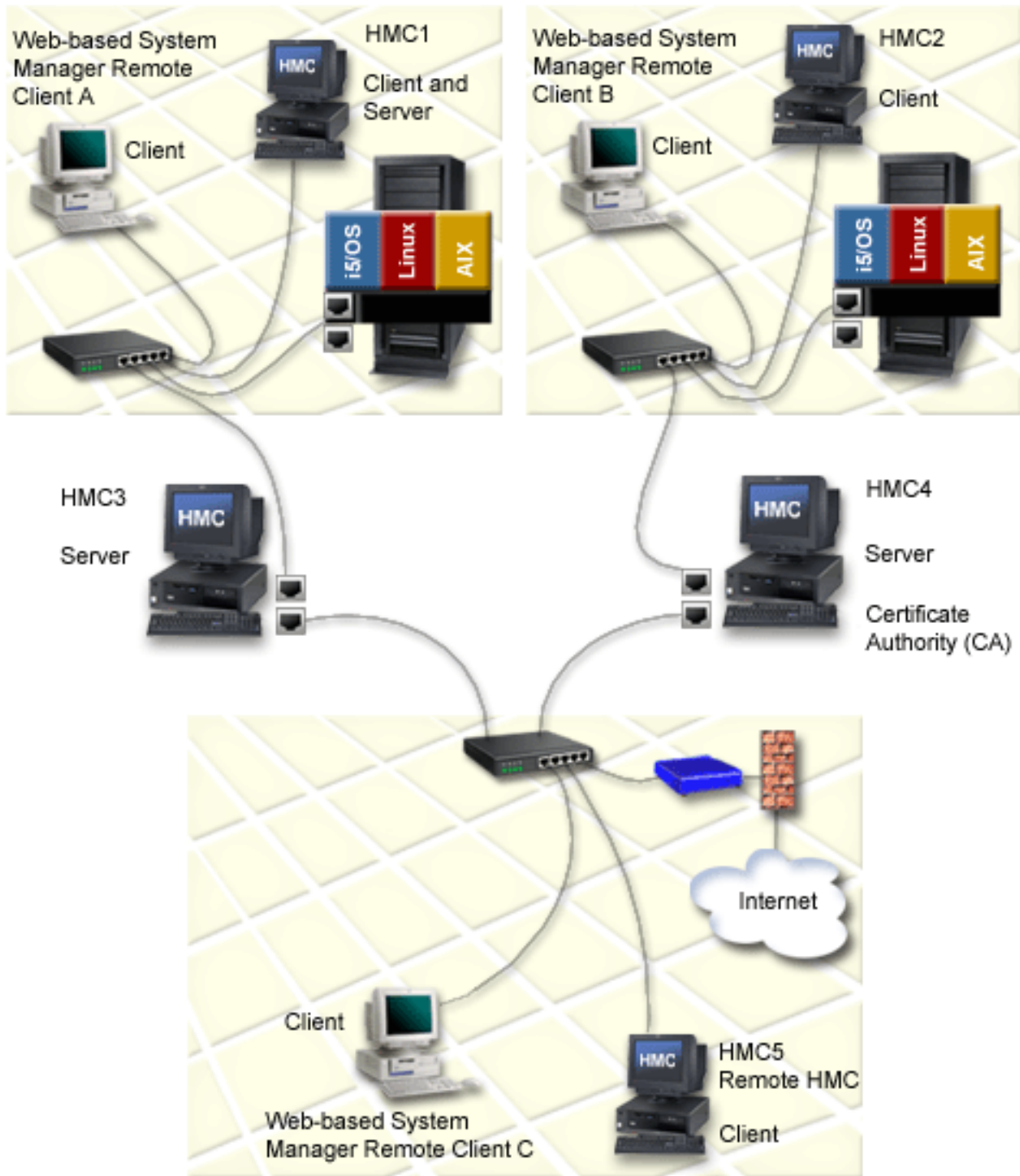


Figure 6. System Manager Security servers and clients

Each server must have a unique private key and a certificate of its public key signed by a CA that is trusted by the clients. Each client must have a copy of the CA's public key.

The following is an overview of tasks involved in "Installing and securing the remote client" on page 62:

1. Configure one HMC as a Certificate Authority (CA).

2. Use this HMC to generate private keys for the servers.
3. Install the private keys on the servers.
4. Configure the servers as secure System Manager servers.
5. Distribute the CA's public key to the servers or clients.

Note: Tasks 3 and 5 are completed by copying the keys to diskette and installing them on the servers or clients.

When should I back up the HMC?

Back up the HMC at regular intervals so that the HMC can be restored in the event of an HMC hardware malfunction.

The backup saves important HMC configuration information, including the following:

- User IDs and roles
- Network configuration information
- Security configuration settings
- Updates Licensed Machine Code components
- Partition profile definitions and snapshots

For more information about backing up the HMC, see *Backing up critical HMC data*.

The HMC keeps a default backup file of the partition data locally, and also on the managed system. The backup file on the managed system is updated each time the HMC partition configuration changes.

If the managed system is in the recovery operating state, the HMC has determined that the partition data stored on the managed system is corrupted, or possibly lost due to a parts replacement service action. The HMC provides the option of overwriting the partition profile data on the managed system with the current partition profile information stored on the HMC. This is why it is important for you to also keep a backup copy of the HMC, with the partition profile data. It is especially important that back up your HMC data in the following instances:

- After you change partition profile information on a managed system
- Before you update managed system Licensed Internal Code
- After you reinstall the HMC machine code or apply corrective service to the HMC
- After you upgrade the HMC machine version to a new level

Setting up the HMC

This section describes how to cable and configure the HMC. This includes installing the HMC into a rack and configuring network connections, security, and service applications.

To set up the Hardware Management Console (HMC), you must complete the following groups of tasks: cabling the HMC to the managed server, gathering configuration settings for your installation, and configuring the HMC. The HMC can be a stand-alone HMC or an HMC you plan to install in a rack. Use the following topics to complete these tasks.

Note: When you have completed the HMC setup, do not power off or disconnect the HMC from the managed system. If the HMC is powered off or disconnected from a nonpartitioned managed system for a period of 14 days, the managed system will no longer recognize the HMC. If this situation occurs and the managed system fails to recognize the HMC, return to this topic and set up the HMC again.

If your system is partitioned, the 14-day time limit does not apply. See the “Postconfiguration steps for the HMC” on page 60 topic.

If you are setting up the HMC along with the setup of a new server, you must perform these tasks in conjunction with other tasks related to your server setup. See Initial server setup for detailed instructions.

To learn more about how to cluster your systems using InfiniBand (IB), see Clustering systems using InfiniBand (IB) hardware.

Cabling the HMC

Connect the HMC cables, connect the Ethernet cable, and connect the HMC to a power source.

DANGER

Electrical voltage and current from power, telephone, and communication cables are hazardous.

To avoid a shock hazard:

- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described below when installing, moving, or opening covers on this product or attached devices.

To Disconnect:

1. Turn everything OFF (unless instructed otherwise).
2. Remove power cords from the outlet.
3. Remove signal cables from connectors.
4. Remove all cables from devices.

To Connect:

1. Turn everything OFF (unless instructed otherwise)
2. Attach all cables to devices.
3. Attach signal cables to connectors.
4. Attach power cords to outlet.
5. Turn device ON.

(D005)

Use the following instructions to help you cable your rack-mounted or stand-alone HMC.

Attention: Do not plug the power cords into the electrical outlet until you are instructed to do so.

1. Use the Specifications for HMC to help ensure that you position the HMC in the correct location.
2. If you are installing a rack-mounted HMC, perform the following steps:

- a. Use the following illustrations to identify the location of the connectors described in these instructions:

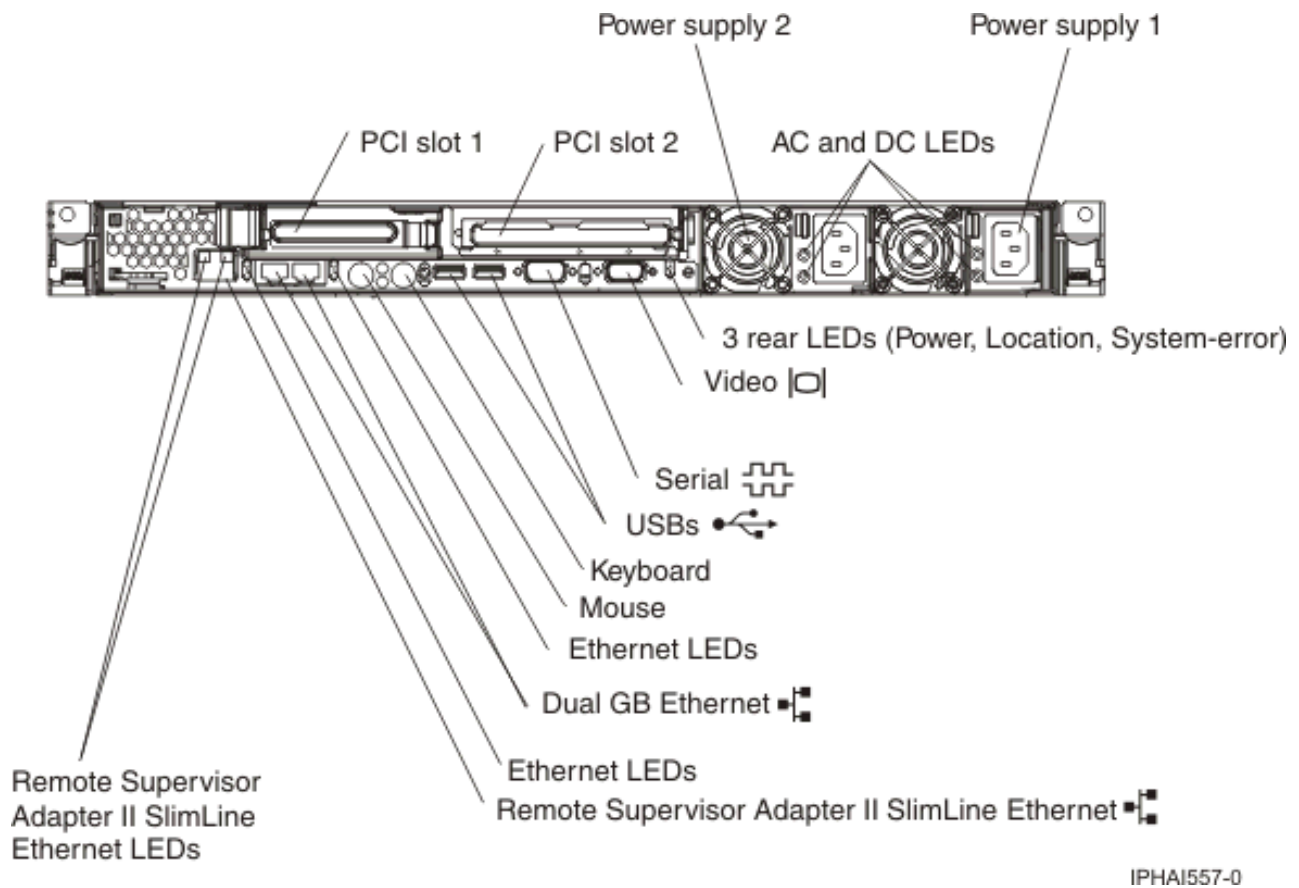


Figure 7. Back view of a rack-mounted HMC (7310-CR3)

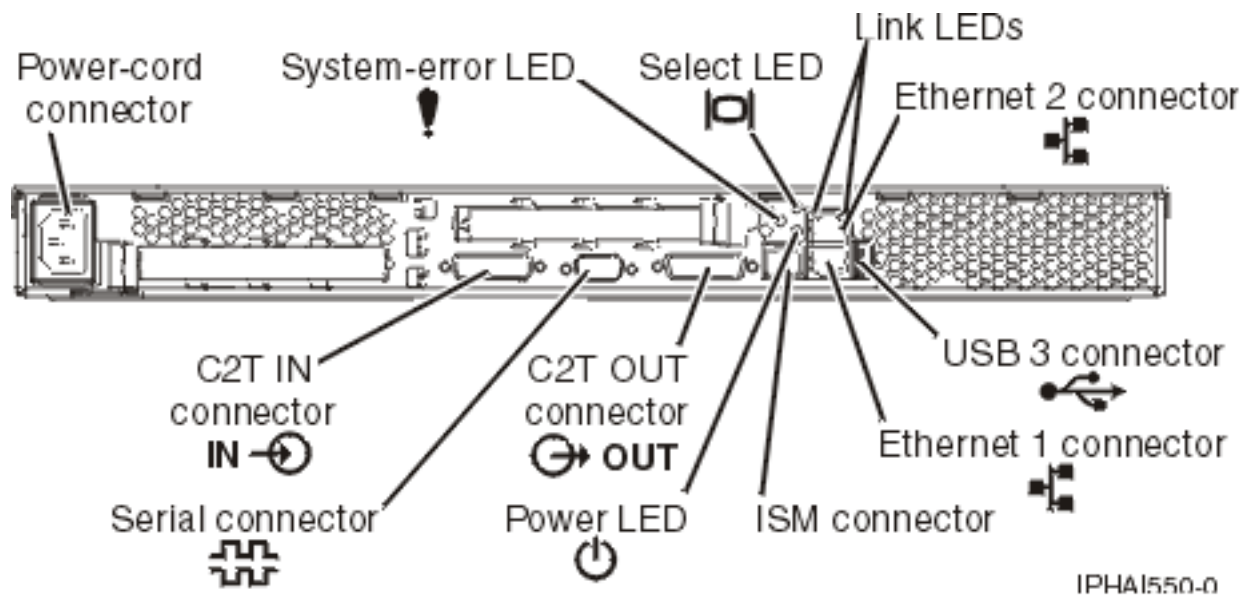


Figure 8. Back view of a rack-mounted HMC (7310-CR2)

- b. Install the HMC into a rack.

c. Connect the monitor, keyboard, and mouse:

For connection to a model 7310-CR2 HMC, connect the keyboard and display to the *C2T-to-KVM* (keyboard, video, mouse) adapter breakout cable that you have previously attached to the HMC. The mouse is integrated with the keyboard.

If you are using a stand-alone monitor, keyboard, and mouse, read the following:

- For connection to a model 7310-CR2 HMC, connect the keyboard and display to the *C2T-to-KVM* (keyboard, video, mouse) adapter breakout cable that you have previously attached to the HMC. If your keyboard and mouse use USB connections, you can also connect them to the USB ports on the front panel of the HMC.
- For connection to a model 7310-CR3 HMC, connect the keyboard, display, and mouse using the USB conversion option cable.

d. Continue with step 4 on page 27.

3. If you are installing a stand-alone HMC, perform the following steps:

- a. Use the following illustrations to identify the location of the connectors described in these instructions:

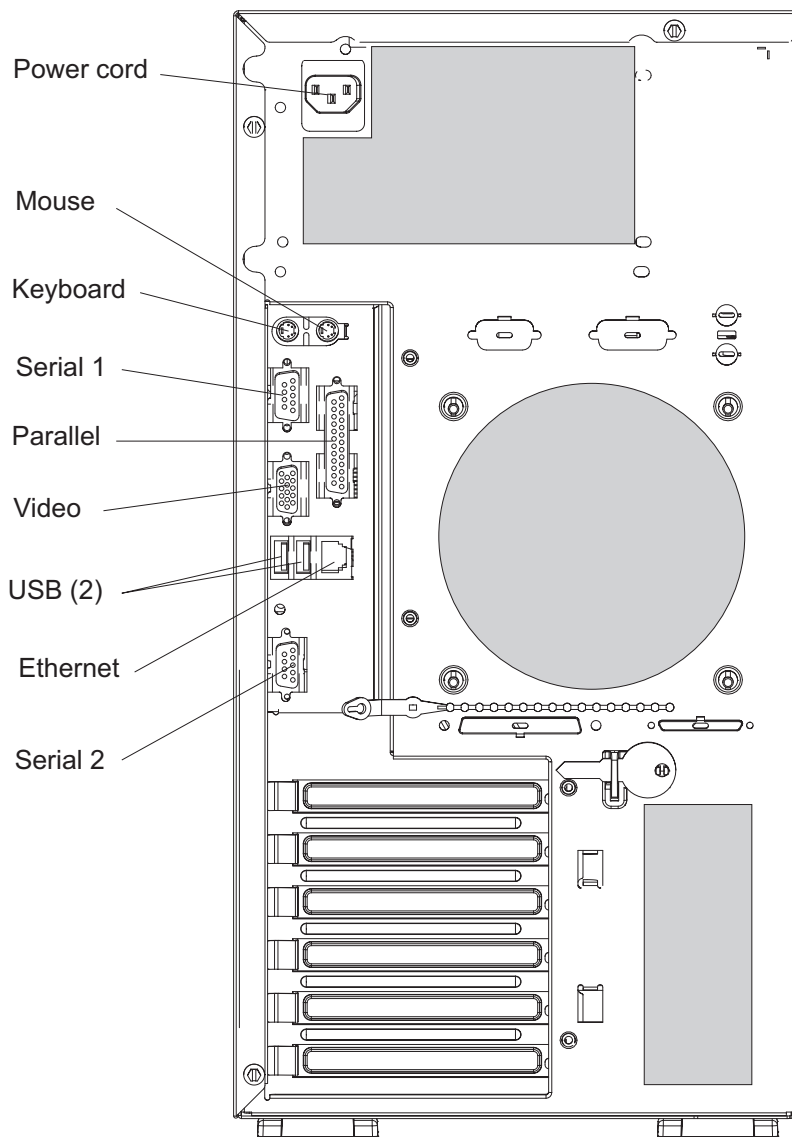


Figure 9. Back view of a deskside 7310-C05

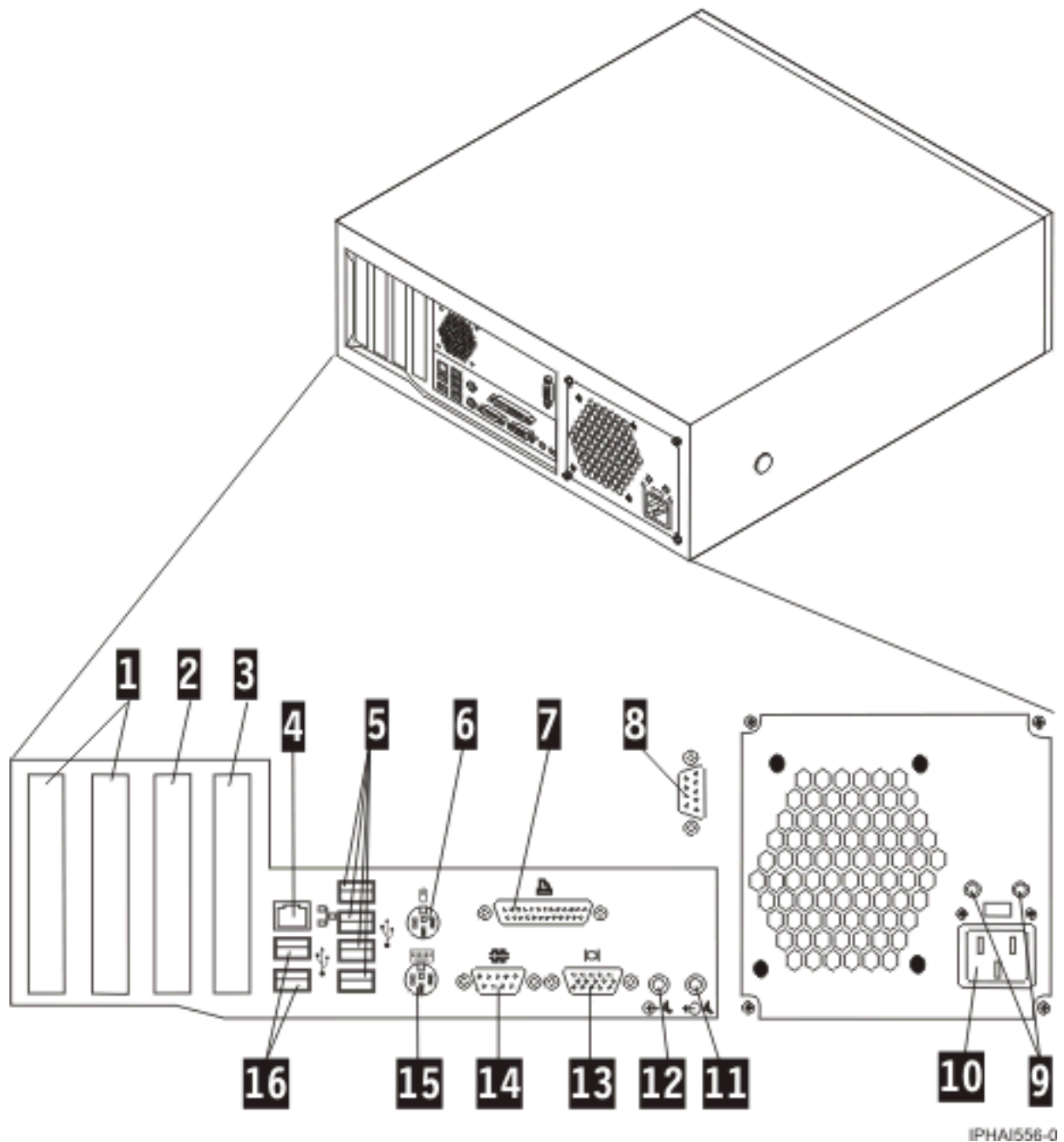


Figure 10. Back view of a stand-alone HMC (7310-C04)

- 1 PCI connectors (slot 1 to left)
- 2 PCI Express (x1) connector
- 3 PCI Express (x16) graphics connector
- 4 Ethernet connector
- 5 USB connectors
- 6 Mouse connector
- 7 Parallel connector

- 9 Diagnostic LEDs
- 10 Power connector
- 11 Audio line-out connector
- 12 Audio line-in connector
- 13 VGA monitor connector
- 14 System connector
- 15 Keyboard connector

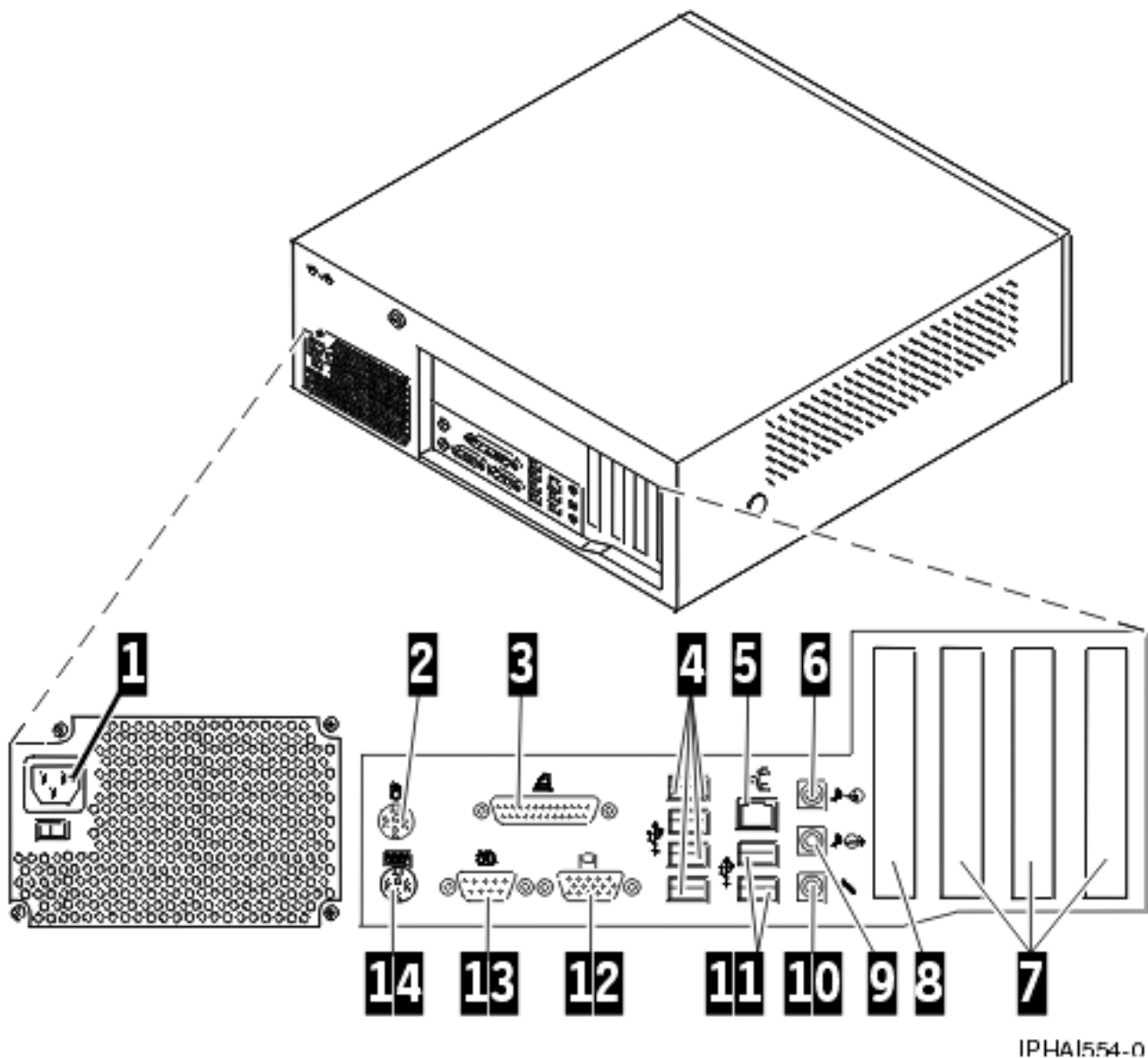


Figure 11. Back view of a stand-alone HMC (7310-C03)

- | | |
|-------------------------------|----------------------------|
| 1 Power connector | 8 AGP slot |
| 2 Mouse connector | 9 Audio line-out connector |
| 3 Parallel connector | 10 Microphone connector |
| 4 USB connectors | 11 USB connectors |
| 5 Ethernet connector | 12 VGA monitor connector |
| 6 Audio line in connector | 13 System connector |
| 7 PCI slots (slot 1 to right) | 14 Keyboard connector |

- b. Attach the monitor cable to the monitor connector, and tighten the screws.
- c. Attach the power cord to the monitor.

- d. Ensure that the voltage selection switch on the HMC is set to the voltage used in your world region. The voltage selection switch is red and is located near the power connector. Move the switch so that the voltage used in your world region is displayed.
 - e. Plug the power cord into the HMC.
 - f. Connect the keyboard and mouse:
 - **USB connections:** Connect the keyboard and mouse to Universal Serial Bus (USB) ports on the HMC. You can connect the keyboard and mouse to the USB ports on the front or back panels.
- Note:** If you are using a stand-alone model 7310-C01 or 7310-C02 HMC, connect the keyboard and mouse to the front-panel USB ports only.
- **PS/2-type connections:** Connect the mouse and keyboard to their connectors on the back panel of the HMC.

4. Connect the modem:

Note: During the installation and configuration of the HMC, the modem might automatically dial out as the HMC follows routine call-out procedures. This is usual behavior.

If you are connecting an external modem, do the following:

- a. Optional: Install the external modem into a rack.
- b. If you have not already done so, connect the modem data cable to the external HMC modem.
- c. Connect the modem data cable to the system port on the HMC labeled with the following symbol:



IPHA1522-0

- d. Use the telephone cable to connect the line port of the external modem to the analog telephone jack on your wall.

If you are connecting to an integrated modem, use the data cable to connect the integrated HMC modem to the appropriate data source. For example, use the telephone cable to connect the HMC modem line port to the analog jack on your wall.

5. Connect the Ethernet (or crossover) cable from the HMC to the managed server:

Note:

- In general, your HMC should be connected to the managed server in a private service DHCP network; specifically, your HMC connection to the 9118-575 server and the 590 and 595 servers must be made in a private service DHCP network.
 - If you have not installed any additional Ethernet adapters in the PCI slots on your HMC, use the primary integrated Ethernet port to complete the following instructions. To find the location of these ports, refer to the illustrations.
 - If you have installed additional Ethernet adapters in the PCI slots, see “Identifying the Ethernet port defined as eth0” on page 42 to determine which Ethernet port you must use.
- You can verify that the Ethernet cable connection is active by observing the green status lights at both the HMC and managed system Ethernet ports as your installation progresses.
- Connect the Ethernet port on the HMC to the Ethernet port that is labeled **HMC1** on the managed server. On the model 9118-575 server and the 590 and 595 servers, use the port labeled J00A on the front bulk power control assembly.

If you are connecting a second HMC to your managed server, connect to the Ethernet port that is labeled **HMC2** on the managed server; on the 9118-575 server and the 590 and 595 servers, use the port labeled J00A on the rear bulk power control assembly.

6. If you use an external modem, plug the modem power supply cord into the HMC modem.
7. Plug the power cords for the monitor, HMC, and HMC external modem into electrical outlets.

Note: Do not connect the managed system to a power source at this time.

8. If you are setting up the HMC to manage a new server, go to Cabling your server. Click **Select by model** and choose the model server you want to cable. Next, select the console you are using, and complete the remaining steps in that checklist.
9. If you are setting up the HMC to manage an existing server, continue with “Gathering information for configuration settings” on page 43.

Installing the HMC into a rack

Use the table provided in this topic to gather required configuration settings that you need to know before you begin the configuration steps.

The following steps are required to install the HMC into a rack:

Note: You can grip any part of the hardware that is blue in color to remove it from or install it in the managed system, open or close a latch, and so on.

DANGER

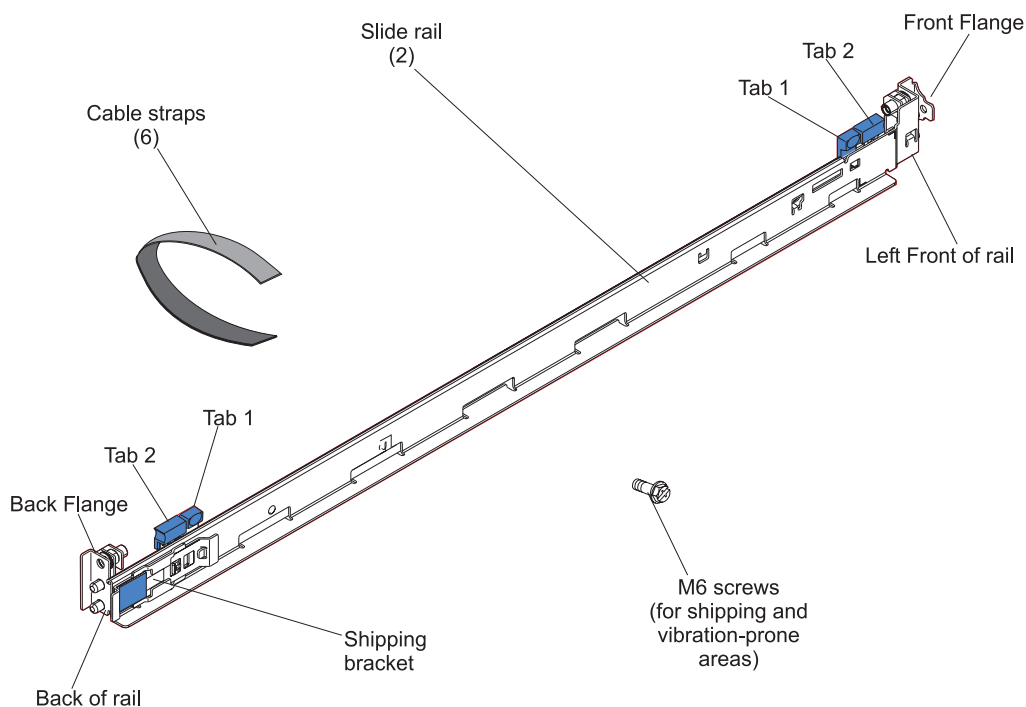
- Always lower the leveling pads on the rack cabinet.
- Always install stabilizer brackets on the rack cabinet.
- To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.
- Rack-mounted devices are not to be used as a shelf or work space. Do not place any object on top of rack-mounted devices.
- Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet before servicing any device in the rack cabinet.
- Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.
- An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

CAUTION:

- Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.
- Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.
- Consideration should be given to the connection of the equipment to the supply circuit so that overloading of the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.
- *(For sliding drawers.)* Do not pull out or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack may become unstable if you pull out more than one drawer at a time.
- *(For fixed drawers.)* This drawer is a fixed drawer and should not be moved for servicing unless specified by manufacturer. Attempting to move the drawer partially or completely out of the rack may cause the rack to become unstable or cause the drawer to fall out of the rack.

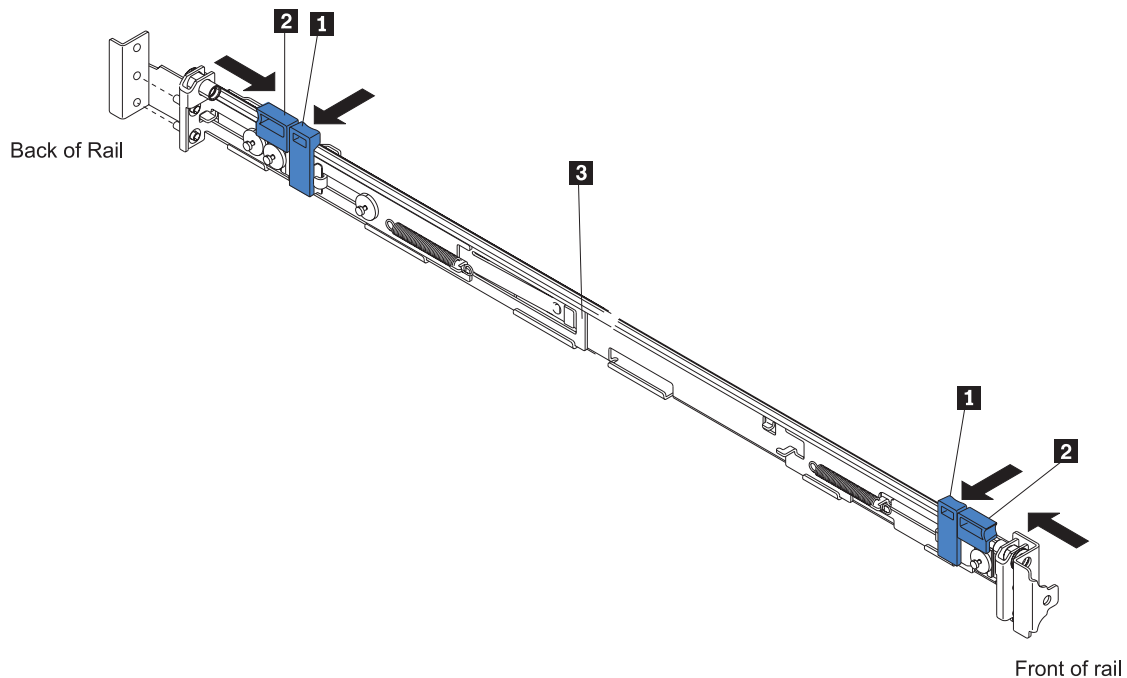
(R001)

1. Use the following illustration to ensure that you have all the items that you need to install the HMC in your rack enclosure. If any items are missing or damaged, contact your place of purchase. For further information about the rack hardware, refer to the documentation that was provided with the rack enclosure.



Attention: Do not place any object weighing more than 50 kg (110 lbs) on top of devices mounted on the rack.

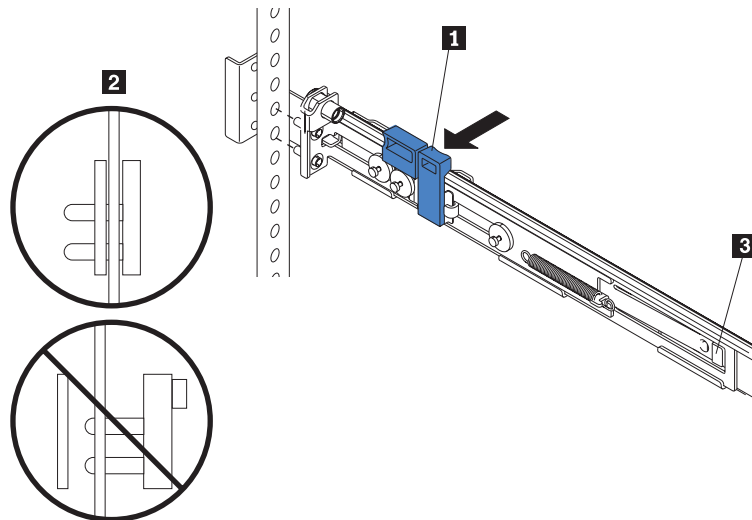
2. Starting with the slide rail that is marked LEFT/FRONT, complete the following tasks to prepare the slide rail for installation in the rack.
 - a. To prevent the rail-adjustment bracket from moving during the next step, press and hold the back of the rail-adjustment bracket 3.
 - b. On the back end of the rail, while holding the blue tab 1 open, press the blue tab 2 to slide the back rail-locking carrier toward the front end until the carrier clicks into the open position.
 - c. On the front end of the rail, while holding the blue tab 1 open, press the blue tab 2 to slide the front rail-locking carrier toward the back end until the carrier clicks into the open position.



IPHA1501-1

3. Position the rail so that the pins on the back rail-locking carrier align with the holes on the back rail-mounting flange. Press the blue tab 1 to release the rail-locking carrier and secure the back of the slide rail onto the back rack-mounting flange.

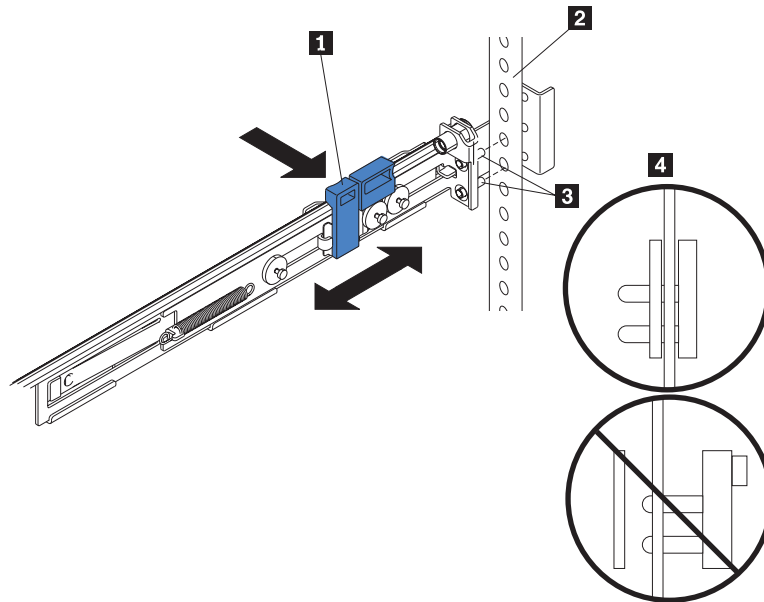
Attention: Ensure that the pins are fully extended through the mounting flange and slide rail 2.



IPHA1502-3

If you need to adjust the slide-rail length, lift the tab 3 and extend the rail-adjustment bracket from the back of the slide rail until it is the appropriate length.

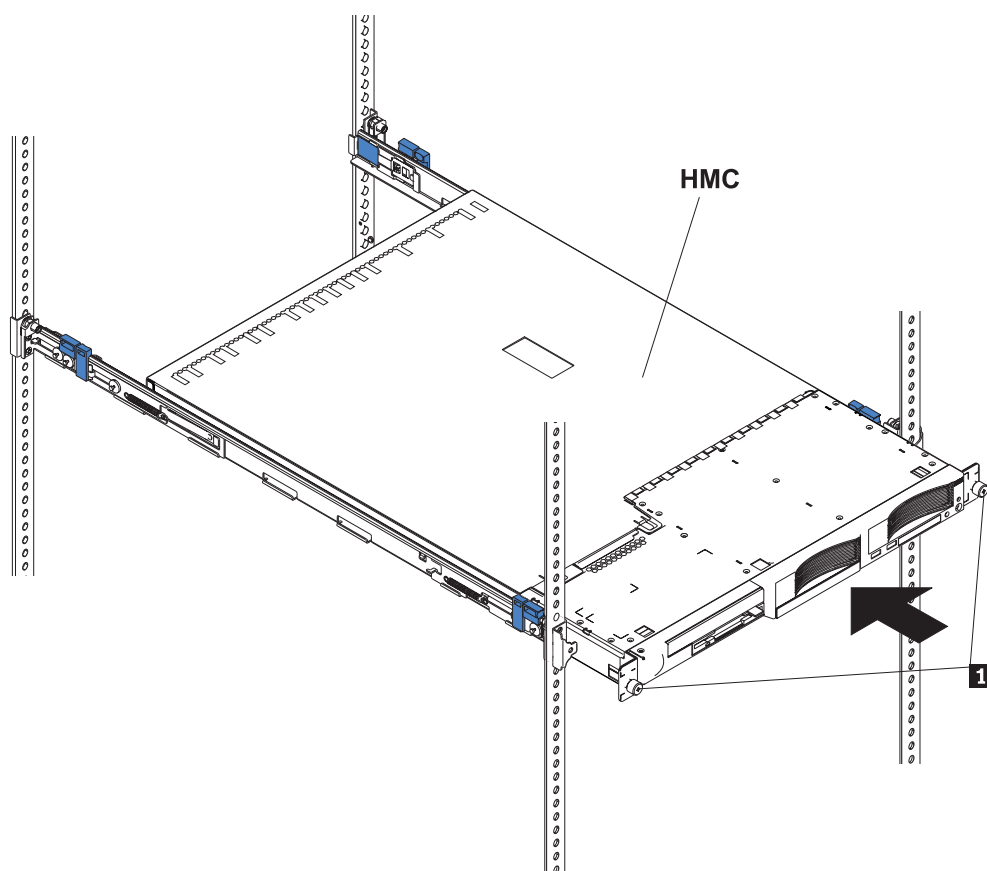
4. Making sure that the rail is level, align the pins 3 on the front rail-locking carrier to the front rack-mounting flange 2. If you adjusted the rail length, push the front rail flange back. Press the blue tab 1 to release the rail-locking carrier and secure the front of the slide rail onto the front rack-mounting flange.



IPHA1503-3

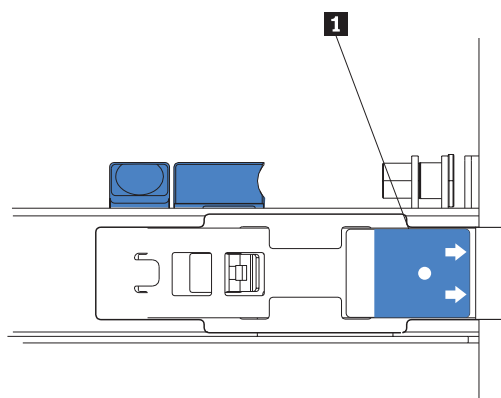
Attention: Ensure that the pins 3 are fully extended through the mounting flange and the slide rail 4.

5. Repeat steps 1 through 4 on page 30 for the slide rail marked RIGHT/FRONT.
6. Align the HMC on the slide rails and push the HMC fully into the rack enclosure.
7. Secure the HMC to the front mounting flanges with the two thumbscrews 1.



IPHA1504-1

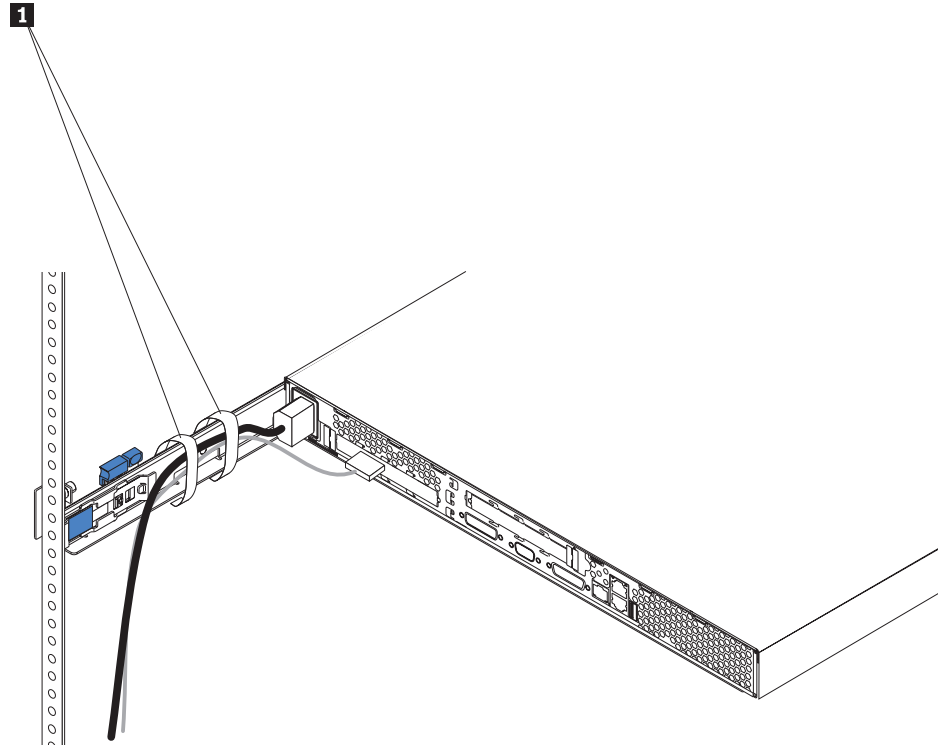
8. If the shipping brackets impede the HMC from fully setting into the rack enclosure, remove the shipping brackets by pressing on the tab 1 as indicated on the shipping bracket, and slide the shipping bracket off the slide rail. Repeat this step for the other shipping bracket. Store the shipping bracket for future use. The following figure shows a side view of the side rail and the shipping bracket tab:



IPHA1505-0

Note: You must reinstall the shipping brackets on the slide rails before you transport the rack enclosure to another location with the HMC installed. To reinstall the shipping bracket, reverse this step.

9. If you are installing a 7310-CR2 HMC, connect the breakout cable (the C2T-to-KVM adapter cable for the keyboard, monitor, and mouse that comes with your HMC) to the port labeled OUT on the back of the HMC, and connect the power cable to the back of the HMC. If you are installing a 7310-CR3 HMC, connect the USB conversion option cable to a USB connector. Route the cables to the lower-left corner of the HMC (as viewed from the back), and use the cable straps **1** to secure the cables to the slide rails.

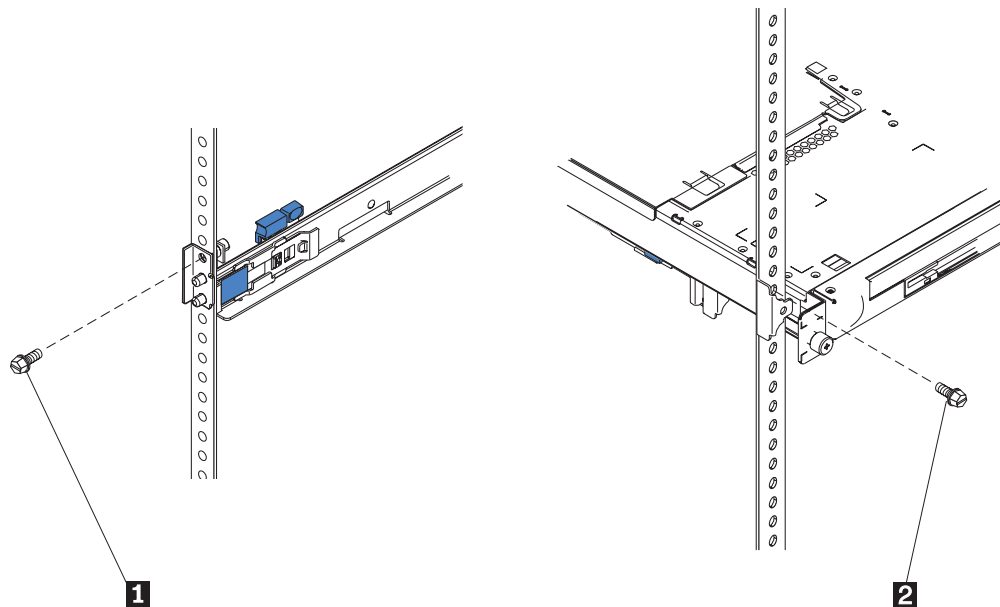


IPHA1506-0

10. If you plan to transport the rack enclosure to another location with the HMC installed, complete the following tasks to secure the HMC to the rack:

Note: To remove the HMC from the rack, reverse these instructions.

- Disconnect the cables from the back of the HMC.
- Slide the HMC out of the rack about 150 mm (6 inches), and insert the M6 screws in the front of each slide rail **2**.
- At the back of the rack, secure the HMC to the rack enclosure with M6 screws **1** and reconnect the cables.



IPHA1507-0

- d. Reinstall the shipping brackets on the slide rails. To reinstall the shipping brackets, reverse the procedure in step 6 on page 31.
 - e. Push the HMC back into the rack and secure it to the rack using the thumbscrews on the front of the rack.
 - f. Reconnect any cables that were disconnected.
11. Continue with step 2c on page 24.

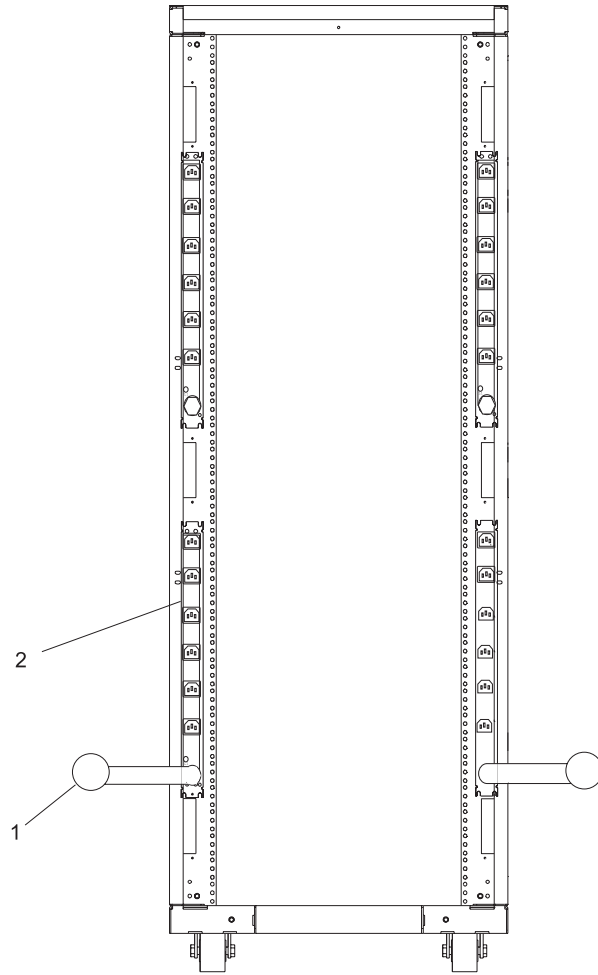
Installing the external modem into a rack

The modem tray supports the MultiTech Systems MultiModem II Model MT5600BA Series modem.

The modem tray attaches to the system rack and holds one or two standalone modems, gateways, or other networking equipment. The modem tray occupies 1 Electronics Industries Association (EIA) location in the rack. If only one modem or other networking unit is installed in the modem tray, a blank filler is used in the empty mounting location to ensure that proper airflow is maintained in the rack. The blank filler also ensures that electromagnetic interference is confined within the rack.

Check the power source on the rack:

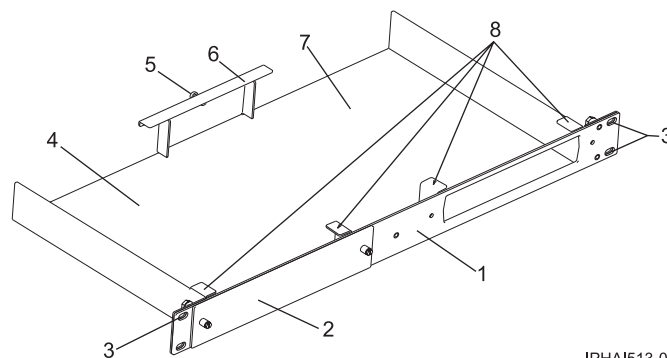
Ensure that the correct power source is available on the rack. The MultiTech Systems MultiModem II Model MT5600BA Series modems are equipped to operate on 120 V ac, 60 Hz, 16 W, or 230 V/50 Hz (international). Racks have power distribution buses (PDB) 2 that supply the correct alternating current and power to operate the modems installed in the modem tray. The main power source plug on the rack is indicated by 1. The PDBs are located at the back and bottom of the rack as shown in the following illustration:



IPHA1521-0

Install the modem into the modem tray:

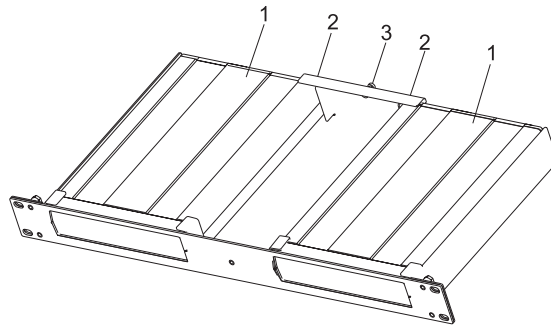
1. Remove the screw 5 securing the retaining bracket 6 at the back of the modem tray 1. The retaining bracket can now be removed from the modem tray. See the following illustration.



IPHA1513-0

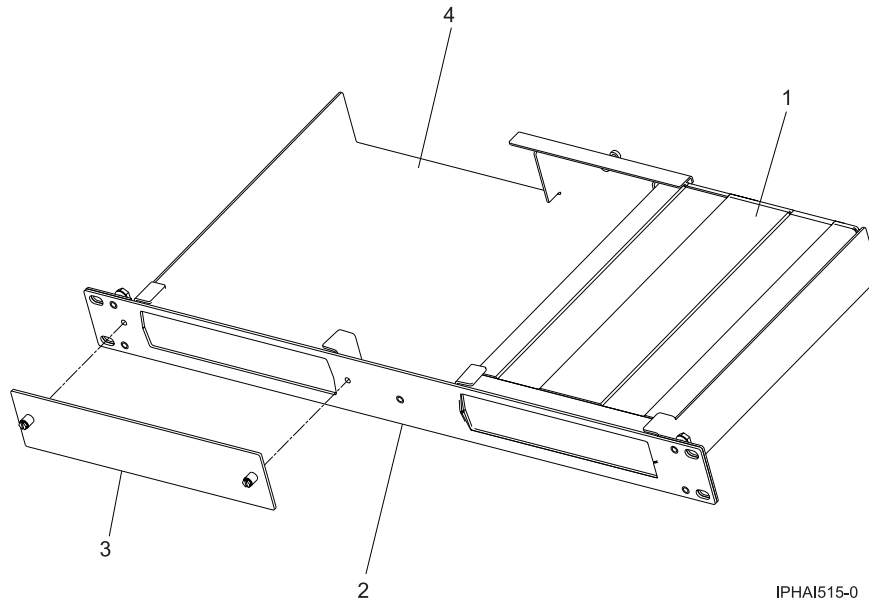
2. Position the modem in the tray 4 or 7 with the front of the modem facing the front of the tray. Slide the front of the modem under the two retainer tabs 8.
3. Position the retaining bracket that was removed in step 1 over the back corner of the modem.
4. Align the screw hole in the retaining bracket to the hole at the back of the modem tray.

5. Reattach the retaining bracket 2 to the back of the modem tray by tightening the retaining bracket screw 3. The installed modems 1 are shown in the following illustration:



IPHA1514-0

6. If you are installing a second modem, do the following:
- Loosen the two screws in the blank filler 2 to detach the filler from the modem tray 2.
 - Remove the blank filler 2 from the front of the empty mounting location 4. See the following illustration.

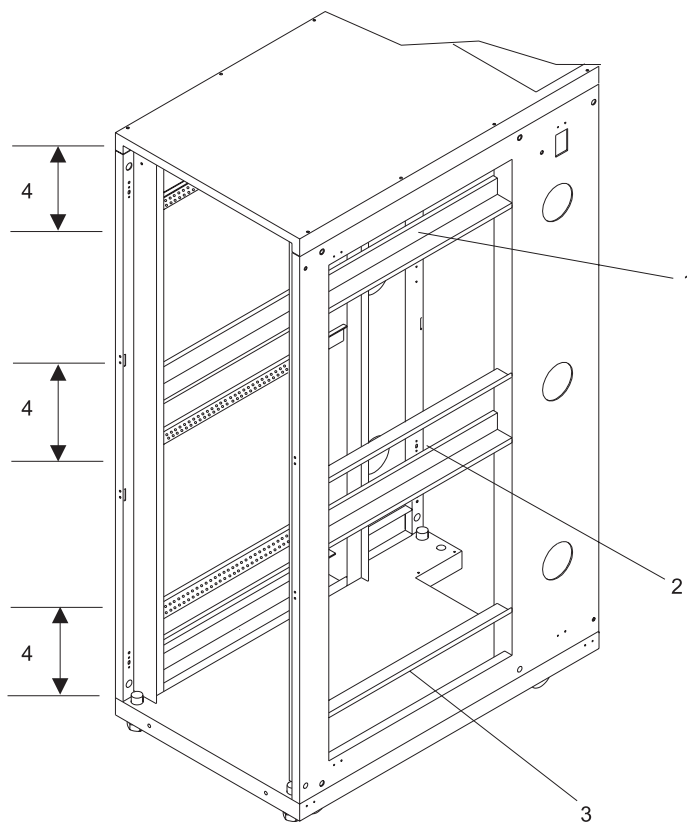


IPHA1515-0

- Repeat steps 1 on page 35 through 5 to install a second modem.

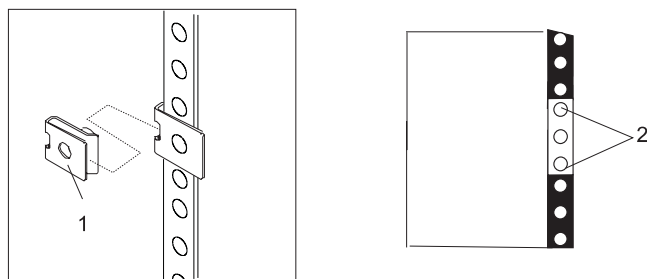
Install the modem tray into the rack:

- Open the rack front and back doors.
- Determine the EIA location for mounting the modem tray into the rack. The modem tray must be mounted at an EIA location adjacent to a horizontal cable-routing support rail on the rack. This mounting location enables the modem data cables and power cables to be correctly routed and secured. The horizontal cable-routing support rails can be identified by their pattern of holes along the rails. The following illustration shows the top horizontal 1, middle horizontal 2, and bottom horizontal 3 cable routing support rails. It then indicates suitable locations for the modem tray 4. The modem tray occupies 1 EIA location in the system rack.



IPHA1516-1

3. Install nut clips 1 on each of the front vertical rails of the rack at the selected EIA installation location 2 as shown in the following illustration.



IPHA1517-0

4. Position the modem tray at the selected installation location, and slide the modem tray into the rack. Ensure that the mounting screw holes on the modem tray align with the nut clips installed on the rack front vertical rails.
5. Insert and tighten the mounting screws.
6. Connect the data cables to the modem by completing the following steps:

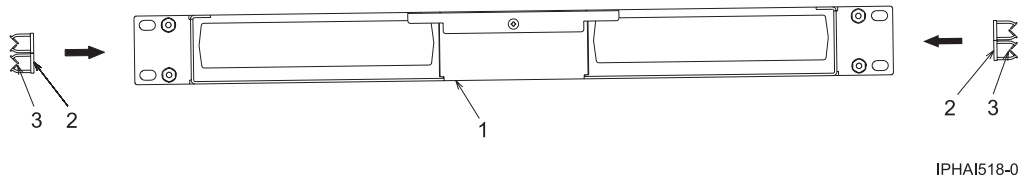
Note: For detailed information about data cable connections, refer to the documentation from the modem manufacturer.

- a. Attach the RS232 cable to the back of the modem. The RS232 cable's pin configuration can be 25-pin to 25-pin, or 9-pin to 25-pin.
- b. Determine the type of additional data cables that will be attached. The modem can operate with either of the following cables:
 - Leased line. Pin configuration can be two-wire or four-wire.

- Telephone line.
- c. Attach the data cables to the back of the modem. Follow the manufacturer's documentation to ensure that the pin configuration is correct.

Note: To gain adequate access to the back of the modem, it might be necessary to slide the system drawer that is located above or below the modem tray out of the rack.

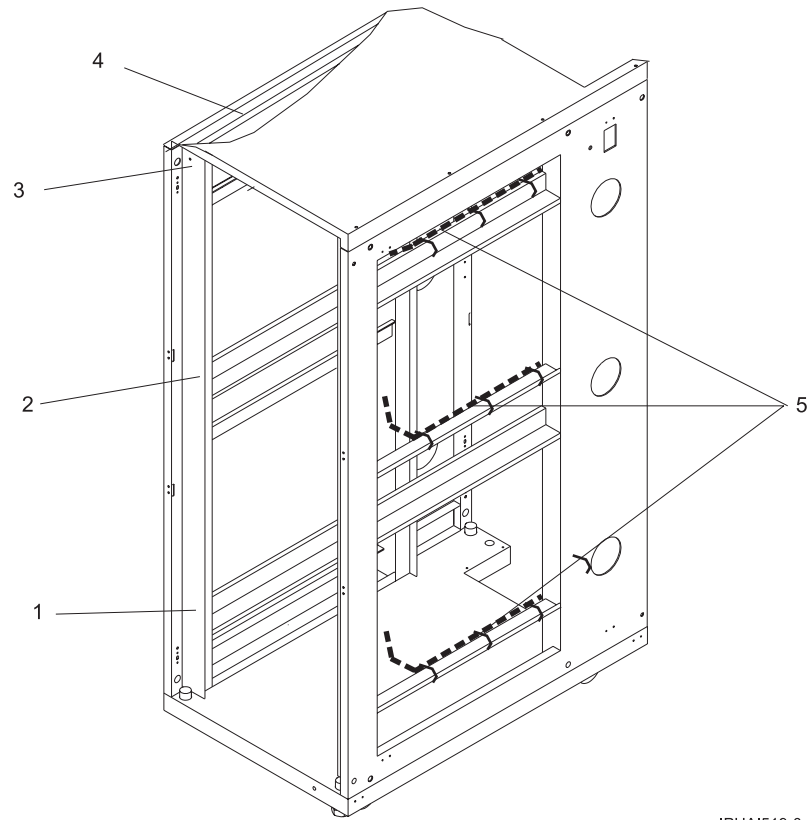
7. Peel off the adhesive covering 2 located on the bottom of each cable clamp 3. Position two cable clamps 3 to each side of the modem tray as shown in the following illustration. Press firmly to adhere the cable clamps 3 to the modem tray. The cable clamps 3 will be used to route cables to the horizontal rack rail.



8. Connect the modem power supply cord to the power connector located on the back of the modem.
9. To avoid cables and the power cord getting pinched between units, route the cables and power cord through the cable clamps located on the side of the modem tray.
10. Route the power cord and data cables from the modem to the appropriate horizontal rail adjacent to the modem tray installation location on the rack.

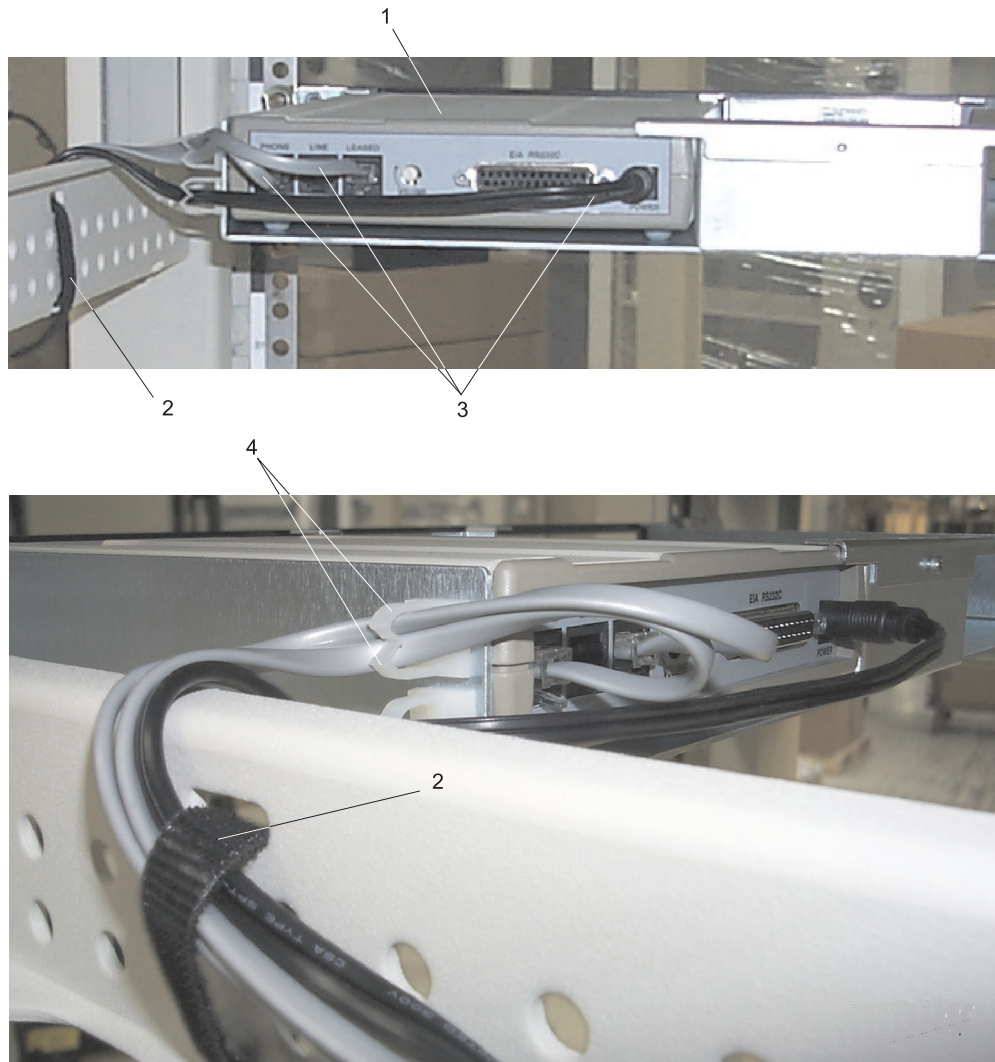
Note: Route the cables and power cord to the closest horizontal support rail. To avoid damage to the cables when other units are slid in or out, ensure the cables and power cord are routed within the EIA space for the modem tray.

The horizontal support rails are located on both sides of the rack. The following illustration shows the bottom 1, middle 2, and top 3 horizontal support rails. It also shows an example of a cable and power cord route at the top of the rack 4 and on the horizontal rails 5.



IPHA1519-0

11. Secure the power cord and data cables **3** to the horizontal rail using the hook-and-loop cable ties **2**. The modem is indicated by **1** and the cable clamps are indicated by **4**. For more detail, see the following illustration:



IPHA1520-0

Note: Before securing the cables and cord, ensure that the connector on each cable or cord is accessible to its destination (such as the data cable reaching the HMC and the power cord from the power supply reaching the PDB).

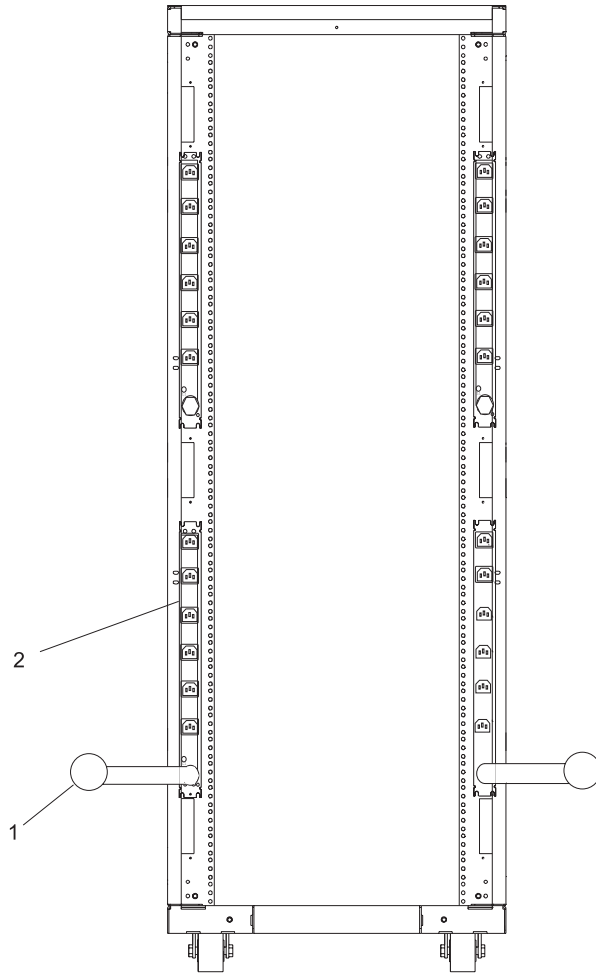
12. Attach one strip of double-sided adhesive tape to the bottom of the power supply.

Note: The bottom of the power supply is the clear surface located opposite the side with the label attached.

13. Position the power supply at the mounting location on the inside of the rack side panel, and press it firmly to adhere the power supply to the rack.
14. Attach a strip of hook-and-loop cable ties to the back vertical rail of the rack. Do not connect the power during the following step.
15. Route the power cord from the power supply to the PDB located at the back of the rack.

Complete the installation:

1. Connect the power cord from the modem to the PDB **2** located inside and at the back of the rack. The main power source plug on the rack is indicated by **1**. See the following illustration for the location of the PDB.



IPHA1521-0

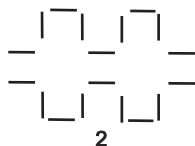
2. Connect the modem to an HMC:

- If you are connecting the modem to an HMC installed in a rack, plug the RS232 cable into the serial port located below the following symbol:



IPHA1522-0

- If you are connecting the RS232 data cable to a stand-alone HMC, plug the cable into serial port 2 (S2). Serial port 2 is the 9-Pin D-Shell socket noted by either of the following symbols:



IPHA1523-0

3. If you are connecting the RS232 data cable to equipment other than an HMC, follow the equipment manufacturer's instructions for connecting the cables.
4. Close the front and back doors of the rack.
5. Continue with step 4b on page 27.

Identifying the Ethernet port defined as eth0

Your Ethernet connection to the managed server must be made using the Ethernet port that is defined as eth0 on your HMC.

If you have not installed any additional Ethernet adapters in the PCI slots on your HMC, the primary integrated Ethernet port is always defined as eth0.

If you have installed additional Ethernet adapters in the PCI slots, the port that is defined as eth0 depends on the location and type of Ethernet adapters you have installed:

Table 3. HMC types and associated rules for Ethernet placement

HMC type	Rules for Ethernet placement
Rack-mounted	<p>The HMC supports only one additional Ethernet adapter.</p> <ul style="list-style-type: none"> If an additional Ethernet adapter is installed, that port is defined as eth0. In this case, the primary integrated Ethernet port is then defined as eth1, and the secondary integrated Ethernet port is defined as eth2. If no adapters are installed, the primary integrated Ethernet port is defined as eth0.
Stand-alone model 7310-C04	<p>The definitions depend upon the type of Ethernet adapter you have installed:</p> <ul style="list-style-type: none"> If only one Ethernet adapter is installed, whether it is a 1 Gigabit Ethernet adapter or a 10/100 Ethernet adapter, that adapter is defined as eth0. If both a 10/100 Ethernet adapter and a 1 Gigabit Ethernet adapter are installed, the 1 gigabit adapter is always defined as eth0. If two 10/100 Ethernet adapters are installed, the adapter in slot 1 is defined as eth0. If two 1 Gigabit Ethernet adapters are installed, the adapter in slot 1 is defined as eth0.

Table 3. HMC types and associated rules for Ethernet placement (continued)

HMC type	Rules for Ethernet placement
Stand-alone model 7310-C03	<p>The definitions are dependent upon the type of Ethernet adapter you have installed:</p> <ul style="list-style-type: none"> • The 1 Gigabit Ethernet adapter, when present, is generally defined as the eth0 location. The exception to this rule is when it is placed in slot 1 (the rightmost PCI slot when viewing the HMC from the back); however, this placement is not recommended. • If multiple 1 Gigabit Ethernet adapters are installed, the configuration is defined in the following order: slot 2 is eth0, slot 3 is eth1, and the integrated Ethernet port is eth2. • If adapters other than the 1 Gigabit Ethernet adapter are installed, the integrated Ethernet port is always defined as eth0.

Gathering information for configuration settings

Use the table provided in this topic to gather required configuration settings that you need to know before you begin the configuration steps.

To successfully configure the HMC, you must understand related concepts, make decisions, and prepare information. Use the following table to identify and gather the information you will need when you configure the HMC.

When you have completed this preparation step, go to “Configuring the HMC” on page 48.

This topic describes planning information for how you want to connect your HMC to your server, to your company network, and to your service provider. Review the related information in the following table to learn more about the decisions you need to make. You might choose to print this page to write down your decisions, requirements, and settings for easy access during the configuration steps.

This information contains references to tasks that are not included in this PDF. You can access the IBM Systems Hardware Information Center on the HMC or on the Web. On the HMC, the information center is in the **Information Center and Setup Wizard** folder. On the Web, the information center is at <http://www.ibm.com/server/library/infocenter>. Select your geographical location, your language preference, and hardware.

Table 4. Preparing for configuration

Preparation task	Where to find related information
If this is a second (redundant) HMC, ensure that the HMC code level of this HMC matches the one you already have.	<p>Determining your HMC machine code version and release</p> <p>Getting HMC machine code fixes and upgrades</p>
<p>Optional: If you plan to create additional users, identify the following information:</p> <ul style="list-style-type: none"> • How many user IDs you want to create • The user ID and password for each additional user you plan to create • What role you plan to assign each user 	Overview of roles

Table 4. Preparing for configuration (continued)


Preparation task	Where to find related information
<p>Determine whether you want to specify the media speed for each Ethernet adapter or let the HMC automatically detect the speed.</p> <p>For initial setup, use automatic detection. However, in some situations, you might want to reduce the speed of the adapter. If you plan to specify the media speed for each Ethernet adapter, identify the media speed and duplex mode for each Ethernet adapter. For example, 100 Mbps full duplex.</p>	
<p>Prepare the following contact information:</p> <ul style="list-style-type: none"> • Company name • Administrator's name • E-mail address • Telephone numbers • Fax numbers • Street address and telephone number for the location of the HMC 	
<p>Determine what type of connection you want to configure to contact your service provider:</p> <ul style="list-style-type: none"> • Dial-up from the local HMC: Determine what telephone numbers you will use to call IBM. • Virtual private network (VPN) through the Internet • Connecting through other systems or partitions: Determine the IP addresses or host names of the systems or logical partitions that the HMC passes through when connecting to your service provider. 	Choosing your connection method to your service provider
<p>Determine whether to register for IBM Electronic Service Agent™. If you decide to register, complete the following tasks:</p> <ol style="list-style-type: none"> 1. Go to My IBM Profile , click Register, and follow the registration instructions. 2. If you plan to authorize users to the Electronic Service Agent information, record your two IBM registered IDs. 	Electronic Service Agent
<p>Identify the Simple Mail Transfer Protocol (SMTP) server and e-mail addresses that will receive notification when problem events occur on the system.</p>	
<p>Determine the following passwords needed to access the managed system. These will be used later when the managed system is powered on.</p> <ul style="list-style-type: none"> • Determine the password you want to use to allow the HMC to access the managed system. • Determine the password you want to assign the Advanced System Management Interface (ASMI) general user ID. • Determine the password you want to assign to the ASMI administrator user ID. 	Overview of the managed system passwords
<p>To add managed systems, identify what systems you plan to add and refer to Figures 3, 4, and 5 to determine how they fit into your network.</p>	
<p>Determine whether you plan to connect the HMC to a private or open network.</p> <p>A private service network provides greater security and is easier to set up. A private service network allows the HMC to automatically detect the managed system. Therefore, it is recommended that you connect the HMC to a private service network.</p> <p>Note: If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network.</p>	"Private and open networks in the HMC environment" on page 12

Table 4. Preparing for configuration (continued)

Preparation task	Where to find related information																				
<p>To connect the HMC to a private service network, complete the following preparation tasks:</p> <ol style="list-style-type: none"> 1. Determine the HMC host name and domain name. Optionally, you can also enter a phrase in the description field. These settings are used to identify your HMC. Note: This step is necessary only if you plan to connect the HMC to an open network after connecting the HMC to a private service network. 2. Determine whether to configure the HMC as the Dynamic Host Configuration Protocol (DHCP) server. If this is the first or only HMC in your private service network, you must configure the HMC as a DHCP server (see Figure 12 on page 46). If this is an additional local HMC on the private service network, configure it as a DHCP client (see Figure 13 on page 47). 3. Select one of the following standard nonroutable IP address ranges for your private service network: <table> <tr> <td>192.168.0.2 – 192.168.255.254</td><td>10.128.0.2 – 10.128.15.254</td></tr> <tr> <td>172.16.0.3 – 172.16.255.254</td><td>10.128.128.2 – 10.128.128.254</td></tr> <tr> <td>172.17.0.3 – 172.17.255.254</td><td>10.128.240.2 – 10.128.255.254</td></tr> <tr> <td>10.0.0.2 – 10.0.0.254</td><td>10.254.0.2 – 10.254.0.254</td></tr> <tr> <td>10.0.128.2 – 10.0.143.254</td><td>10.254.240.2 – 10.254.255.254</td></tr> <tr> <td>10.0.255.2 – 10.0.255.254</td><td>10.255.0.2 – 10.255.0.254</td></tr> <tr> <td>10.1.0.2 – 10.1.15.254</td><td>10.255.128.2 – 10.255.143.254</td></tr> <tr> <td>10.1.255.2 – 10.1.255.254</td><td>10.255.255.2 – 10.255.255.254</td></tr> <tr> <td>10.127.0.2 – 10.127.15.254</td><td>9.6.24.2 – 9.6.24.254</td></tr> <tr> <td>10.127.255.2 – 10.127.255.254</td><td>9.6.25.2 – 9.6.25.254</td></tr> </table> Note: If you decide to connect your private service network to an open network in the future, using standard nonroutable IP addresses now will allow your DHCP servers to co-exist on the open network. 4. If you plan to configure the HMC as a DHCP client, an IP address is generated by the HMC already in the private service network (see Figure 13 on page 47). If you choose to use static IP addresses, select an address that is within the range used by the other systems in the network. 	192.168.0.2 – 192.168.255.254	10.128.0.2 – 10.128.15.254	172.16.0.3 – 172.16.255.254	10.128.128.2 – 10.128.128.254	172.17.0.3 – 172.17.255.254	10.128.240.2 – 10.128.255.254	10.0.0.2 – 10.0.0.254	10.254.0.2 – 10.254.0.254	10.0.128.2 – 10.0.143.254	10.254.240.2 – 10.254.255.254	10.0.255.2 – 10.0.255.254	10.255.0.2 – 10.255.0.254	10.1.0.2 – 10.1.15.254	10.255.128.2 – 10.255.143.254	10.1.255.2 – 10.1.255.254	10.255.255.2 – 10.255.255.254	10.127.0.2 – 10.127.15.254	9.6.24.2 – 9.6.24.254	10.127.255.2 – 10.127.255.254	9.6.25.2 – 9.6.25.254	<p>“HMC as a DHCP server” on page 16</p>
192.168.0.2 – 192.168.255.254	10.128.0.2 – 10.128.15.254																				
172.16.0.3 – 172.16.255.254	10.128.128.2 – 10.128.128.254																				
172.17.0.3 – 172.17.255.254	10.128.240.2 – 10.128.255.254																				
10.0.0.2 – 10.0.0.254	10.254.0.2 – 10.254.0.254																				
10.0.128.2 – 10.0.143.254	10.254.240.2 – 10.254.255.254																				
10.0.255.2 – 10.0.255.254	10.255.0.2 – 10.255.0.254																				
10.1.0.2 – 10.1.15.254	10.255.128.2 – 10.255.143.254																				
10.1.255.2 – 10.1.255.254	10.255.255.2 – 10.255.255.254																				
10.127.0.2 – 10.127.15.254	9.6.24.2 – 9.6.24.254																				
10.127.255.2 – 10.127.255.254	9.6.25.2 – 9.6.25.254																				
<p>To configure an open network, first configure a private service network, and then connect a different adapter on the HMC to your company network. If you plan to connect the HMC to an open network, complete the following preparation tasks:</p> <ol style="list-style-type: none"> 1. Complete the preparation tasks for configuring a private service network, and then continue with the following steps. 2. Complete the following preparation tasks to connect your private service network to an open network: <ol style="list-style-type: none"> a. If you plan to enable Domain Name System (DNS), complete the following tasks: <ol style="list-style-type: none"> 1) Identify the DNS server IP addresses. 2) Determine the order in which the addresses will be searched. 3) Determine the order in which the domain suffixes will be searched. b. Select the adapter to use as the default gateway for the open network. c. Identify the gateway address. d. If you plan to control the HMC remotely or give remote access to others, you must change the firewall settings to the HMC. Identify the applications or IP addresses you want to allow through the HMC’s firewall (see Figure 14 on page 48). 																					

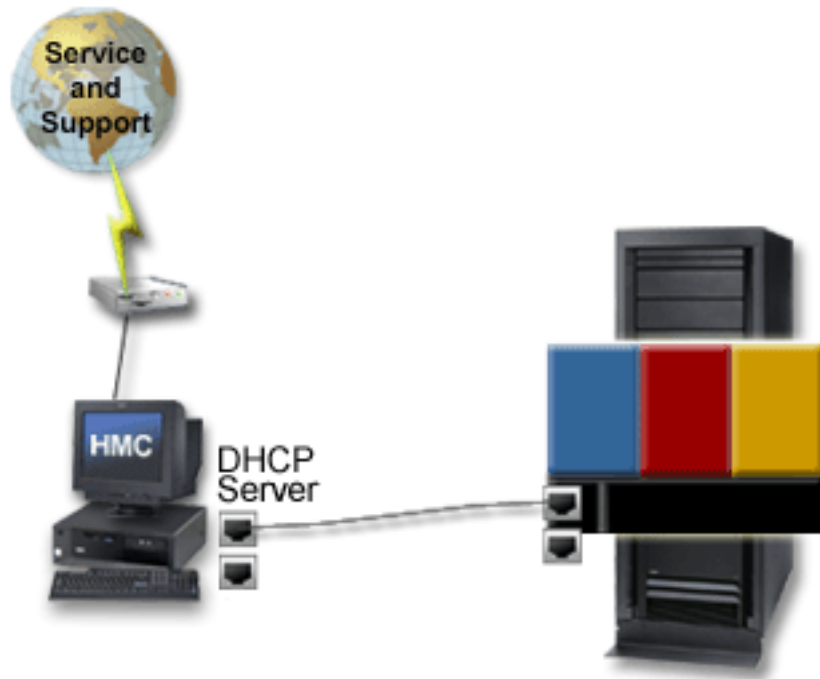


Figure 12. Private service network: Example 1

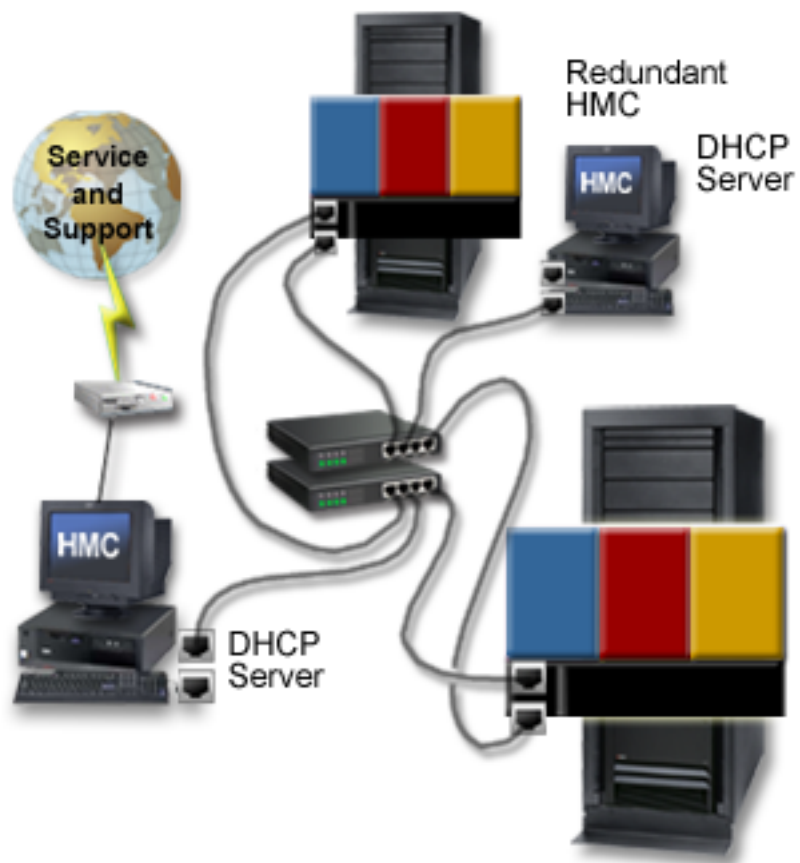


Figure 13. Private service network: Example 2

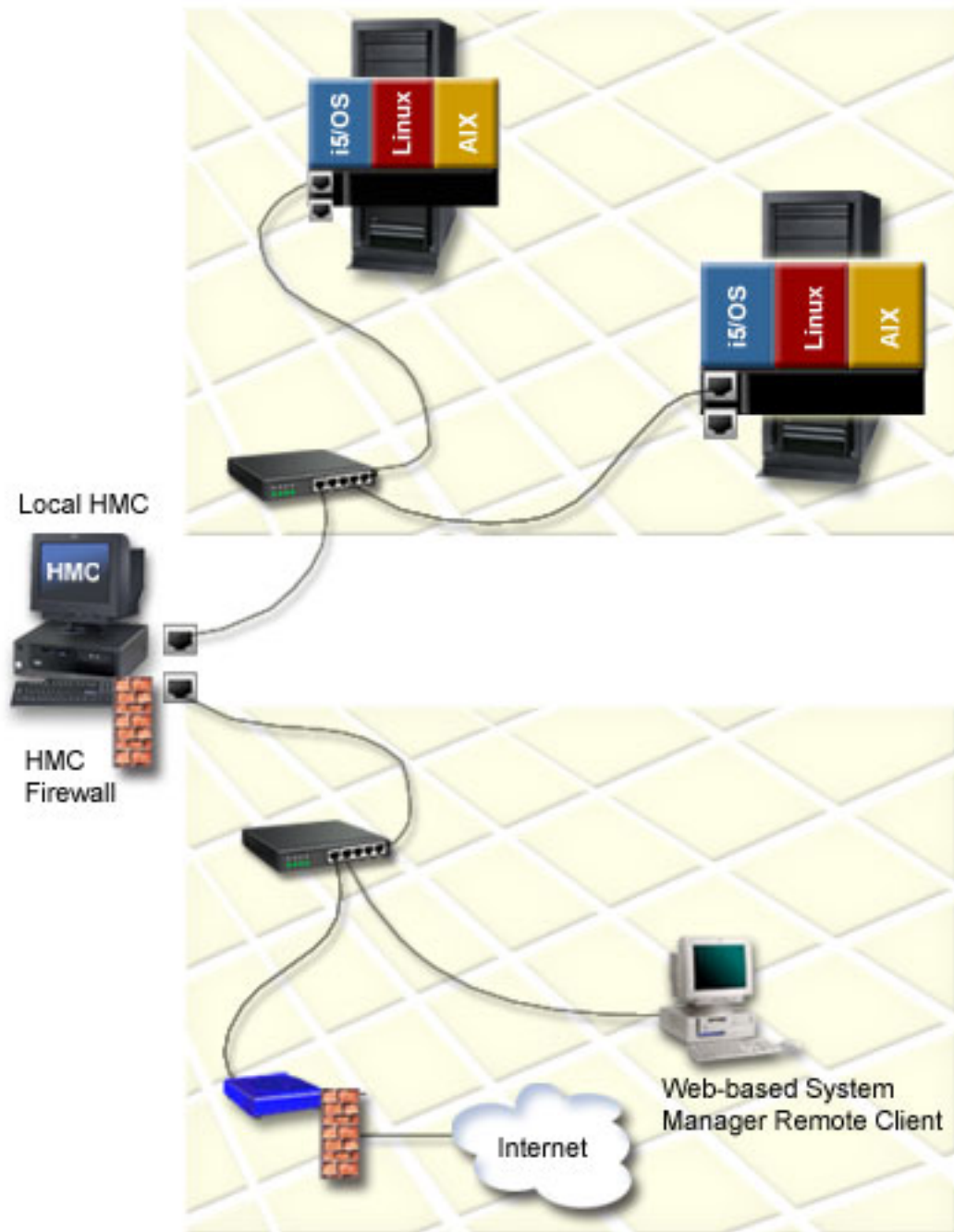


Figure 14. Open network

Configuring the HMC

Configure network connections, security, service applications, and some user preferences.

Depending on the level of customization you intend to apply to your HMC configuration, you have several options for setting up your HMC to suit your needs. The Guided Setup wizard is a tool on the HMC designed to make the setup of the HMC quick and easy. You can choose a fast path through the wizard to quickly create the recommended HMC environment, or you can choose to fully explore the

available settings that the wizard guides you through. You can also perform the configuration steps without the aid of the wizard using the HMC configuration checklist.

Before you start, gather the required configuration information that you will need to complete the steps successfully. See “Gathering information for configuration settings” on page 43 for a list of the required information.

Configuring the HMC using the fast path through the Guided Setup wizard

In most cases, the HMC can be set up to operate effectively using many of the default settings. Use this fast path checklist to prepare the HMC for service quickly and efficiently. When you have completed the steps in this checklist, your HMC will be configured as a Dynamic Host Configuration Protocol (DHCP) server in a private (directly connected) network.

The Guided Setup wizard guides you through a wide range of configuration options that you might need to consider when you set up your HMC. Often, however, the HMC can be set up to operate effectively using many of the default settings. Use this checklist to prepare the HMC for service. When you have completed the steps in this checklist, your HMC will be configured as a Dynamic Host Configuration Protocol (DHCP) server in a private (directly connected) network.

Prerequisites:

To complete the Guided Setup wizard using the fast path, you need to have the following information available:

- New passwords for the predefined **hscroot** and **root** user IDs. These passwords must be at least 7 characters in length.
- Details about your company:
 - Administrator name
 - Telephone and fax numbers
- Details about the geographic location of your HMC
- Optional: Your IBM ID for the Electronic Service Agent. To obtain this ID, you must register at the following Web site: <https://www.ibm.com/registration/selfreg>
- Optional: SMTP server and e-mail addresses for problem notification.
- New passwords for the managed system, the Advanced System Management general user ID, and the Advanced System Management administrator user ID.

Start the fast path through the Guided Setup Wizard:

To use the fast path to configure your HMC, follow these steps:

Starting the HMC and passwords:

1. Ensure that the managed system is not connected to a power source. For rack-mounted HMCs, this means that the only device plugged into the power distribution bus (PDB) before you plug in the main power supply is the HMC. (See the “Cabling the HMC” on page 22 topic if you are not sure.)
2. Turn on the HMC by pressing the power button.
3. Wait for the HMC to automatically select the default language and locale preference after 30 seconds.
4. Log in to the HMC:
 - ID: **hscroot**
 - Password: **abc123**
5. To continue, accept the Hardware Management Console license agreements. If you decline the Hardware Management Console license agreements, you cannot complete the HMC configuration.
6. Click **OK** on the Guided Setup entry window.
7. Click **Next** on the Welcome window.

8. Verify and change, if necessary, the time, date, and time zone settings. Click **Next**.
9. Change the **hscroot** password:
 - a. Enter the new password twice. The password must be at least 7 characters in length.
 - b. Click **Next**.
10. Change the **root** password:
 - a. Enter the new password twice. The password must be at least 7 characters in length.
 - b. Click **Next**.
 - c. Click **Next** again.
11. Click **Next** on the Next Steps summary window.

Configuring network settings:

1. On the second Configure Network Settings window, select the LAN adapter labeled **eth0**. Click **Next**.
2. On the LAN adapter speed window, click **Next**.
3. On the Configure (LAN adapter name) window, click **Next**.
4. On the second Configure (LAN adapter name) window, select **private service network**. Click **Next**.
5. On the third Configure (LAN adapter name) window, select **Yes, enable the HMC as a DHCP server**. Click **Next**.
6. On the Configure Network Settings window, select **No**. (You can configure any remaining LAN adapters later.) Click **Next**.
7. Click **Next** on the Next Steps summary window.

Configuring connectivity to your service provider:

1. On the Specify Contact Information window, type the contact information for the administrator of your HMC. Click **Next**.
2. On the Specify Contact Information window, type the contact address information for the location of your HMC. Click **Next**.
3. On the Specify Contact Information window, select the **Use the administrator mailing address** box, or clear it to enter a different address for the HMC, as required. Click **Next**.
4. On the Configure Connectivity to Your Service Provider window, click **Next**.
5. Click **Accept** on the Agreement for Service Programs window.
6. On the Configure Dial-up from the Local HMC window:
 - a. Click **Modem Configuration**. To make an off-site telephone call at your company, type the number in the **Dial prefix** field. Click **OK**.
 - b. To add a telephone number to your service provider, click **Add**.
 - 1) Select the appropriate country or region.
 - 2) Select the appropriate state or province.
 - 3) Select the appropriate telephone number from the list.
 - 4) In the **Phone number** field, edit the selected telephone number, if necessary. For instance, if the selected telephone number is a local call from your site, you might need to remove the area code.
 - 5) Click **OK**.
 - c. Click **Next**.
7. On the Authorize Users for Electronic Service Agent window, enter your IBM IDs (skip this step if you do not have an IBM ID). Click **Next**.
8. On the Notification of Problem Events window, specify the SMTP server and port. Click **Add** to specify one or more e-mail addresses for notification of problem events. Click **Next**.
9. On the Summary window, click **Finish**.

Monitoring your configuration:

1. On the Status window, monitor the progress of the different configuration settings you selected. This window might show a status of Pending for some tasks for several minutes. Click **View Log** to see status messages relating to each task. Click **OK** on the status message window to close it. Click **Close** at any time to close the Guided Setup wizard. Tasks that are still running will continue to run.

Complete the configuration steps listed under **After you have completed the Guided Setup wizard** in the “Configuring the HMC using the Guided Setup wizard” topic.

Configuring the HMC using the Guided Setup wizard

The Guided Setup wizard guides you through numerous configuration settings that you might choose to use in your environment.

To perform a customized configuration of your HMC, use these instructions.

Note: Use the fast path through the Guided Setup wizard to complete configuration of your HMC quickly and easily with minimal customization. See “Configuring the HMC using the fast path through the Guided Setup wizard” on page 49 for instructions.

Prerequisites:

Complete the configuration preparation activity described in the “Gathering information for configuration settings” on page 43 topic.

Run the Guided Setup Wizard:

Use the following instructions to configure your HMC using the Guided Setup wizard.

Note: If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network using the eth0 Ethernet connection.

1. Ensure that the managed system is not connected to a power source.
2. Start the Guided Setup wizard:
 - a. Turn on the HMC by pressing the power button.
 - b. If English is your language preference, continue with step 2e.
 - c. If your language preference is a language other than English, type the number **2** when you are prompted to change the locale.

Note:

- 1) This prompt times out in 30 seconds if you do not act.
- 2) If your numeric keypad does not work, use the numeric keys instead.
- d. Select the locale you want to display from the list in the Locale Selection window, and click **OK**. The locale identifies the language that the HMC interface displays.
- e. Log in to the HMC using the following default user ID and password:
ID: hscroot
Password: abc123
You will be prompted later to provide a new 7-character password for this ID.
- f. To continue, accept the Hardware Management Console license agreements. If you decline the license agreement, you cannot complete the HMC configuration.
- g. When the Guided Setup wizard is displayed, complete the wizard to configure the HMC. If the Guided Setup wizard is not displayed, you can access it manually from the HMC interface. See “Accessing the Guided Setup wizard using the HMC interface” on page 53.

After you have completed the Guided Setup Wizard:

1. After you have completed the Guided Setup wizard, complete the following tasks:
 - a. Connect the managed system to a power source. The managed system will then power on its service processor. After the service processor is powered on, proceed to the next step. This process will take 3 to 5 minutes. The following sequence of events signals that power has been applied to the service processor (with the exception of the model 9118-575 server and the 590 and 595 servers):
 - 1) Progress indicators, also referred to as checkpoints, appear on the control panel display while the system is being started. The display might appear blank for a few moments during this sequence.
 - 2) When the service processor has completed its power-on sequence, the green power-on light blinks slowly and the output on the control panel is similar to the following:


```
01    N    V=F
                T
```
 - b. Click **Server and Partitions > Server management** to view the status of your managed system. (For the model 9118-575 server and the 590 and 595 servers, also click **Server and Partitions > Frame management** to view the status of the frame.) It may take a few minutes for the status to display.
 - c. If the status shows Pending Authentication, then go to step 1d. If you receive the message Authentication Failed, or if you do not receive a message, see “Troubleshooting HMC setup” on page 86.

Note: If you did not configure your HMC as a Dynamic Host Configuration Protocol (DHCP) server, the HMC will not automatically detect the managed system. To detect the managed system, see Add another managed system and enter the IP address that you assigned to the managed server when it is requested.

 - d. Set passwords for the managed system. (For the model 9118-575 server and the 590 and 595 servers, set passwords for the managed system and the frame.) Did you receive the message Pending Authentication?
 - **Yes:** The HMC will prompt you to set the passwords for the managed system. If you are not prompted by the HMC to set these passwords after several minutes, right-click the server entry on the console. The window for setting passwords opens. Set the password for each as directed.
 - **No:** Set the managed system passwords using the HMC interface:
 - 1) Set the managed system password. For instructions, see **Update your platform password** in the HMC online help. You can find this topic in the online help index under **Update** and **Platform password**.
 - 2) Set the password for the Advanced System Management general user ID. For instructions, see **Update your Advanced System Management (ASM) general password** in the HMC online help.
 - 3) Set the password for the Advanced System Management administration user ID. For instructions, see **Update your Advanced System Management (ASM) administrator password** in the HMC online help.
 - e. Access the ASMI to set the time of day on the system:
 - 1) Access the ASMI using the HMC.
 - 2) Set the time of day on the system.
 - f. Start the managed system
 - g. Ensure that you have one logical partition on the managed system. For instructions, see Creating logical partitions from the manufacturing default configuration.
 - h. Optional: Add another managed system
2. When you are finished configuring the HMC, complete the setup steps that apply to your situation:
 - If you are installing a new server with your HMC, return to your initial server setup checklist and configure logical partitions or install one or more operating systems.

- If you are not installing a new server at this time, complete the optional tasks described in “Postconfiguration steps for the HMC” on page 60 to further customize your configuration.

Accessing the Guided Setup wizard using the HMC interface:

If the Guided Setup wizard did not display when you started the HMC for the first time, complete the following steps to access the Guided Setup wizard using the HMC interface:

1. In the navigation area, expand the HMC you want to work with. HMCs are listed by host name or IP address.
2. Click **Information Center and Setup Wizard**.
3. In the contents pane, click **Launch the Guided Setup wizard**.

Configuring the HMC using the HMC configuration checklist

The HMC configuration checklist provides a complete list of all HMC configuration tasks, guiding you through the process of successfully configuring your HMC. Choose this option if you prefer not to use the Guided Setup wizard.

Complete the following checklist to successfully set up your HMC. You will have to restart your HMC for the configuration settings to take effect, so you might want to print this checklist and keep it with you as you configure your HMC. The first section of the checklist, called HMC configuration checklist, contains all the tasks necessary to set up your HMC. The last step directs you to a topic that contains optional setup tasks to further configure your system.

This information contains references to tasks that are not included in this PDF. You can access the IBM Systems Hardware Information Center on the HMC or on the Web. On the HMC, the information center is in the **Information Center and Setup Wizard** folder. On the Web, the information center is at <http://www.ibm.com/server/library/infocenter>. Select a continent, your language preference, and hardware.

Prerequisites

Before you begin this checklist, be sure to complete the configuration preparation activity described in “Gathering information for configuration settings” on page 43.

HMC configuration checklist

- Start the HMC.
- If you have not yet done so, get HMC fixes to ensure that your HMC has the latest updates. Return to this checklist when you have completed this step.
- Set the date and time.
- Change predefined passwords.
- Optional: Create additional users and return to this checklist when you have completed this step.
- Configure network connections:
 - To configure LAN adapters, follow these steps (perform each task for each LAN adapter).

Note: If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network using the eth0 Ethernet connection.

 - Set the media speed.
 - Select the network type.
 - Unless the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, configure the HMC as a Dynamic Host Configuration Protocol (DHCP) server.
 - If the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, set the IP address.
 - If you selected the open network, change HMC firewall settings.
 - If you are using an open network and a fixed IP address, set identification information.
 - If you are using an open network and a fixed IP address, configure a routing entry as the default gateway.
 - If are using an open network and a fixed IP address, configure domain name services.

HMC configuration checklist

- If are using a fixed IP address and have DNS enabled, configure domain suffixes.
- Test the connection from the HMC to the managed system.
- Set up your server to connect to service and support and return to this checklist when you have completed this step.
- Connect the managed system to a power source. If you receive the message Authentication Pending, continue with the next step in this checklist.

If you receive the message Authentication Failed, or you do not receive a message, see “Troubleshooting HMC setup” on page 86.

- Set passwords for the managed system:
 - If you received the message Authentication Pending, the HMC will prompt you to set the passwords for the managed system.
 - If you did not receive the message Authentication Pending, complete the following steps to set the passwords for the managed system. (For the model 9118-575 server and the 590 and 595 servers, set passwords for the managed system and the frame.)
 - Set the managed system password. For instructions, see **Update your platform password** in the HMC online help.
 - Set the password for the Advanced System Management general user ID. For instructions, see **Update your Advanced System Management (ASM) general password** in the HMC online help.
 - Set the password for the Advanced System Management administration user ID. For instructions, see **Update your Advanced System Management (ASM) administrator password** in the HMC online help.
- Access the ASMI to set the time of day on the system:
 - Access the ASMI using the HMC.
 - Set the time of day on the system.
- Start the managed system and return to this checklist when you have completed this step.
- Ensure that you have one logical partition on the managed system. For instructions, see Creating logical partitions from the manufacturing default configuration.
- Optional: Add another managed system and return to this checklist when you have completed this step.
- If you are installing a new server with your HMC, return to your initial server setup checklist and configure logical partitions or install one or more operating systems.
- If you are not installing a new server at this time, complete the optional tasks described in “Postconfiguration steps for the HMC” on page 60 to further customize your configuration.

Changing the predefined passwords for hscroot and root user IDs:

Learn how to change your predefined passwords.

It is essential to your system’s security that you change all predefined passwords immediately. For more information about changing the predefined passwords for hscroot and root user IDs, do the following:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by host name or IP address.
2. Expand **HMC Management**.
3. Click **HMC Users**.
4. In the contents pane, click **Manage HMC users, roles, and access**.
5. Click the **User** icon.
6. Right-click the **hscroot** icon to change the hscroot password or the **root** icon to change the root password.
7. Select **Change Password**.
8. Type the new password in the first field. The password must be a minimum of 7 characters in length.
9. Confirm the new password by typing it again in the **Retype new password** field.

Configuring network connections:

Configure network connections to allow the HMC to talk to managed systems or logical partitions. Set the identification information, configure domain name services, and configure the LAN adapters.

Note: If you are using both a virtual Ethernet and network address translation (NAT) in your network setup, the partition and the HMC might experience communications problems.

To configure LAN adapters, complete the following tasks for each LAN adapter:

1. "Setting the media speed."
2. "Selecting the network type."
3. Unless the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, see "Configuring the HMC as a DHCP server" on page 56.
4. If you have configured your HMC as a DHCP server, see "Verifying that your HMC DHCP private network is configured correctly" on page 57.
5. If the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, see "Setting the IP address" on page 58.
6. If you selected the open network, see "Configuring a routing entry as the default gateway" on page 59.
7. If you selected the open network, see "Changing HMC firewall settings" on page 58.

Configuring LAN adapters:

Understand how to configure your LAN adapters.

To configure LAN adapters, complete the following tasks for each LAN adapter:

1. Set the media speed.
2. Select the network type.
3. Unless the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, see Configuring the HMC as a DHCP server.
4. If the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, see Setting the IP address.
5. If you selected the open network, see Configuring a routing entry as the default gateway.
6. If you selected the open network, see Changing HMC firewall settings.

Setting the media speed:

Specify the media speed and duplex mode of the Ethernet adapter:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **LAN Adapters** tab.
6. Select the LAN adapter you want to work with and click **Details**.
7. Click the **Lan Adapter** tab.
8. In the Local area network information section, select the media speed.
9. Click **OK**.

Selecting the network type:

You can connect your HMC to a private or open network.

A *private service network* consists of the HMC and the managed systems. A private service network is restricted to consoles and the systems they manage, and is separate from your company network. An *open network* consists of your private service network and your company network. An open network might contain network endpoints in addition to consoles and managed systems, and might span across multiple subnets and network devices.

To select the network type, complete the following steps:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **LAN Adapters** tab.
6. Select the LAN adapter that you want to work with and click **Details**.
7. Click the **Lan Adapter** tab.
8. In the Local area network information page, select **Private** or **Open**.
9. Click **OK**.

Configuring the HMC as a DHCP server:

Dynamic Host Configuration Protocol (DHCP) provides an automated method for dynamic client configuration.

Clients that are DHCP enabled automatically obtain their own IP address and configuration parameters from the server. In a private service network, configure your first or only HMC as a DHCP server. The HMC then provides nonroutable IP addresses to its managed systems. This allows the HMC to co-exist with other DHCP servers in your company network when you connect your private service network to an open network. For more information, see “HMC as a DHCP server” on page 16.

Note: If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network using the eth0 Ethernet connection.

To configure the HMC as a DHCP server, complete the following steps:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **LAN Adapters** tab.
6. Select the LAN adapter that you want to work with and click **Details**.
7. Click the **Lan Adapter** tab.
8. In the DHCP Server section, check **Enable DHCP Server** to enable the HMC as a DHCP server.
9. Enter the address range of the DHCP server.
10. Click **OK**.

If you configured your HMC to be a DHCP server on a private network, you must verify that your HMC DHCP private network is configured correctly. For information about connecting your HMC to a private network, see “Selecting the network type” on page 55. To verify that your HMC DHCP private network is configured correctly, see “Verifying that your HMC DHCP private network is configured correctly” on page 57.

Verifying that your HMC DHCP private network is configured correctly:

This section applies to all DHCP-managed managed systems. Read this article to learn how to verify that your HMC DHCP private network is configured correctly.

The following systems require that the HMC is configured as a DHCP server on a private network:

- IBM System p5™ 575
- IBM eServer p590
- IBM eServer p595
- IBM eServer i595

If your HMC is configured as a DHCP server on a private network and is not communicating correctly with the managed system, or you have recently modified your network configuration (moved a managed system, replaced an HMC, or added a second HMC), use the following instructions to determine if your DHCP-managed private network is configured correctly.

Note: If your HMC is set up as a DHCP server on a private network, do not use the static IP commands `mksysconn` and `rmsysconn` to change HMC connection settings. These commands are intended for use on a public network only, where the HMC is not set up as DHCP server and managed servers use static IP addresses.

If a system administrator previously assigned an IP address to the system through a manually executed static IP command, Support must remove the manual connection and establish a DHCP connection between the HMC and the server. This section describes how to identify any manually assigned IP addresses so that an authorized service provider can remove them.

To identify a manually assigned IP address so that your HMC can communicate correctly with your managed systems, you must perform the following high-level tasks. Detailed step-by-step task descriptions of how to perform these tasks are specified below.

1. Identify the configured HMC IP connection addresses and compare them to the list of IP addresses assigned by the DHCP server.
2. Identify the HMC IP connection addresses that have been correctly assigned through the DHCP server, for which no further action is required.
3. Identify any manually configured HMC IP connection addresses that DHCP did not assign and that need to be corrected by support.

To identify manually assigned IP addresses when the HMC is configured as a DHCP server, do the following

1. Create a list of all of the configured HMC IP connections. On the HMC command line, type the following command:

```
lssysconn -r all
```

This command displays the following information for service processors and Bulk Power Cards (BPCs) on the network for which the HMC has configured IP connection:

element type, MTMS, IP address(es), connection state

2. Make a note of all IP addresses that are displayed. You will need these addresses later.
3. Display a list of the DHCP IP addresses that have been assigned. To do this, type the following HMC command:

```
lshmc -n -F clients
```

The output of this command lists all IP addresses that have been assigned by the HMC's DHCP server.

4. Make a note of all IP addresses that are listed in the output.

5. Compare the `lssysconn` and `lshmc` lists. If an IP address is displayed in the output for both the `lshmc -n -F` clients and `lssysconn -r` all commands, the IP address was assigned by the HMC DHCP server and the connection is being managed by the HMC DHCP server.
6. Remove from the list any address that is displayed in the output of the `lshmc -n -F` clients command but not displayed in the output of the `lssysconn -r` all command, and is not in the list of servers that use static IP addresses.

Note: If an IP address is displayed in the `lshmc -n` output and not in the `lssysconn -r` all output, that IP address was assigned by the HMC DHCP server. However, it is not a current connection on the HMC. The DHCP server keeps a history of all IP address assignments in the event that the connection is re-established. The DHCP server might also have assigned an IP address if an unknown device on the private network requested a DHCP IP address from the HMC.

7. If the HMC is managing servers on both a private and a public network, any connections to the service processor on the public network (not in the private network address range) must also be identified and removed from this list. If there are no IP addresses remaining in the list that contains the `lssysconn -r` all output, the HMC DHCP server has assigned all of the system IP addresses, and the network configuration is working correctly.
8. If there are any IP addresses not removed from the list taken from the `lssysconn -r` all command, this address was not assigned by the HMC's DHCP server. These IP address assignments must be corrected, so that they can be automatically reassigned by the HMC DHCP server. Contact an authorized service provider and request that someone correct the manually assigned IP addresses that you have identified.

If you have followed this procedure and not all of your connections appear to be active (for example, two connections for each 590/595 system, one for each 575 system, and two for each frame), call an authorized service provider for additional support.

Setting the IP address:

To set your IP address, use the following steps:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **LAN Adapters** tab.
6. Select the LAN adapter that you want to work with and click **Details**.
7. Click the **Lan Adapter** tab.
8. Select **Obtain an IP address automatically** or **Specify an IP address**.
9. If you selected to specify an IP address, enter the TCP/IP interface address and the TCP/IP interface network mask.
10. Click **OK**.

Changing HMC firewall settings:

In an open network, a firewall usually controls outside access to your company network. The HMC also has a firewall on each of its Ethernet adapters. If you want to control the HMC remotely or give remote access to others, modify the firewall settings of the Ethernet adapter on the HMC that is connected to your open network.

To configure a firewall, use the following steps:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.

2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **LAN Adapters** tab.
6. Select the LAN adapter that you want to work with and click **Details**.
7. Click the **Firewall** tab.
8. Using one of the following methods, you can allow any IP address using a particular applications through the firewall, or you can specify one or more IP addresses:
 - Allow any IP address using a particular application through the firewall:
 - a. From the top box, highlight the application.
 - b. Click **Allow Incoming**. The application displays in the bottom box to signify that it has been selected.
 - Specify which IP addresses to allow through the firewall:
 - a. From the top box, highlight an application.
 - b. Click **Allow Incoming by IP Address**.
 - c. On the Hosts Allowed window, enter the IP address and the network mask.
 - d. Click **Add** and click **OK**.
9. Click **OK**.

Setting identification information:

Identification information includes the HMC's hostname, the domain name, and the HMC's description.

To identify your system to the network, complete the following steps:

1. In the navigation area, expand the HMC you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **Identification** tab.
6. In the **Console name** field, enter the HMC's hostname.
7. Enter the domain name.
8. In the **Computer description** field, enter the HMC's description.
9. Click **OK**.

Configuring a routing entry as the default gateway:

To configure a routing entry as the default gateway, use the following steps:

1. In the navigation area, expand the HMC you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **Routing** tab.
6. In the Default gateway information section:
 - a. Enter the gateway address of the routing entry you want to set as the default gateway.
 - b. Enter the gateway device of the routing entry you want to set as the default gateway.
7. Click **OK**.

Configuring domain name services:

If you plan to set up an open network, configure domain name services.

Domain Name System (DNS) is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Configuring domain name services includes enabling DNS and specifying the domain suffix search order.

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **Name Services** tab.
6. Check **DNS enabled** to enable DNS.
7. If you enabled DNS, specify the DNS server search order and the domain suffix search order.
8. Click **OK**.

Configuring domain suffixes:

The list of domain suffixes is used to resolve an IP address starting with the first entry in the list.

The domain suffix is a string appended to a hostname that is used to help resolve its IP address. For example, a hostname of myname might not be resolved. However, if the string myloc.mycompany.com is an element in the domain suffix table, then there will be an attempt to also resolve myname.mloc.mycompany.com.

To configure a domain suffix entry, use these steps:

1. Enter a string to be used as a domain suffix entry.
2. Click **Add** to add it to the list.

Testing the connection between the HMC and the managed system:

This option enables you to verify that you are properly connected to the network.

To test network connectivity, you must be a member of one of the following roles:

- super administrator
- service representative

To test network connectivity, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, click the **HMC Configuration** icon.
3. In the Contents area, click **Test Network Connectivity**.
4. Type the host name or IP address of any system to which you want to connect.
5. Click **OK**.

To understand how the HMC can be used in a network, see “HMC network connections” on page 11.

For more information about configuring the HMC to connect to a network, see “Configuring the HMC using the HMC configuration checklist” on page 53.

Postconfiguration steps for the HMC:

After you have installed and successfully configured the HMC, you can perform these optional tasks as necessary.

Optional: Postconfiguration tasks

- Back up the HMC.
- Configure logical partitions.
- Install the operating systems.
- Access the operating systems using the HMC.
- Configure Capacity on Demand.

Replacing an HMC

Learn about the tasks you must perform when replacing an HMC.

If you are replacing an HMC that is set up as a DHCP server, you must first reinstall the HMC code base by using one of the following:

- The recovery media that was provided with your HMC
- The recovery media that you last used to upgrade your HMC

You must also reinstall your customized HMC configuration data by using backup media.

Procedures for replacing an HMC differ, depending on which HMC version you have installed. To determine your HMC version, see [Determining your HMC machine code version and release](#) and then return here.

These instructions assume that you have created a backup of your HMC configuration data from the HMC being replaced. For more information about backing up important HMC data, see [Backing up critical HMC data](#). If you do not have a backup of the HMC, these procedures are the same as those described in “Setting up the HMC” on page 21.

For HMC V4.5 or earlier

1. Insert the HMC recovery media, then power on or reboot the HMC. The HMC powers on and loads from the media.
2. Press F8 to select **Install/Recovery**.
3. Press F1 to continue. After the installation is complete, the HMC prompts you to insert the backup media.
4. Insert the backup media. When you are finished, the HMC is restored to the state that it was in at the time that the backup was created.
5. After the HMC interface has been restored, verify that your HMC DHCP private network is configured correctly. For more information, see [Verifying that your HMC DHCP private network is configured correctly](#).

For HMC V5.0 or later

1. Insert the HMC recovery media, then power on or reboot the HMC. The HMC powers on from the media and displays the **Backup/Upgrade/Restore/Install** panel.
2. Select **Install** and click **Next**. Wait for the installation to complete.
3. Select **1 - Install additional software from media** from the menu displayed to install the second HMC recovery media.
4. Remove the recovery media and insert the second media.
5. Press Enter to start the installation of the second recovery media.
6. After the installation is complete, remove the second recovery media, insert the backup media, and select **1 - Restore Critical Console Data** from the menu to restore data from the backup media. When you are finished, the HMC is restored to the state that it was in at the time that the backup was created.

7. After the HMC interface has been restored, verify that your HMC DHCP private network is configured correctly. For more information, see *Verifying that your HMC DHCP private network is configured correctly*.

Installing and securing the remote client

Install the Web-based System Manager Remote Client or install the Web-based System Manager Remote Client for Java Web Start.

You can access your Hardware Management Console (HMC) remotely by installing the remote client on your PC. The remote client provides flexibility by allowing you to manage your system from virtually anywhere you have a PC. Up to five remote clients can be logged in simultaneously. There are some tasks you cannot perform using the remote client. These tasks include determining the level of HMC code, restarting the HMC interface, and configuring System Manager Security for certificate authority or viewing overview and status information. System Manager Security ensures that the HMC can operate securely in client/server mode. Servers and clients communicate over the Secure Sockets Layer (SSL) protocol, which provides server authentication, data encryption, and data integrity.

To set up the remote client and secure the HMCs in your network, perform the following procedures for Web-based System Manager Remote Client for Java Web Start or the Web-based System Manager.

Web-based System Manager Remote Client for Java Web Start

1. "Configuring one HMC as a certificate authority"
2. "Generating private key ring files for the servers" on page 63
3. "Installing private key ring files on the servers" on page 63
4. "Distributing the certificate authority's public key with Web-based System Manager Remote Client for Java Web Start" on page 64
5. "Viewing configuration properties" on page 65
6. "Configuring HMC object manager security" on page 66
7. "Installing the Web-based System Manager Remote Client for Java Web Start" on page 67
8. "Uninstalling the Web-based System Manager Remote Client for Java Web Start" on page 68

Web-based System Manager Remote Client

1. "Configuring one HMC as a certificate authority"
2. "Generating private key ring files for the servers" on page 63
3. "Installing private key ring files on the servers" on page 63
4. "Installing the Web-based System Manager Remote Client" on page 66
5. "Distributing the certificate authority's public key with Web-based System Manager Remote Client" on page 64
6. "Viewing configuration properties" on page 65
7. "Configuring HMC object manager security" on page 66
8. "Uninstalling the Web-based System Manager Remote Client" on page 67

To install Web-based System Manager on AIX®, see the *Web-based System Manager Administration Guide*.

Configuring one HMC as a certificate authority

This procedure defines a system as an internal certificate authority (CA) for HMC security and creates a public key ring file for the CA that you can distribute to all of the clients that access the servers.

1. Verify that you are using a local HMC and not the Web-based System Manager Remote Client.

2. Ensure that you are logged in as the hscroot user at the HMC that is being configured as the internal CA.
3. In the navigation area, expand the local HMC. It is the first HMC in the list.
4. Expand **System Manager Security**.
5. Click **Certificate Authority**.
6. In the System Manager Certificate Authority window, click **Configure this system as a System Manager Certificate Authority**. You can also select **Configure** from the Certificate Authority menu.
7. Use the online help to guide you through completing the task.

Note: Remember the password you set for the CA private key file. You will need this password when you generate private key ring files for the servers.

Generating private key ring files for the servers

Use the certificate authority (CA) to generate private key ring files for the servers. The private key ring file consists of the private key and the server certificate.

Note: If the system defined as a CA will also be used in server mode, you must complete the steps for generating and installing private key ring files on that system.

1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand **System Manager Security**.
3. Click **Certificate Authority**.
4. In the System Manager Certificate Authority window, click **Generate Servers' Private Key Ring Files**. You can also select **Generate Keys** from the Certificate Authority menu.
5. In the Password window, type the CA private key file password. This password was created when the HMC was configured as the CA.
6. Click **OK**.
7. In the Generate Server's Private Key Ring Files window, use the help information to guide you through completing the task.
8. Click **OK** when you are finished.

Installing private key ring files on the servers

Follow these steps to correctly install private key ring files.

1. Copy the server private key ring files to removable media:
 - a. In the navigation area, expand the local HMC. It is the first HMC in the list.
 - b. Expand **System Manager Security**.
 - c. Click **Certificate Authority**.
 - d. In the System Manager Certificate Authority window, click **Copy Servers' Private Key Ring Files to removable media**. You can also select **Copy Servers' Keys** from the Certificate Authority menu.
 - e. When the Copy Server's Private Key to removable media dialog displays, insert the media.
 - f. Click **OK** to copy the servers' private key ring files to removable media.
2. Install the private key ring file on each server. Repeat the following steps for each server for which you generated a private key ring file:
 - a. In the navigation area, expand the local HMC. It is the first HMC in the list.
 - b. Expand **System Manager Security**.
 - c. Click **Server Security**.
 - d. In the System Manager Server Security window, click **Install the private key ring file for this server**. You can also select **Install Key** from the Server menu.

- e. In the Install Private Key Ring File window, select **removable media** as the source for the server private key ring file. Insert the removable media containing the server's key into the removable media drive.
 - f. Click **OK**.
3. Configure the server as a secure System Manager server. Repeat the following steps for each server on which you installed a private key ring file:
 - a. In the navigation area, expand the local HMC. It is the first HMC in the list. HMCs are listed by hostname or IP address.
 - b. Expand **System Manager Security**.
 - c. Click **Server Security**.
 - d. In the System Manager Server Security window, click **Configure this system as a Secure System Manager server**. You can also select **Configure** from the Server menu.
 - e. Use the help to guide you through completing the task.

Distributing the certificate authority's public key with Web-based System Manager Remote Client for Java Web Start

If you are using the Web-based System Manager Remote Client for Java Web Start, use the following instructions to copy the certificate authority (CA) public key ring file (SMpubkr.zip) to each server that you will use to download the remote client.

If the system defined as a CA will also be used in server mode, you must complete the steps for distributing the CA's public key for that system. Although the CA public key was created on this system, it is not in the correct location for the system to be used as a server.

1. On the CA system, perform the following steps to copy the CA's public key to removable media:
 - a. In the navigation area, expand the local HMC. It is the first HMC in the list.
 - b. Expand **System Manager Security**.
 - c. Click **Certificate Authority**.
 - d. In the System Manager Certificate Authority window, click **Copy this Certificate Authority's Public Key Ring File to removable media**. You can also select **Copy out CA Public Key** from the Certificate Authority menu.
 - e. When the Copy CA Public Key to Removable Media window opens, insert a diskette.
 - f. Select **HMC or AIX client** to write the file to a tar diskette.
 - g. Click **OK** to copy the public key ring file.
2. Copy a CA's public key from diskette to each server. Repeat the following steps for each client or server:
 - a. In the navigation area, expand the local HMC. It is the first HMC in the list.
 - b. Expand **System Manager Security**.
 - c. Click **Certificate Authority**.
 - d. In the System Manager Certificate Authority window, click **Copy another Certificate Authority's Public Key Ring File from removable media**. You can also select **Copy in CA Public Key** from the Certificate Authority menu.
 - e. When the Copy CA Public Key from removable media window opens, insert the removable media that contains the copied CA's public key ring file.
 - f. Click **OK** to copy the public key ring file.

Distributing the certificate authority's public key with Web-based System Manager Remote Client

If you are using the Web-based System Manager Remote Client, follow these instructions to copy the CA's public key ring file (SM.pubkr) to the Web-based System Manager directory of each client:

1. The Web-based System Manager Remote Client must be installed on the client before proceeding. If you have not yet installed the Web-based System Manager Remote Client, perform the steps in "Installing the Web-based System Manager Remote Client" on page 66, and then return to these instructions.
2. On the CA system, perform the following steps to copy the CA's public key to removable media:
 - a. If you plan to distribute the CA's public key to an HMC or AIX client, ensure that the disk is a tar media.
If you plan to distribute the CA's public key to a PC client, ensure that the media is formatted for DOS.
 - b. In the navigation area, expand the local HMC. It is the first HMC in the list.
 - c. Expand **System Manager Security**.
 - d. Click **Certificate Authority**.
 - e. In the System Manager Certificate Authority window, click **Copy this Certificate Authority's Public Key Ring File to removable media**.
 - f. When the Copy CA Public Key to Removable Media window opens, insert the media.
 - g. Select the type of client or server to which you want the public key ring file to be copied:
 - Select **HMC or AIX client** to write the file to a tar media.
 - Select **PC client** to write the file to media in DOS file format.
 - h. Click **OK** to copy the public key ring file.
3. To copy a CA's public key from removable media to each HMC client:
Repeat the following steps for each client or server:
 - a. In the navigation area, expand the local HMC. It is the first HMC in the list.
 - b. Expand **System Manager Security**.
 - c. Click **Certificate Authority**.
 - d. In the System Manager Certificate Authority window, click **Copy another Certificate Authority's Public Key Ring File from removable media**.
 - e. When the Copy CA Public Key from Removable Media window opens, insert the diskette that contains the copied CA's public key ring file.
 - f. Click **OK** to copy the public key ring file.
4. Distribute the CA's public key to your Windows, Linux, or AIX remote clients using the following steps:
Use command line or stand-alone tools to copy the CA's public key from removable media to the codebase directory of the remote client. The CA's public key file must be copied in binary format. The codebase directory locations are:
 - On a Windows client: **Program files\websm\codebase**
 - On an AIX client: **/usr/websm/codebase**
 - On a Linux client: **/opt/websm/codebase**

Viewing configuration properties

You can view the properties of the certificate authority (CA) and of any server. The property windows provide read-only information for the CA and the servers.

View CA properties

1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand **System Manager Security**.
3. Click **Certificate Authority**.
4. Select **Properties**.
5. Type the password.

View server properties

1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand **System Manager Security**.
3. Click **Server Security**.
4. Select **View properties for this server** from the task list.

Configuring HMC object manager security

Learn about how to configure object manager security.

1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand **System Manager Security**.
3. Click **Object Manager Security**.
4. Click **Configure Object Manager Security**.
5. Select a socket mode.
6. Click **OK**.

If you are using the Web-based System Manager Remote Client for Java Web Start, install this product now. See “Installing the Web-based System Manager Remote Client for Java Web Start” on page 67.

Installing the Web-based System Manager Remote Client

Follow these steps to successfully install the Web-based System Manager Remote Client.

1. Uninstall the previous version of the Web-based System Manager Remote Client.
2. Type the following address in your machine’s Web browser:
`http://system name/remote_client.html`
The *system name* is the name of the HMC you plan to access remotely.
3. Enter your HMC user ID and password.
4. Click **InstallShield**.
5. Click **Windows** to download the **setup.exe** file or click **Linux** to download the **wsmlinuxclient.exe** file.
6. If you are using a Linux system, run the following command to make the **wsmlinuxclient.exe** file executable:
`chmod 755 wsmlinuxclient.exe`
7. Run the **wsmlinuxclient.exe** file or the **setup.exe** file to begin the installation process. If you encounter problems with this step, see Troubleshooting for help.
8. When the Remote Client Installer window displays, click **Next** to continue.
9. To install using the default location, click **Next**. Otherwise, browse or type the desired location and click **Next**. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package. If any of the information shown is incorrect, click **Back** to make corrections.
10. Click **Next** to start the installation. A status window displays a message indicating the installation completed successfully or error messages if errors occurred during the installation.
11. Click **Finish** to close the window.
12. Type the following address in your machine’s Web browser:
`http://system name/remote_client_security.html`
The *system name* is the name of the HMC you plan to access remotely.
13. Click **Windows** to download the **setupsec.exe** file or click **Linux** to download the **setupsecl.exe** file.
14. Run the **setupsecl.exe** file or the **setupsec.exe** file to begin the installation process. If you encounter problems with this step, see Troubleshooting for help.
15. When the Remote Client Security Installer window displays, click **Next** to continue.

16. To install using the default location, click **Next**. Otherwise, browse or type the desired location and click **Next**. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package.

Note: Be sure the location you select in this step is the same location that you selected when installing the remote client.

17. If any of the information shown is incorrect, click **Back** to make corrections. Click **Next** to start the installation. A status window displays a message indicating the installation completed successfully, or error messages if an error occurred during the installation.
18. Click **Finish** to close the window.

Note: To make a secure connection from the Remote Client, you must configure security on the HMC and copy the CA's public key to the client. See Web-based System Manager Remote Client tasks.

Uninstalling the Web-based System Manager Remote Client

To install the latest version of the Web-based System Manager Remote Client, you must uninstall any previous versions from your Linux or Windows PC.

Linux

1. Run the following command:
`installdir/_uninst/uninstall`
The *installdir* is the name of the directory where the remote client is located.
2. Run the following command:
`installdir/_uninstssl/uninstallssl`
The *installdir* is the name of the directory where your remote client is located.

Windows

Complete the following steps once to uninstall the Web-based System Manager Remote Client and again to uninstall remote client security:

1. From the task bar, select **Start > Settings > Control panel**.
2. In the Control window, double-click the **Add/Remove Programs** icon.
3. From the list of programs on the Install/Uninstall tab, select **Web-Based System Manager Remote Client** to uninstall the remote client and **Remote Client Security** to uninstall remote HMC client security.

Note: Earlier versions of the remote client might display as Web-based System Manager PC Client and the remote client security as Web-based System Manager PC Client Security.

4. Click **Change/Remove** to start the Uninstall wizard.
5. Click **Next** in the initial window.
6. Click **Next** in the Confirmation window. A status window displays a message indicating that the uninstallation completed successfully or error messages if errors occurred during the uninstallation.
7. Click **Finish** to close the window.
8. Repeat steps 1 through 7 to uninstall remote client security.

Installing the Web-based System Manager Remote Client for Java Web Start

Complete the following steps to install the Web-based System Manager Remote Client for Java Web Start.

1. Type the following address in your PC's Web browser:
`http://system name/remote_client.html`

The *system name* is the name of the HMC you plan to access remotely.

2. Enter your HMC user ID and password.
3. From the Web-based System Manager Remote Client Selection page, click **Java Web Start**.
4. If you currently do not have it installed, download Java Web Start.

If you do not have Java Web Start currently installed on your client, click **Java Web Start for Windows** for a Windows client or **Java Web Start for Linux** for a Linux client on the Web-based System Manager Remote Client for Java Web Start Installation page to download the installation image. Download the most recent compatible version. Click on each version to see system requirements.

- To install on a Windows client, double-click the downloaded image to launch the installation wizard.
- To install on a Linux client, use the following command:

```
rpm -i ibm-linux-jre.i386.rpm
export PATH=$PATH:/opt/IBMJava2-142/jre/bin
cd /
/opt/IBMJava2-142/jre/javaws/updateSettings.sh
```

Note: Run the last line (/opt/IBMJava2-142/jre/javaws/updateSettings.sh) from the root directory.

5. Go back to the Web-based System Manager Remote Client for Java Web Start Installation page, and click **Remote Client** to download the remote client to your PC.
6. Launch the Web-based System Manager Remote Client for Java Web Start using the Web-based System Manager icon.

Note: If you installed the Web-based System Manager Remote Client for Java Web Start on a Linux system, launch Web-based System Manager one of the following ways:

- Use a virtual terminal session to launch the Web-based System Manager Remote Client for Java Web Start:
 - a. Open a virtual terminal session and navigate to the directory in which you installed Java Web Start. This is usually the javaws directory.
 - b. Launch Java Web Start by executing the javaws command.
 - c. From the Java Web Start Application Manager, select **View > Downloaded Applications**.
 - d. Select **Web-based System Manager Remote Client**.
 - e. Select **Application > Start Web-based System Manager** to launch the remote client.
- Use the browser to launch the Web-based System Manager Remote Client for Java Web Start:
 - a. Type the following address in your machine's Web browser:
`http://system name/remote_client.html`

where *system name* is the name of the HMC you plan to access remotely.
 - b. Click **Java Web Start**.
 - c. Click **Remote Client**.

Uninstalling the Web-based System Manager Remote Client for Java Web Start

To uninstall the Web-based System Manager Remote Client for Java Web Start from your PC, complete the following steps:

1. From the View menu in the Java Web Start Application Manager, select **Downloaded Applications**.
2. Click the **Web-based System Manager Remote Client** icon.
3. Click **Application > Remove Application**.

Working with the HMC

Describes how to perform actions that pertain to the HMC itself.

To learn more about the commands you can use to operate the HMC remotely, see [Overview of HMC tasks](#).

To learn more about how to cluster your systems using InfiniBand (IB), see [Clustering systems using InfiniBand \(IB\) hardware](#).

Basic operations

Describes the basic operations that you can perform on your HMC, such as starting the HMC, changing the language HMC language, and logging off the HMC.

This topic provides information on how to perform basic operations on your HMC:

Starting the HMC

Explains how to start the HMC interface.

To start the HMC, do the following:

1. Turn on the HMC by pressing the power button.
2. If English is your language preference, continue with step 5.
3. If your language preference is a language other than English, type the number **2** when you are prompted to change the locale.

Note: This prompt times out in 30 seconds if you do not act.

4. Select the locale that you want to display from the list in the Locale Selection window, and click **OK**. The locale identifies the language that the HMC interface displays.
5. Log in to the HMC using the following default user ID and password:

ID: hscroot

Password: abc123

6. Press Enter.

Shutting down, rebooting, and logging off the HMC

Explains how to shut down, reboot, and log off the HMC interface

This task allows you to shut down, reboot, and log off the HMC interface.

Attention: Use the white button on the HMC to perform a manual shutdown only if the server does not respond to any tasks performed from the console, such as shutting down the HMC.

If an operating system is open and running on a partition, and you decide to shut down, reboot, or log off the HMC interface, the operating system continues to run without interruption.

To log off the HMC interface, do the following:

1. In the main menu, click **Console > Exit**. At this point, you can select to save the state of the console for the next session by selecting the check box next to the option.
2. Click **Exit Now**.

Setting the date and time

Describes how to change the date and time for the HMC

The battery-operated clock keeps the date and time for the HMC. You might need to reset the console date and time if the battery is replaced, or if you physically move your system to a different time zone. If you change the date and time information, the change does not affect the systems and logical partitions that the HMC manages.

To change the date and time for the HMC, do the following:

1. Ensure that you are a member of one of the following roles:
 - Super administrator
 - Service representative
 - Operator
 - Viewer
2. In the navigation area, expand the HMC you want to work with. HMCs are listed by hostname or IP address.
3. Expand **HMC Management**.
4. Click **HMC Configuration**.
5. In the contents pane, click **Customize Console Date and Time**.
6. Enter the date, time, and time zone, and click **OK**.

Note: The time setting will adjust automatically for daylight saving time in the time zone you select.

Changing the HMC interface language

Describes how to change the interface language that you see on the HMC interface, as well as the locale

When you power on the HMC, the HMC prompts you to change the interface language and locale. The *locale* is the language in which you want the HMC to display. Changes made using this procedure affect the language and locale for the HMC server. If you are using the remote client to connect to the HMC, the language and locale settings on your Windows operating system determine the settings that the remote client uses to display the HMC on your PC.

Any user role can change the HMC interface language.

To change the HMC interface language and locale when you power on the HMC, do the following:

1. Power on the HMC.
2. When you are prompted to change the language and locale, select the language and locale you want to display. If nothing is selected within 20 seconds, the dialog exits. By default, the **Exit now and prompt again for locale change** option is selected. The boot continues.
3. Click **OK**. When the HMC completes the power-on process, the language and locale that you selected are displayed.

To change the HMC interface language and locale using the HMC Configuration application, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **HMC Configuration** icon.
3. In the Contents area, click **Change Current Language and Locale**.
4. In the window, select the language and locale you want to display.
5. Click **OK**.
6. Log off the HMC interface and then log in.

Configuring the HMC keyboard layout

Describes how to configure the keyboard layout.

When you power on the HMC, the HMC prompts you to configure the keyboard layout. If you do not respond, the HMC continues to power on, using the previous keyboard configuration. English is the default setting.

Any user role can change the keyboard layout.

Note: If you previously selected the **Do not run this program to change keyboard layout on the next system boot** option and you want to change the keyboard layout again, open a restricted shell (rshterm) and use the following **chhmc** command:

```
chhmc -c kbdcfg -s enable
```

To configure the keyboard layout when you power on the HMC, do the following:

1. Power on the HMC.
2. When the Keyboard Layout Configuration Screen displays, select the **Change to a new keyboard layout** option. If nothing is selected within 20 seconds, the dialog exits. By default, the **Do not change keyboard layout and run this program again on the next system boot** option is selected. The boot continues.
3. Select the desired keyboard layout from the list.
4. Select the appropriate option if you want to run this program on the next system boot and press Enter.

Viewing recent HMC activity

Explains how to view recent HMC activity.

To see a log of recent HMC activity, you can view console events. Each event has an associated time stamp.

The following is a sample of the events recorded:

- When a logical partition was activated
- When a system was powered on
- When a logical partition was shut down
- Results of a scheduled operation

To view console events, you must be a member of one of the following roles:

- super administrator
- service representative
- operator
- product engineer

To view console events, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, click the **HMC Configuration** icon.
3. In the Contents area, select **View Console Events**.

Working with partition profile information

Back up, restore, initialize, and remove profile information for the logical partitions.

You can back up, restore, initialize, and remove profiles that you have created. This topic describes each of these options.

For more information about creating profiles, see [Creating new logical partitions and partition profiles](#).

Backing up partition profile data

Describes how to back up profile data on the HMC.

This topic describes how to back up logical partition profile data.

To back up partition profile data, you must be a member of one of the following roles:

- super administrator
- service representative

To back up partition profile data, do the following:

1. In the Contents area, select the managed system.
2. From the menu, click **Selected > Profile Data > Backup**.
3. Type the name you want to use for this backup file.
4. Click **OK**.

Initializing profile data

Explains how to initialize the profile data.

When you initialize profile data, you return the managed system to a state that does not have any logical partitions or profiles. You can perform this task in order to stabilize your managed system if the profile data becomes corrupt.

Important: After you perform this task, any profiles that you created prior to initialization are erased. Use this procedure only under the direction of your service provider.

To initialize profile data, your authority level must be a super administrator.

Note: You can initialize profile data only when the managed system is in the *Operating* or *Standby* state and all the partitions are in the *Not Activated* state.

To initialize profile data, do the following:

1. In the Contents area, select the managed system.
2. From the menu, select **Selected > Profile Data > Initialize**.
3. Click **Yes**.

Restoring profile data

Explains how to read the profile data from the previously backed-up file on the HMC and load this data to the managed system.

Selecting this menu item restores profile data to the HMC from a backup file stored on the HMC hard drive.

Note: This is not a concurrent procedure. When the data is restored, the managed system powers on to Partition Standby. For more information about power-on modes, see Managed system power-on modes.

To restore stored profile data on the HMC hard drive, you must be a member of one of the following roles:

- super administrator
- service representative

To restore profile data, do the following:

1. In the Contents area, select the managed system.

2. From the menu, select **Selected > Profile Data > Restore**.
3. Select the profile information that you want to restore from the list of backup files.
4. Select a restore option.
5. Click **OK**.

Removing profile data

Explains how to remove the previously backed-up file on the HMC.

To remove stored profile data from the HMC hard disk drive, you must be a member of one of the following roles:

- super administrator
- service representative

To remove stored profile data, do the following:

1. In the Contents area, select the managed system.
2. From the menu, select **Selected > Profile Data > Remove**.
3. Select the profile data that you want to remove.
4. Click **OK**.

Collecting and viewing resource utilization data

This section describes how to gather and view resource utilization information.

You can use your HMC to collect and view the types of system activities that affect partition performance and capacity. The following are the types of events that the HMC records:

- Shared processor utilization data
- Any managed system change that affects data collection
- Any partition change that affects data collection

You can use this data to analyze trends and make resource adjustments.

These topics are intended for HMC users who want to collect and view resource utilization data. For more information, click on the associated topic link:

Setting the HMC to collect resource utilization data for managed systems

Use this procedure to set the Hardware Management Console (HMC) to collect resource utilization data for any of the managed systems that it manages.

To set the HMC to collect resource utilization data, you must be a super administrator or operator. For more information about user roles, refer to Tasks and roles.

When you set the HMC to collect resource utilization data for a managed system, the HMC collects utilization data for memory and processor resources (including 5250 CPW where applicable). The HMC collects utilization data into records called events. Events are created at the following times:

- At periodic intervals (hourly, daily, and monthly)
- When you make system-level and partition-level state and configuration changes that affect resource utilization
- When you start up, shut down, and change the local time on the HMC

To set the HMC to collect resource utilization data, follow these steps:

1. In the navigation area, open the object with the same name as your HMC.
2. Open **Server and Partition**.
3. Select **Utilization Data Management**.

4. In the contents area, click **Change Settings for Utilization Data Collection**.
5. Specify the managed systems for which you want to collect utilization data.

For which managed systems do you want to collect utilization data?	Complete the following:
All managed systems that are managed by the HMC	<ol style="list-style-type: none"> 1. Select All Managed Systems. 2. Select Enable under All Managed Systems and click OK.
Specific managed systems	<ol style="list-style-type: none"> 1. Select Select from the following. 2. Select Enable beside each managed system for which you want to collect utilization data and click OK.

Viewing resource utilization data for a managed system

Use this procedure to view the resource utilization data for a managed system using the Hardware Management Console (HMC).

Before you can view resource utilization data for a managed system, you must set the HMC to collect utilization data. For more information on how to set the HMC to collect utilization data, see “Setting the HMC to collect resource utilization data for managed systems” on page 73.

Users with any user role can view resource utilization data for managed systems. For more information about user roles, refer to Tasks and roles.

The HMC collects utilization data for memory and processor resources (including 5250 CPW where applicable). The HMC collects utilization data into records called events. Events are created at the following times:

- At periodic intervals (hourly, daily, and monthly)
- When you make system-level and partition-level state and configuration changes that affect resource utilization
- When you start, shut down, and change the local time on the HMC

To view the resource utilization data for a managed system, follow these steps:

1. In the navigation area, open **Server and Partition**.
2. Select **Utilization Data Management**.
3. In the contents area, click **View Utilization Data**.
4. Specify the managed system whose resource utilization data you want to view in the **Managed System** field.
5. Select whether you want to view the data that was collected hourly, daily, or monthly.
6. Specify the date and time range whose resource utilization events you want to view. The date and time information that you specify here are based on the local time on the HMC and not necessarily the time on the managed systems.
7. Specify the maximum number of resource utilization events that you want to view and click **OK**. A window displays with a list of the resource utilization events that match the given criteria.
8. To view more detailed information about a resource utilization event, select an event and then click **OK**. To view more information about the selected utilization event, select the **View** menu option.

Backing up and restoring the HMC

This section describes how to back up HMC data.

The HMC provides the tools you need to back up and restore important HMC data.

Backing up the HMC does not back up the data on the server. For more information about backing up data on a logical partition, select the topic that matches your logical partition's configuration:

- Backing up and recovering i5/OS® data These topics provide instructions for backing up and restoring i5/OS installations.
- Backing up and recovering AIX logical partitions These topics provide instructions for backing up and restoring AIX installations.
- Backing up and recovering Linux installations These topics provide instructions for backing up and restoring Linux installations.

Setting up the network interface as a startup device

This section describes how to enable the F12 function key to set up the network interface as a startup device.

On some HMC models, the F12 function key is not enabled for use when the HMC is powered on. These steps enable the F12 function key so that you can specify the network interface as a startup device.

To set up the network interface as a startup device, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

To set up the network interface as a startup device, do the following:

1. Shut down and power off the HMC. For more information, see "Shutting down, rebooting, and logging off the HMC" on page 69.
2. Power on the HMC console.
3. Press F1 to start the BIOS Setup utility.
4. Find and select **Startup** or **Start Options**.
5. Select **Startup Sequence** to view the list of startup devices.
6. Depending on the type of HMC (desktop or rack-mounted), use the +/- key or arrow key to make the network interface an entry in the startup list, after the hard disk.
7. If the HMC is a desktop, find and enable the Start up Device Menu prompt. This enables the F12 function key when the HMC powers on, so that you can select the network device in your startup list. For CR2 and CR3 machine types, the Planar Ethernet PXE/DHCP entry should have Planar Ethernet 1 and Planar Ethernet 2.

On desktop HMC machines, do the following:

- a. Press Esc.
 - b. Select **Devices -> Network Setup**.
 - c. Ensure that **PXE Boot Agent** and **PXE Base code** are set to **Enabled**. If these settings are not enabled, networking will not occur.
8. When you have finished, save the settings and exit the BIOS setup utility to restart the boot process.

You can now press F12 to select the network device as the startup device. If a DHCP server can accept PXE requests from the HMC, and has the required files, the HMC will boot from it, then the Backup/Upgrade/Restore/Install window opens.

Beginning with HMC Version 5 Release 2.0, the **chhmc** command can be used on some HMC machine types to set the network interface as a startup device. To enable network boot on the HMC, use the following command:

```
chhmc -c netboot -s enable
```

When the command completes, you can the following command to verify that network boot has been enabled:

```
lshmc -r
```

The command then displays the following:

```
ssh=enable,xntp=disable,websm=enable,http=enable,netboot=enable
```

To disable network boot, use the **chhmc** command:

```
chhmc -c netboot -s disable
```

Setting up a remote system for HMC installation, backup, or restoration over the network

Describes the steps you take to prepare your server to allow an HMC to connect to a network and perform an installation, backup, or restore operation over the network.

To perform a network boot of the HMC, you must have the following:

- You must have a system that has DHCP, NFS, and TFTP servers installed and running. To perform a backup or restore in secure mode, you need an ssh server running on the system.
- The system must be accessible to the HMC over a network.
- The syslinux package must be installed on the system; this package gives you access to the pxelinux.0 boot loader file.
- You must have obtained the following required HMC images and stored them in the location specified in the steps following the table.

Table 5. Required images

File name	File content
bzImage	Kernel image
initrd.gz	RAM Disk file system
disk1.img	Base image
disk2.img	Base HMC image
disk3.img	Information center image

To set up your server to allow an HMC to contact the network and perform an installation, backup, or restore operation over the network, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

To set up your server to allow an HMC to contact and perform an installation, backup, or restore operation over the network, do the following:

1. Log in as root.
2. Check the `/etc/xinetd.d/tftp` configuration file and look up the `server_args`. The default setting is usually `/var/tftp`.
3. Create the directory `/var/tftp`. Run the following command:

```
mkdir -p /var/tftp
```
4. Edit the `/etc/dhcpd.conf` file and add the two lines that are highlighted in the following sample `dhcpd.conf` file, if they are not already in the file.

```

allow bootp;
allow booting;
ddns-update-style none;
default-lease-time 14400;
max-lease-time 172800;
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.200;
    option routers 192.168.1.1;
    option domain-name "somecompany.com";
    option domain-name-servers 192.168.1.1;
    filename "pxelinux.0";
}

```

This sample file specifies the range of IP addresses to be served by the DHCP server. One of the IP addresses in this range will be assigned to the HMC when it broadcasts a request to obtain an IP address. The bootloader that will be used is pxlinux.0 in the /var/tftp directory. This file is part of the syslinux package and is usually located in the /usr/lib/syslinux directory.

5. Copy the pxelinux.0 file to the /var/tftp directory. Run the following command:

```
cp /usr/lib/syslinux/pxelinux.0 /var/tftp/
```

6. Create the /var/tftp/hmc and /var/tftp/pxelinux.cfg directories by running the following commands: :

```
mkdir -p /var/tftp/hmc
mkdir -p /var/tftp/pxelinux.cfg
```

7. Copy the bzImage and initrd.gz files that you previously downloaded from your provider to the /var/tftp/hmc directory.
8. Create a directory (for example, /home/hmc) and use NFS to export this directory. If you want to use this directory to back up the HMC over the network, you must allow write access to it.

- a. Run the following command to create the directory:

```
mkdir -p /home/hmc
```

- b. Edit the /etc/exports file, and add the following line:

```
/home/hmc          *(ro)
```

To export the directory with write access, replace *(ro) with *(rw).

- c. Run the following command to export the directory:

```
exportfs -va
```

9. Copy the disk1.img, disk2.img and disk3.img files that you previously downloaded from your provider to the /home/hmc directory.
10. Create a file, named default, in the /var/tftp/pxelinux.cfg directory. This file must contain the following data:

```

default hmc
label hmc
    kernel hmc/bzimage
    append initrd=hmc/initrd.gz media=network
        server=192.168.1.1 dir=/home/hmc
        mode=manual vga=0x317

```

This default configuration file indicates that the kernel file bzImage will be installed from the /var/tftp/hmc directory. The HMC uses file initrd.gz in the /var/tftp/hmc directory as the RAM disk, records the server's IP address (192.168.1.1), and confirms that the /home/hmc/ directory on the server contains the necessary images.

The server is now ready to accept requests from the HMC.

Backing up the entire HMC hard drive to a remote system

Describes how to use the network to back up the entire HMC hard drive.

You can use your HMC to back up the entire hard disk of your HMC to a remote system. Your remote system must have Network File System (NFS) or Secure Shell (ssh) configured and this network must be accessible from the HMC. To complete this task, you must shut down and reboot the HMC. Do not use the remote commands or the remote client to perform these tasks. Use an HMC hardware console.

To back up the HMC hard drive to a remote system, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

To back up the HMC hard drive to a remote system, do the following:

1. Shut down and power off the HMC. For more information, see “Shutting down, rebooting, and logging off the HMC” on page 69.
2. Power on the HMC console with the HMC recovery media (V5R1.0 or later) in the DVD drive. If you want to start the HMC interface from a configured network boot server, make sure the network interface is one of the devices in your startup sequence. To view the list of startup devices, press F12 when the HMC powers on, and select the network interface from which you want to boot. If the F12 function key is not enabled, see “Setting up the network interface as a startup device” on page 75 to enable it.
3. Select the backup option and click **Next**.
4. Select the network interface to use for communicating with the remote server. If you are starting the HMC by contacting a network boot server, and this server is also the remote server to which you want to back up the data, then select the default settings. Then click **Next** and go to 6. If you do not select the default settings, continue with the next step.
5. If you do not select the Default settings, you must select the network protocol to use with the selected interface. You can choose to obtain an IP address from a DHCP server in your network or assign a static IP address to the selected network interface. Make your selection and click **Next**.
6. If you did not select the default settings, type the IP address or host name of your remote server. The backup file will be created using the gzip compression utility and the **tar** command. Therefore, it is recommended that you specify a file with the .tgz extension in the **File on remote host** field. If you have selected the default network settings, you must use the directory setup in your network boot configuration. This information is displayed in the **File on remote host** field. After you have completed all the required information, click **Next**.
7. Select the method you want to use to transfer the data from your HMC to the remote server. If you choose to encrypt the data, your remote host must have secure shell server (SSH) running. If you choose to transfer the data without encryption, your remote host must have Network File Server (NFS) running, and the directory to which you want to back up data must be exported for write access. Make your selection and click **Next**.
8. If you select to transfer the data using encryption, you must type the remote server’s user ID and password.
9. Verify the information you entered is correct and click **Finish**. When the backup completes, the HMC interface displays.

If you have modified the startup sequence by pressing F1 when you powered on the HMC, you must reboot the HMC and change the settings again. When you change the startup sequence, ensure that your hard disk is listed before the network interface in the startup sequence.

Backing up critical HMC data

Describes how to back up important console information to DVD, a remote system mounted to the HMC file system (such as NFS), or a remote site through FTP.

Using the HMC, you can back up all important data, such as the following:

- User-preference files

- User information
- HMC platform-configuration files
- HMC log files
- HMC updates through Install Corrective Service

Note: Use the archived data *only* in conjunction with a reinstallation of the HMC from the product CDs. For information about how to reinstall the HMC, see “Reinstalling the HMC machine code” on page 82.

The Backup function saves the HMC data stored on the HMC hard disk to DVD, a remote system mounted to the HMC file system (such as NFS), or a remote site through FTP. Back up the HMC after you have made changes to the HMC or to the information associated with logical partitions.

Note: The DVD must be formatted in the DVD-RAM format before data can be saved to the DVD.

To back up the HMC, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

To back up the HMC, do the following:

1. In the Navigation area, click the **Licensed Internal Code Maintenance** icon.
2. In the Contents area, click the **HMC Code Update** icon.
3. Select **Back up Critical Console Data**.
4. Select an archive option. You can back up to DVD on the HMC, back up to a remote system mounted to the HMC file system, or a remote site through FTP.
5. Follow the instructions on the window to back up the data.

Restoring the entire HMC hard drive using the network

Describes how to use the network to restore the entire HMC hard drive using a previously saved network file.

You can use your HMC to restore your HMC hard disk from a remote system. To complete this task, you must first have a backup copy available on your network. To learn more about backing up the entire HMC hard drive to a remote system, see “Backing up the entire HMC hard drive to a remote system” on page 77. Your remote system must have Network File System (NFS) or Secure Shell (ssh) configured and this network must be accessible from the HMC. To complete this task, you must shut down and reboot the HMC. Do not use the remote commands or the remote client to perform these tasks. Use an HMC hardware console.

To restore the HMC hard drive from a remote system, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

To restore the HMC hard drive to a remote system, do the following:

1. Shut down and power off the HMC. For more information, see “Shutting down, rebooting, and logging off the HMC” on page 69.
2. Power on the HMC console with the HMC Recovery media (V5R1.0 or later) in the DVD drive. If you want to start from a configured network boot server, make sure the network interface is one of the devices in your startup sequence. To view the list of startup devices, press F12 when the HMC

powers on, and select the network interface from which you want to boot. If the F12 function key is not enabled, see “Setting up the network interface as a startup device” on page 75 to enable it.

3. Select the restore option and click **Next**.
4. Select the network interface to use for communicating with the remote server. If you are restoring the HMC by contacting a network boot server, and this server is also the remote server to which you want to restore the data, then select the default settings. Press **Next** and go to 7.
5. If you do not select the Default settings, you must select the network protocol to use with the selected interface. You can choose to obtain an IP address from a DHCP server in your network, or assign a static IP address to the selected network interface. Make your selection and click **Next**.
6. If you did not select the Default setting, enter the IP address or host name of your remote server and type the backup file name in the **File on remote host** field. If you have selected the default network settings, you must use the directory setup in your network boot configuration. This information is displayed in the **File on remote host** field. After you have completed all the required information, click **Next**.
7. Select the method you want to use to transfer the data from your remote server to your HMC. If you choose to encrypt the data, your remote host must have secure shell server (SSH) running. If you choose to transfer the data without encryption, your remote host must have Network File Server (NFS) running, and the directory to which you want to back up data must be exported for write access. Make your selection and click **Next**.
8. If you want to transfer the data using encryption, type a user ID and password on the remote server when you are prompted for them, and click **Next**.
9. Verify the information you entered is correct and click **Finish**. When the restore operation completes, the HMC interface displays.

If you have modified the startup sequence by pressing F1 when you powered on the HMC, you must reboot the HMC and change the settings again. When you change the startup sequence, ensure that your hard disk is listed before the network interface in the startup sequence.

Restoring critical HMC data

Describes how to restore critical HMC data.

Backing up critical console data includes both backup data and corrective service data.

Restore HMC backup data *only* in conjunction with a reinstallation of the HMC. For information about how to reinstall the HMC, see “Reinstalling the HMC machine code” on page 82.

Note: For this operation, you must have one of the following:

- The backup DVD media
- Access to the remote server where the archive was created by using the procedure in “Backing up critical HMC data” on page 78

To restore the HMC data, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

Select the data-restoration procedure based on the data archiving method used:

Restoring from DVD:

Restore data that was archived to DVD.

If the critical console data has been archived on a DVD, do the following:

1. Select **1 - Restore Critical Console Data** from the menu displayed at the end of the HMC reinstallation.
2. Insert the DVD containing the archived console data. On the first boot of the newly installed HMC, the data is automatically restored.

Restoring from a remote server:

Restore data that was archived to a remote FTP or NFS sever.

If the critical console data has been archived remotely, do the following:

1. Manually reconfigure network settings to enable access to the remote server after the HMC is newly installed. For information about configuring network settings, see “Configuring the HMC” on page 48.
2. In the Navigation area, click the **Licensed Internal Code Maintenance** icon.
3. In the Contents area, click the **HMC Code Update** icon.
4. Select **Restore Remote Console Data**.
5. Select the type of remote restoration.
6. Follow the directions on the window to restore the critical console data. The data automatically restores from the remote server when the system is rebooted.

Scheduling and reviewing HMC backups

Explains how to schedule backups of important console information.

You can schedule a backup to DVD to occur once, or you can set up a repeating schedule. You must provide the time and date that you want the operation to occur. If the operation is scheduled to repeat, you must select how often you want this backup to run (hourly, daily, weekly, or monthly).

Note: Only the most-recent backup image is stored at any time on the DVD.

To schedule a backup operation, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. In the Navigation area, click the **HMC Configuration** icon.
3. In the Contents area, click **Schedule Operations**.
4. From the list, select the HMC you want to back up and click **OK**.
5. Select **Options > New**.
6. In the Add a Scheduled Operation window, select **Backup Critical Console Data** and click **OK**.
7. In the appropriate fields, enter the time and date that you want this backup to occur.
8. If you want this scheduled operation to repeat, click the **Repeat** tab and select the intervals at which you want the backup to repeat and press Enter.
9. When you have set the backup time and date, click **Save**. When the Action Completed window opens, click **OK**. A description of the operation displays in the Scheduled Operations window.

Saving HMC upgrade data

Explains how to save upgrade data so that you can reinstall it if the HMC must be recovered.

You can save the current HMC configuration in a special disk partition on the HMC. Save upgrade data before you upgrade your HMC software to a new version or release. This action allows you to restore HMC configuration settings after upgrading.

Note: The special disk partition can hold only one level of backup data. Every time you perform this task, previous backup data is overwritten by the latest backup. To proceed with the upgrade after

saving upgrade data, you must place the new HMC recovery CD in the DVD drive and immediately reboot the HMC. Any configuration changes made on the HMC after you saved the upgrade data will not be saved.

To save upgrade data, do the following:

1. Expand the **Licensed Internal Code Maintenance** folder, then select the HMC application in the Navigation area.
2. Select the **Save Upgrade Data** task in the content area. An information window opens that prompts you to select the media (hard drive or DVD).
3. Select the appropriate media.
4. Click **Continue**.
5. Click **OK** to confirm and close the information window.

Reinstalling the HMC machine code

Explains how to reinstall the HMC machine code prior to restoring critical backup data and it describes how to reinstall the HMC interface onto the HMC PC and install backup information.

If the HMC is not responding, you can use the recovery CD to reinstall the HMC onto the HMC PC. After you reinstall the HMC machine code, you can restore the backup data that you created to recover your critical console information. For information about how to restore the HMC backup data, see “Restoring critical HMC data” on page 80.

To reinstall the HMC machine code, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

To reinstall the HMC machine code, do the following:

1. Shut down and power off the HMC. For more information, see “Shutting down, rebooting, and logging off the HMC” on page 69.
2. Power on the HMC console and insert the HMC recovery media if you want to install from it. The HMC powers on from the media and displays the Backup/Upgrade/Restore/Install window. If you want to install from the network and have a network boot server configured, make sure the network interface is one of the devices in your startup sequence. To view the list of startup devices, press F12 when the HMC powers on, and select the network interface from which you want to boot. If the F12 function key is not enabled, see “Setting up the network interface as a startup device” on page 75 to enable it.
3. Select the Install option, and click **Next**.
4. Select **Install from media** if you are using media. If you are not installing from media, select **Install from network**. Click **Next**.
5. If you install from media, you are prompted to install the next media. Select **1 - Install additional software from media** to install the subsequent media. If you install from a network, you must complete the next step.
6. After the installation is complete, select **1 - Install additional software from media** from the menu displayed to install the subsequent media.
7. Select **1 - Restore Critical Console Data** from the menu to restore data from a DVD. To restore from a remote server, select **2 - Finish the Installation**.

Working with users, roles, and passwords

Learn how to perform HMC user administration tasks.

The following topics provide information about HMC user administration tasks:

Creating an HMC user

Describes how to create HMC users.

You can create various users using the HMC. The hscroot, root, and hscpe user IDs are special, or reserved. The hscpe user is created for use by your service provider when performing problem determination.

To create a user, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. Click the **HMC users** icon.
3. In the Contents area, click **Manage HMC Users and Access**. The User Profiles window opens.
4. Click **User > Add**. Fill in the appropriate fields and click **OK**.

Viewing an HMC user description

Describes how to view HMC user definitions.

To view a user description, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. Click the **HMC users** icon.
3. In the Contents area, click **Manage HMC Users and Access**. The User Profiles window opens.
4. Click **User > Modify**. The current user description is displayed.

To read about the tasks each HMC user role can perform and the commands associated with each task, see Overview of HMC tasks.

Copying HMC user information

Describes how to copy existing user information.

To copy HMC user information, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. Click the **HMC users** icon.
3. In the Contents area, click **Manage HMC Users and Access**. The User Profiles window opens.
4. Click **User > Copy**. Fill in the appropriate fields and click **OK**.

Deleting an HMC user

Describes how to delete an HMC user.

To delete a user, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. Click the **HMC users** icon.
3. In the Contents area, click **Manage HMC Users and Access**. The User Profiles window opens.
4. Select the user that you want to remove.
5. Click **User > Remove**. The Delete Item Verification window opens.
6. Click **Yes**.

Creating a customized HMC role

Describes how to create a customized HMC role

To create a customized HMC role, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. Click the **HMC users** icon.

3. In the Contents area, click **Manage Access Task Roles and Managed Resource Roles**. The Customized User Controls window opens.
4. Click **Task Roles**.
5. Click **File > Add**. The Add Role window opens.
6. Fill in the appropriate fields and click **OK**.

Editing HMC user information and roles

Describes how to change HMC user description.

To edit HMC user information and roles, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. Click the **HMC users** icon.
3. In the Contents area, click **Manage HMC Users and Access**. The User Profiles window opens.
4. Click **User > Modify**. Fill in the appropriate fields and click **OK**.

Changing HMC user passwords

Describes how to change an existing HMC user's password.

To change HMC user passwords, do the following:

1. In the Navigation area, expand the **HMC Management** folder.
2. Click the **HMC users** icon.
3. In the Contents area, click **Manage HMC Users and Access**. The User Profiles window opens.
4. Click **User > Modify**. Type the new password and click **OK**.

Using the HMC remote command line

Provides information about using the command-line interface on the HMC.

The command-line interface is useful in the following situations:

- When consistent results are required. If you have to administer several managed systems, you can achieve consistent results by using the command-line interface. The command sequence can be stored in scripts and run remotely.
- When automated operations are required. After you have developed a consistent way to manage the managed systems, you can automate the operations by invoking the scripts from batch-processing applications, such as the **cron** daemon, from other systems.

This topic provides information about using the command line interface on the HMC.

For HMC command descriptions, see the HMC commands topic.

Viewing HMC remote command information

Describes the remote command line.

To view command information, type **man** and then the command name. For example, to learn more about the "Create a user for the HMC" (**mkhmcusr**) command, type the following at the command line:

```
man mkhmcusr
```

For HMC command descriptions, see the HMC commands topic.

Setting up secure script execution between SSH clients and the HMC

Describes how to ensure that the script executions between SSH clients and the HMC are secure.

Note: To enable scripts to run unattended between an **SSH** client and an HMC, the SSH protocol must already be installed on the client's operating system.

HMCs typically are placed inside the machine room where managed systems are located, so you might not have physical access to the HMC. In this case, you can remotely access it using either the remote client or the remote command-line interface. This topic describes how to ensure that your script executions between SSH clients and the HMC are secure.

To enable scripts to run unattended between an **SSH** client and an HMC, do the following:

1. In the Navigation area, select **HMC Management**.
2. In the Navigation area, click **HMC Configuration**.
3. In the Contents area, click **Enable/Disable Remote Command Execution**.
4. When the window opens, select the box to enable SSH.
5. Create an HMC user with one of the following roles:
 - super administrator
 - service representative
6. On the client's operating system, run the SSH protocol key generator. To run the SSH protocol key generator, do the following:
 - a. To store the keys, create a directory named `$HOME/.ssh` (either RSA or DSA keys can be used).
 - b. To generate public and private keys, run the following command:
`ssh-keygen -t rsa`

The following files are created in the `$HOME/.ssh` directory:

```
private key: id_rsa
public key: id_rsa.pub
```

The write bits for both group and other are turned off. Ensure that the private key has a permission of 600.

7. On the client's operating system, use `ssh` and run the **mkauthkeys** command to update the HMC user's `authorized_keys2` file on the HMC by using the following command:

```
ssh userid@hostname "mkauthkeys --add '<the key string from $HOME/.ssh/id_dsa.pub>'"
```

Deleting the key from the HMC

To delete the key from the HMC, select one of the following procedures:

You can use this procedure to delete the key from the HMC by modifying various files:

1. On the logical partition, use the **scp** command to copy the `authorized_keys2` file from the HMC to the logical partition, as follows:
`scp userid@host_name ~/.ssh/authorized_keys2 /tmp/mykeyfile`
2. In the `/tmp/mykeyfile` file, remove the line that contains the key and host name of the system that you want to be able to run HMC commands remotely.
3. On a logical partition, use the **scp** command to copy the new file to the HMC:
`scp /tmp/mykeyfile userid@host_name ~/.ssh/authorized_keys2`
4. If you want to enable password prompting for all hosts that access the HMC through **ssh**, use the **ssh** command to remove the key file from the HMC:
`scp userid@hostname:~/.ssh/authorized_keys2 authorized_keys2`
5. Edit the `authorized_keys2` file and remove all lines in this file, then copy it back to the HMC. For example:

```
scp authorized_keys joe@somehost:.ssh/authorized_keys2
```

OR

You can use the command line to delete the key from the HMC by using the **mkauthkeys** command. For example:

```
ssh userid@hostname "mkauthkeys --remove 'joe@somehost'"
```

Enabling and disabling HMC remote commands

Explains how to enable or disable the remote command-line interface access to the HMC using the SSH facility.

You can enable or disable the remote command-line interface access to the HMC using the SSH facility.

To enable or disable remote commands, you must be a member of one of the following roles:

- super administrator
- service representative

To enable or disable remote commands, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **HMC Configuration** icon.
3. In the Contents area, click **Enable/Disable Remote Command Execution**.
4. Select the appropriate check box.
5. Click **OK**.

To disable the firewall that is enabled by default, you must access the network settings on the HMC.

To disable the HMC firewall, see “Changing HMC firewall settings” on page 58.

Troubleshooting HMC setup

Troubleshoot common HMC setup problems.

The following topics contain information about common problems that might occur during the setup of the Hardware Management Console (HMC). The topics also contain common resolutions to those problems. The first topic applies to the HMC in general. The second topic applies to the remote client.

Setting up the HMC

Problem: You configured the HMC as a DHCP server, but the HMC did not automatically discover the managed system.

Resolution: This usually indicates that the managed system was connected to a power source before the HMC was configured as the DHCP server. This situation caused the managed system to initialize to its IP address to the default values (HMC1 as 192.168.2.147 and HMC2 as 192.168.3.147) instead of waiting for an address from the HMC.

To correct the configuration on the model 9118-575 server or the 590 or 595 managed servers, contact your service provider.

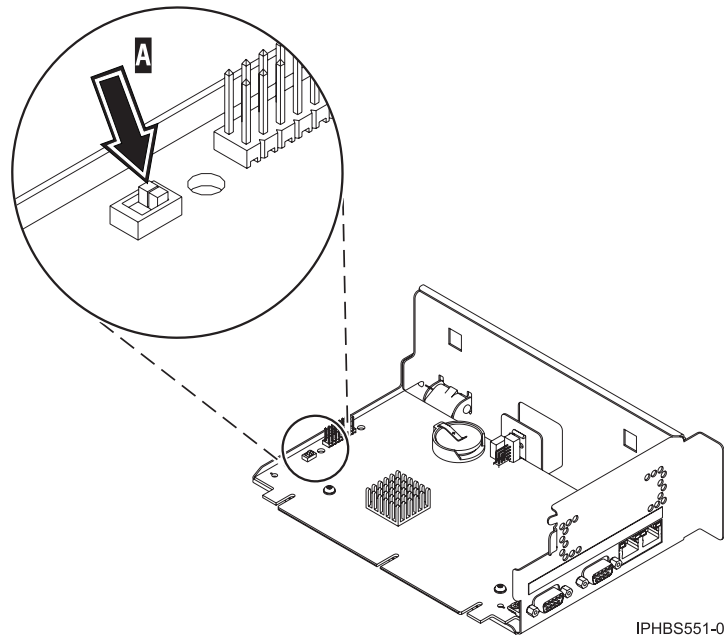
To correct the configuration for the model 520, 550, and 570 managed servers, complete the following tasks:

1. Shut down the managed system by pressing and holding the power button.
2. Remove the connection between the managed system and its power source.
3. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

If you had changed the IP address of the service processor using the ASM interface, use the appropriate procedure for your model:

Model 520

1. Shut down the managed system by pressing and holding the power button.
2. Remove the connection between the managed system and its power source.
3. Remove the connection between the HMC and its power source.
4. Remove the service processor assembly as instructed in the Remove the model 520 service processor assembly topic. Begin with the step following "Disconnect the power source...". When you have removed the service processor, proceed to the next step.
5. To reset the service processor assembly, move both service processor reset toggle switches **A** from their current position to the opposite position. See Figure 15.



IPHBS551-0

Figure 15. Model 520 service processor switch

6. Reinsert the service processor into the managed system. For instructions, see Replace the model 520 service processor assembly.
7. Reconnect the HMC to its power source and start the HMC.
8. Log in to the HMC.
9. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

Model 550:

1. Shut down the managed system by pressing and holding the power button.
2. Remove the connection between the managed system and its power source.
3. Remove the connection between the HMC and its power source.
4. The service processor switch is located beneath the second power supply. To access the service processor switch, you must remove the second power supply. For instructions, see Remove the model 550 power supply .
5. To reset the service processor, move the service processor reset toggle switch **A** from its current position to the opposite position. See Figure 16 on page 88.

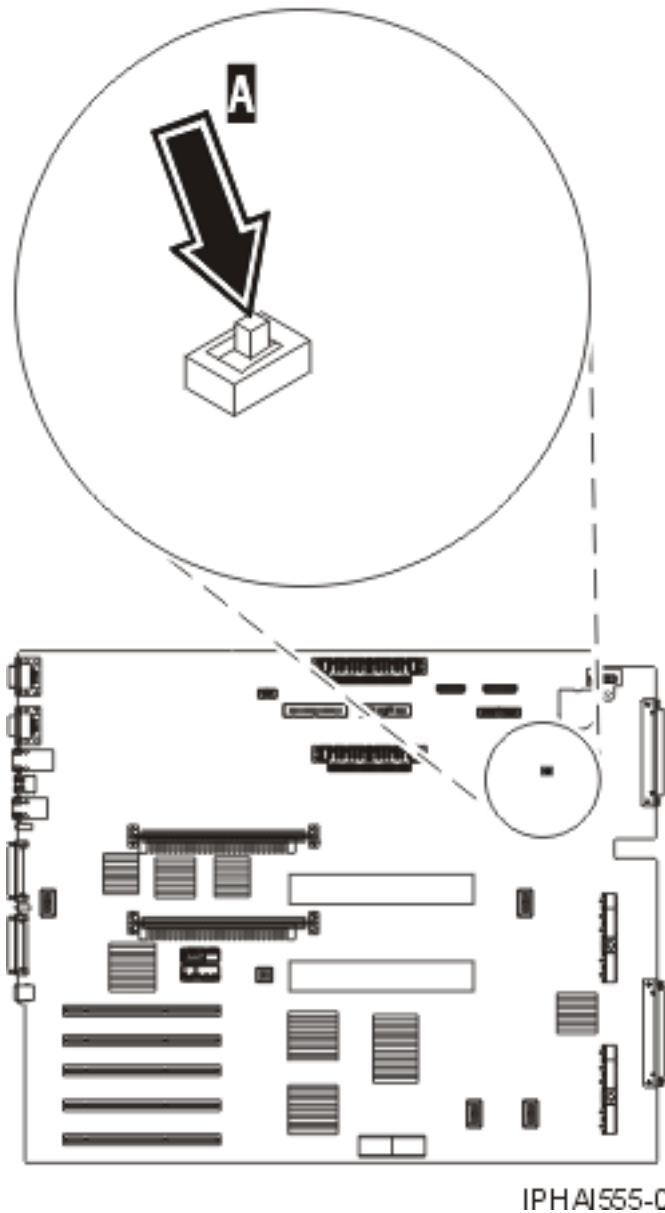


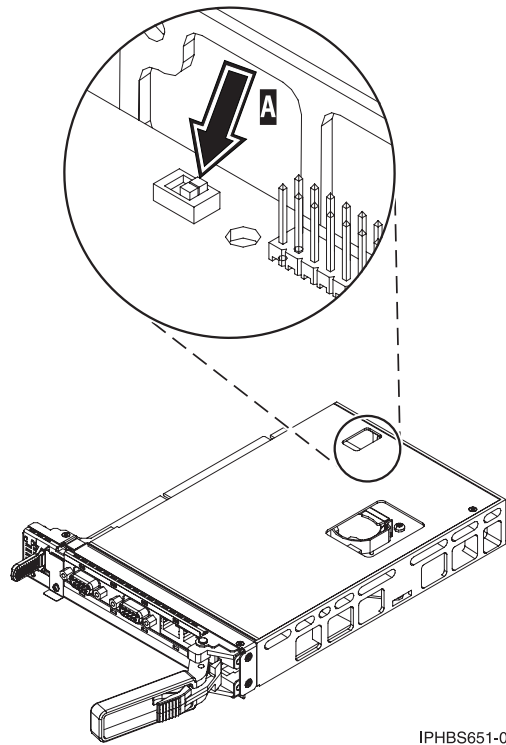
Figure 16. Model 550 service processor switch

6. Reinsert the power supply into the managed system. For instructions, see Replace the model 550 power supply.
7. Reconnect the HMC to its power source and start the HMC.
8. Log in to the HMC.
9. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

Model 570:

1. Shut down the managed system by pressing and holding the power button.
2. Remove the connection between the managed system and its power source.
3. Remove the connection between the HMC and its power source.

4. To remove the service processor assembly, follow the instructions in the Remove the model 570 service processor assembly topic. Begin with the step following "Disconnect the power source..." in the instructions. When you have removed the service processor, proceed to the next step.
5. Reset the service processor by moving both service processor reset jumpers **A** from their current position to the opposite position. See Figure 17.



IPHBS651-0

Figure 17. Model 570 service processor switch

6. Reinsert the service processor into the managed system. See Replace the model 570 service processor assembly.
7. Reconnect the HMC to its power source and start the HMC.
8. Log on to the HMC.
9. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

Problem: Obtaining Bulk Power Controller (BPC) or Flexible Service Processor (FSP) IP addresses in a private switched network using DHCP.

Resolution: Perform one the following tasks:

- If spanning tree is enabled on the switch and you want it to remain enabled, the portfast option must also be enabled. This setting will allow the switch to forward all packets from the port onto the LAN immediately and not check the spanning tree first.
- Disable the spanning tree on the switch for the BPC or FSP ports.

Note: Different manufacturers might use different terminology regarding these settings. The switch must be modified using portfast or other commands to accommodate connectivity delays. After validating the exact ports on the switch that the FSP or BPC is using, a network administrator must log in to the switch to make the changes to the specific ports.

Problem: After setting up the HMC, the managed system's status is Authentication Failed.

Resolution: This usually indicates that the managed system password was set prior to HMC

configuration. In this situation, the HMC does not recognize the managed system password and cannot access the managed system. To correct this situation, update the password on the managed system.

Installing the remote client

Problem: The `wsmlinuxclient.exe` or the `setupsec1.exe` file does not run.

Resolution: Modify the permissions on the file so that you have execute permissions. To modify the permissions, type the following command at the command prompt:

```
chmod 755 filename
```

Problem: Changes do not take effect immediately after installing the Web-based System Manager Remote Client or the remote client security on a Linux system

Resolution: Perform one of the following tasks:

- Log off your current session and log in again.
- Source your `./etc/profile` file.

Problem: You receive an error message that you cannot complete a connection

Resolution: You may receive a message that looks similar to the following:

Cannot complete connection to hostname *myhmc*.

Possible problems are:

1. Host *myhmc* is not a valid hostname.
2. Host *myhmc* is not currently operating or is not connected to the network.
3. Host *myhmc* is not running an operating system with a version of Web-based System Manager that is compatible with your client version of Web-based System Manager.
4. The time to connect could have exceeded the time limit set in the `websm.cfg` file (`remote_timeout`).
5. The `inetd` subsystem on host *myhmc* may not have been initialized on the 9090 port to start the WServer.

Additional information might be in the file `/var/websm/data/wserver.log` on host *myhmc*.

Possible solutions include the following tasks:

- The following reasons are most common for this message:
 - You might have exceeded the limit of remote connections allowed to the HMC you are trying to access remotely.
 - By default, the HMC uses a connect port of 9090 to handle the initial login communication. If you cannot enter your user ID and password, it means that you cannot connect to the 9090 port. Often this is because too many sessions were canceled incorrectly and the 9090 port is overloaded. Restart the HMC you are trying to access remotely to cancel remote sessions that were incorrectly disconnected.
- Log on to the HMC you are trying to access remotely and verify that *myhmc* is the host name of that HMC.
- Locate the HMC that you are trying to access remotely and verify that it is operating and connected to the network.
- Ensure that the version of the Web-based System Manager of the HMC you are trying to access remotely is the same version as the Web-based System Manager Remote Client.
- The time it takes for your remote client to connect to the HMC you want to manage remotely has exceeded the time limit. To solve this problem, improve your connection speed. To do this, you might have to change the way in which the remote client and the HMC you want to manage remotely are connected.

Performing a File System Check on HMC Reboot

Problem: Failed file system check (fsck) displays the following error message, "Enter the root password or hit Control-D to reboot."

Resolution: Perform the following task:


1. Type the root password.
2. Run a file-system check by entering *fsck file system* where *file system* is the name of the file system that fails the file system check. When the checking is done, a prompt window opens.
3. Type reboot or press Control-D.

Related information

View and print information related to the Adding the HMC topic collection.

Listed below are Web sites and information center topics that relate to the Managing the Hardware Management Console topic collection.

Web site

The Web-based System Manager Remote Client can be installed on AIX, Linux, or the HMC. For more information about installing and using Web-based System Manager on AIX, see the Web-based System Manager Administration Guide  (<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/topic/com.ibm.aix.wsmadmn/doc/wsmadmn/wsmadmn.htm>).

Other information


- Managing your server using the HMC
- Initial server setup
- Adding another console:
 - Advanced System Management Interface
 - Operations Console
 - Twinaxial console
- Customer service and support
- Migrating or upgrading your server
- HMC commands

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

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

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

The manufacturer may not offer the products, services, or features discussed in this document in other countries. Consult the manufacturer's representative for information on the products and services currently available in your area. Any reference to the manufacturer's product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any intellectual property right of the manufacturer may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any product, program, or service.

The manufacturer may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the manufacturer.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: THIS INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. The manufacturer may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to Web sites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this product and use of those Web sites is at your own risk.

The manufacturer may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning products not produced by this manufacturer was obtained from the suppliers of those products, their published announcements or other publicly available sources. This manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products not produced by this manufacturer. Questions on the capabilities of products not produced by this manufacturer should be addressed to the suppliers of those products.

All statements regarding the manufacturer's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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
eServer
i5/OS
OpenPower
IBM
iSeries
pSeries
System i
System i5
System p
System p5

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

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

Regulatory 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 meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

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.

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 is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

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

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.

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.

Radio Protection for Germany

Dieses Gerät ist berechtigt in Übereinstimmung mit Dem deutschen EMVG vom 9.Nov.92 das EG-Konformitätszeichen zu führen.

Der Aussteller der Konformitätserklärung ist die IBM Germany.

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse A. Für diese von Geräten gilt folgende Bestimmung nach dem EMVG:

Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.

(Auszug aus dem EMVG vom 9.Nov.92, Para.3, Abs.4)

Hinweis

Dieses Genehmigungsverfahren ist von der Deutschen Bundespost noch nicht veröffentlicht worden.

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 meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to CISPR 22 / European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Properly shielded and grounded cables and connectors 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.

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.

Electromagnetic Interference (EMI) Statement - Korea

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

Radio Protection for Germany

Dieses Gerät ist berechtigt in Übereinstimmung mit Dem deutschen EMVG vom 9.Nov.92 das EG-Konformitätszeichen zu führen.

Der Aussteller der Konformitätserklärung ist die IBM Germany.

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse B. Für diese von Geräten gilt folgende Bestimmung nach dem EMVG:

Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.

(Auszug aus dem EMVG vom 9.Nov.92, Para.3, Abs.4)

Hinweis

Dieses Genehmigungsverfahren ist von der Deutschen Bundespost noch nicht veröffentlicht worden.

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.

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>.



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.



IBM Cryptographic Coprocessor Card Return Program

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>.



Printed in USA