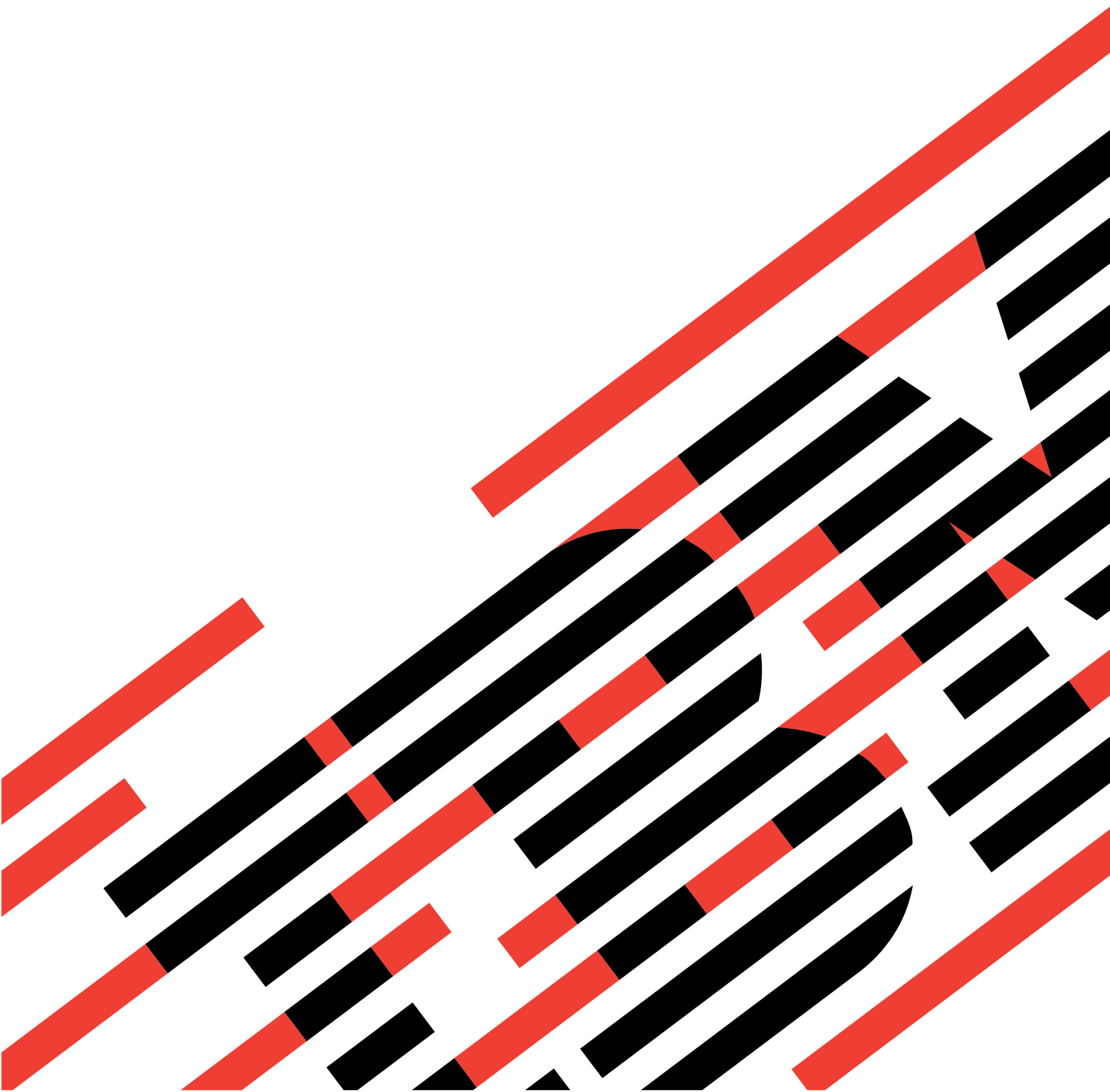




BladeCenter Management Module

User's Guide





@server

BladeCenter Management Module

User's Guide

Note: Before using this information and the product it supports, read the general information in “Notices” on page 33.

Third Edition (August 2003)

© Copyright International Business Machines Corporation 2002, 2003. All rights reserved.

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

Contents

Safety	v
Introducing the BladeCenter management module	1
Management module controls and indicators	2
Management module input/output connectors	3
Video connector	3
Keyboard connector	3
Mouse connector	4
Remote management and console Ethernet connector	4
Configuring the management module and BladeCenter unit	4
Setting up the remote connection	6
Using the management and configuration program	8
Configuring SNMP	29
Saving and restoring the configuration file	31
Notices	33
Edition notice	33
Trademarks	34
Important notes	34
Product recycling and disposal	35
Battery return program	35
Electronic emission notices	36
Federal Communications Commission (FCC) statement	36
Industry Canada Class A emission compliance statement	36
Australia and New Zealand Class A statement	36
United Kingdom telecommunications safety requirement	36
European Union EMC Directive conformance statement	36
Taiwanese Class A warning statement	37
Chinese Class A warning statement	37
Japanese Voluntary Control Council for Interference (VCCI) statement	37
Power cords	37
Index	41

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 **Safety Information** (安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítajte Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

Statement 1:



DANGER

Electrical current from power, telephone, and communication cables is 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.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **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 in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	To Disconnect:
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 8:



CAUTION:

Never remove the cover on a power supply or any part that has the following label attached.



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

WARNING: Handling the cord on this product or cords associated with accessories sold with this product, will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

ADVERTENCIA: El contacto con el cable de este producto o con cables de accesorios que se venden junto con este producto, pueden exponerle al plomo, un elemento químico que en el estado de California de los Estados Unidos está considerado como un causante de cancer y de defectos congénitos, además de otros riesgos reproductivos. ***Lávese las manos después de usar el producto.***

Introducing the BladeCenter management module

This *Management Module User's Guide* contains information about configuring the management module and managing the IBM® @server BladeCenter™ unit and blade servers.

Your BladeCenter unit comes with one hot-swap management module in management bay 1. You can add a management module in management bay 2.

Notes:

1. Only one management module will be active, or primary; the second management module, if present, provides redundancy.
2. When two management modules are installed in the BladeCenter unit, both management modules must always have the same level of firmware, which must be a level that supports redundant management modules, to ensure smooth changeover from the active module to the redundant module. Go to the IBM Support Web site at <http://www.ibm.com/pc/support/> and obtain the latest level of firmware.

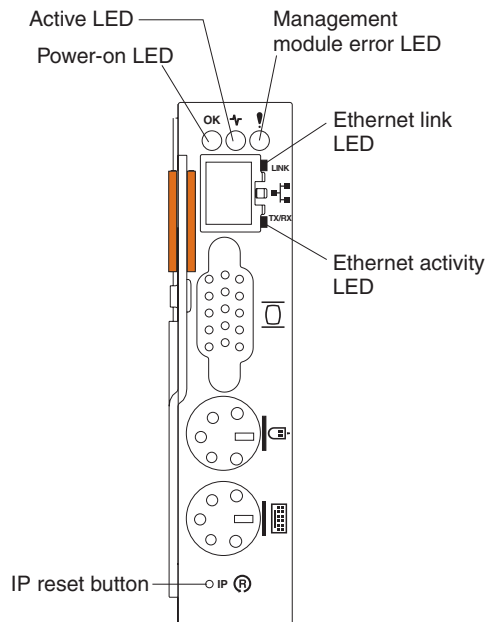
The management module functions as a service processor and a keyboard/video/mouse (KVM) multiplexor for the multiple blade servers. You configure the BladeCenter unit and modules through the management module, configuring such information as the switch module IP addresses. The management module provides the following external connections: keyboard, mouse, and video for use by a local console, and one RJ-45 connector for a 10/100 Mbps Ethernet remote management connection.

The service processor in the management module communicates with the service processor in each blade server for such functions as:

- Blade server power-on requests
- Blade server error and event reporting
- Blade server requests for keyboard, mouse, and video
- Blade server requests for diskette drive, CD-ROM drive, and USB port

The management module also communicates with the I/O modules, power modules, blower modules, and blade servers in the BladeCenter unit to detect their presence or absence and any error conditions, sending alerts when required.

Management module controls and indicators



Management module LEDs: These LEDs provide status information about the management module and remote management connection. For additional information, see the “Light Path Diagnostics” section in the *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *BladeCenter Documentation CD*.

- **Power-on:** When this green LED is lit, the management module has power.
- **Active:** When this green LED is lit, it indicates that this management module is actively controlling the BladeCenter unit.

Note: Only one management module actively controls the BladeCenter unit. If there are two management modules installed in the BladeCenter unit, this LED is lit on only one.

- **Management module error:** When this amber LED is lit, it indicates that an error has been detected somewhere on this management module. When this indicator is lit, the system error LED on each of the BladeCenter system LED panels is also lit.
- **Ethernet link:** When this green LED is lit, there is an active connection through the port to the network.
- **Ethernet activity:** When this green LED is flashing, it indicates that there is activity through the port over the network link.

Management module IP reset button: Do not press this button unless you intend to erase your configured IP addresses for the management module and lose connection with the remote management station, the I/O modules, and the blade servers. If you press this button, you will need to reconfigure the management module settings (see the information beginning with “Setting up the remote connection” on page 6 for instructions).

Press this recessed button to reset the IP configuration of the management module network interfaces (Ethernet 1, Ethernet 2, gateway address, and so forth) to the factory defaults and then restart the management module.

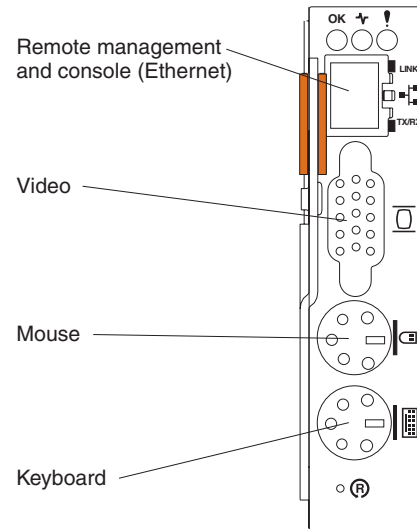
Use a straightened paper clip to press the button.

Management module input/output connectors

The management module has the following I/O connectors:

- One video
- One PS/2[®] keyboard
- One PS/2 mouse
- One 10/100 Mbps Ethernet for remote console and management

The following illustration shows the I/O connectors on the management module.

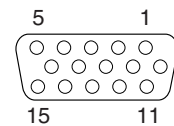


Note: See the *IBM BladeCenter Management Module Installation Guide* for information about how to cable two management modules.

Video connector

Your BladeCenter management module contains one standard video connector. The integrated video controller on each blade server is compatible with SVGA and VGA and communicates through this video port.

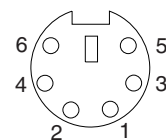
Use this connector to connect a video monitor to the BladeCenter unit.



Keyboard connector

Your BladeCenter management module contains one PS/2-style keyboard connector.

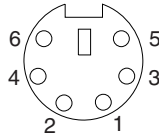
Use this connector to connect a PS/2 keyboard to the BladeCenter unit.



Mouse connector

Your BladeCenter management module contains one PS/2-style mouse connector.

Use this connector to connect a PS/2 mouse to the BladeCenter unit.



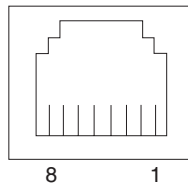
Remote management and console Ethernet connector

Your BladeCenter management module contains one 10/100 Mb Ethernet connector that provides the remote connection to the network management station on the network.

Use this port for remote management and remote console.

The network management station, through this port, can access control functions running in the service processor on each blade server or within each switch module. However, it cannot use this port to communicate with application programs running in the blade servers. The network management station must direct those communications through a network connected to the external ports in the I/O modules in the BladeCenter unit.

The following illustration shows the Ethernet connector that is on the management module.



Configuring the management module and BladeCenter unit

Important

You configure only the primary (active) management module. The secondary management module receives the configuration and status information automatically from the primary management module when necessary. The configuration information in this chapter applies to the primary or only management module in the BladeCenter unit.

When the BladeCenter unit is started initially, it automatically configures the remote management port on the active (primary) management module, so that you can configure and manage the BladeCenter unit and blade servers. You configure and manage the BladeCenter unit remotely, through the management module, using the Web-based user interface.

Note: You can also configure the switch modules directly through an external switch module port, using a Telnet interface or a Web browser. See the documentation that comes with the switch module for more information.

For the management module to communicate with the I/O modules in the BladeCenter unit, you will need to configure the IP addresses for the following internal and external ports:

- The external Ethernet (remote management) port on the management module (see the information beginning on page 24 for instructions). The initial management module autoconfiguration enables the network management station to connect to the management module to configure the port completely and to configure the rest of the BladeCenter unit.
- The internal Ethernet port on the management module for communication with the I/O modules (see the information beginning on page 24 for instructions).
- The management port on each switch module, for communication with the management module (see the information beginning on page 21 for instructions). You configure this port by configuring the IP address for the switch module.

Note: Some types of I/O modules, such as the pass-thru module, have no management port.

To communicate with the blade servers for functions such as deploying an operating system or application program, you also will need to configure at least one external (in-band) port on an Ethernet switch module in I/O module bay 1 or 2. See the *IBM @server BladeCenter Type 8677 Installation and User's Guide* for information about configuring external ports on Ethernet switch modules.

Note: If a pass-thru module is installed in I/O-module bay 1 or 2 (instead of an Ethernet switch module), you will need to configure the network switch that the pass-thru module is connected to; see the documentation that comes with the network switch.

The management module supports the following Web browsers for remote access. The Web browser that you use must be Java-enabled, must support JavaScript 1.2 or later, and must have the Java 1.4.1 Plug-In installed.

- Microsoft® Internet Explorer 4.0 (with Service Pack 1), or later
- Netscape Navigator 4.72, or later (version 6.x is not supported)

Notes:

1. For best results when using the Web browser, set the resolution on your monitor to 800 x 600 pixels or higher and 256 colors.
2. The Web interface does not support the double-byte character set (DBCS) languages.

The Web-based user interface communicates with the management and configuration program that is part of the firmware that comes with the management module. You can use this program to perform tasks such as:

- Defining the login IDs and passwords
- Selecting recipients for alert notification of specific events
- Monitoring the status of the BladeCenter unit and blade servers
- Controlling the BladeCenter unit and blade servers
- Accessing the I/O modules to configure them
- Changing the drive startup sequence in a blade server

- Setting the date and time
- Using a remote console for the blade servers
- Changing ownership of the keyboard, video, and mouse
- Changing ownership of the CD-ROM drive, diskette drive, and USB port
- Activating On Demand blade servers

Note: The IBM Director program is a system-management product that comes with the BladeCenter unit. To configure the remote alert recipients for IBM Director over LAN, the remote alert recipient must be an IBM Director-enabled server.

You also can use the management and configuration program to view some of the blade server configuration settings. See “Using the management and configuration program” on page 8 for more information.

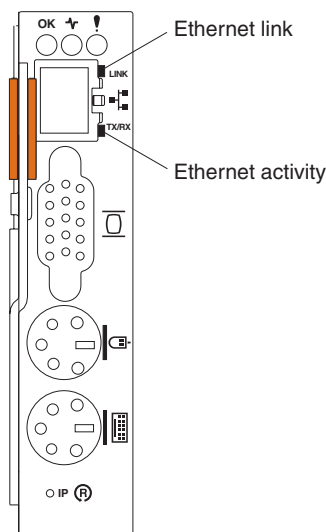
Setting up the remote connection

To configure and manage the BladeCenter unit and blade servers, you must first set up the remote connection through the external Ethernet port on the management module.

Cabling the Ethernet port

Complete the following steps to connect the Ethernet cable to the management module:

1. Connect one end of a Category 5 or higher Ethernet cable to the Ethernet port on the management module. Connect the other end of the Ethernet cable to the network.
2. Check the Ethernet LEDs to ensure that the network connection is working. The following illustration shows the locations of the Ethernet LEDs.



Ethernet link LED

When this green LED is lit, there is an active connection through the port to the network.

Ethernet activity LED

When this green LED is flashing, it indicates that there is activity through the port over the network link.

Configuring the management module for remote access

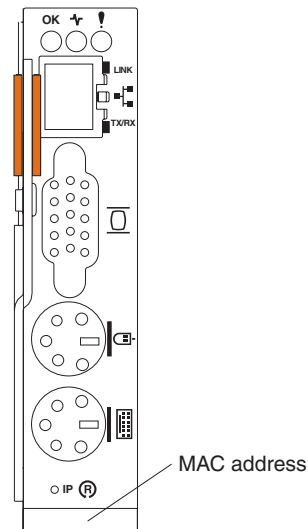
After you connect the active management module to the network, the Ethernet port connection is configured in one of the following ways:

- If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, the host name, IP address, gateway address, subnet mask, and DNS server IP address are set automatically.
- If the DHCP server does not respond within 2 minutes after the port is connected, the management module uses the static IP address and subnet address.

Either of these actions enables the Ethernet connection on the active management module.

Make sure your computer is on the same subnet as the management module, and use your Web browser to connect to the management module (see “Starting the management and configuration program” on page 8 for more information). In the browser **Address** field, specify the IP address the management module is using:

- If the IP address was assigned through a DHCP server, get the IP address from your network administrator.
- The factory-defined static IP address is 192.168.70.125, the default subnet address is 255.255.255.0, and the default host name is MMxxxxxxxxxxxx, where xxxxxxxxxxxx is the burned-in medium access control (MAC) address. The MAC address is on a label on the management module, below the IP reset button.



Note: If the IP configuration is assigned by the DHCP server, the network administrator can use the MAC address of the management module network interface to find out what IP address and host name are assigned.

Communicating with the IBM Director software

The IBM Director program is a system-management product that comes with the BladeCenter unit. The IBM Director software communicates with the BladeCenter unit through the Ethernet port on the active management module.

Note: See the IBM Support Web site at <http://www.ibm.com/pc/support/> for the version of IBM Director software that you can use to manage redundant management modules.

To communicate with the BladeCenter unit, the IBM Director software needs a managed object (in the Group Contents pane of the IBM Director Management Console main window) that represents the BladeCenter unit. If the BladeCenter management module IP address is known, the network administrator can create an IBM Director managed object for the unit. If the IP address is not known, the IBM Director software can automatically discover the BladeCenter unit (out-of-band, using the Ethernet port on the BladeCenter management module) and create a managed object for the unit.

For the IBM Director software to discover the BladeCenter unit, your network must initially provide connectivity from the IBM Director server to the BladeCenter management-module Ethernet port. To establish connectivity, the management module attempts to use DHCP to acquire its initial IP address for the Ethernet port. If the DHCP request fails, the management module uses the static IP address assigned to it. Therefore, the DHCP server (if used) must be on the management LAN for your BladeCenter unit.

Notes:

1. All management modules are preconfigured with the same static IP address. You can use the management module Web interface to assign a new static IP address for each BladeCenter unit. If DHCP is not used and you do not assign a new static IP address for each BladeCenter unit before attempting to communicate with the IBM Director software, only one BladeCenter unit at a time can be added onto the network for discovery. Adding multiple units to the network without a unique IP address assignment for each BladeCenter unit results in IP address conflicts.
2. For switch communication with the IBM Director server through the management module external Ethernet port, the switch module internal network interface and the management module internal and external interfaces must be on the same subnet.

Using the management and configuration program

This section provides instructions for using the management and configuration program in the active management module.

Starting the management and configuration program

Complete the following steps to start the management and configuration program:

1. Open a Web browser. In the address or URL field, type the IP address or host name assigned for the management module remote connection (see “Configuring the management module for remote access” on page 7 for more details).

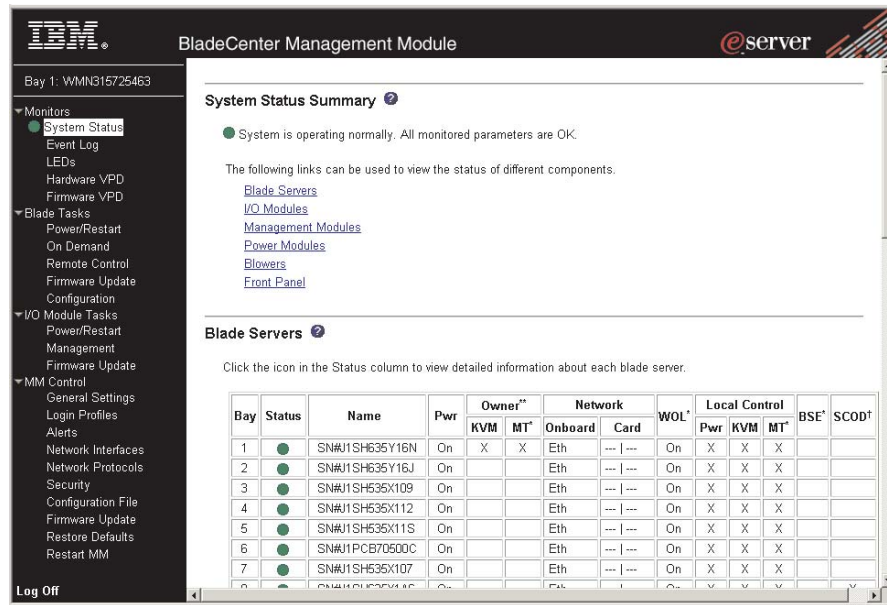
The Enter Network Password window opens.

2. Type your user name and password. If you are logging in to the management module for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log.

Note: The initial user ID and password for the management module are:

- User ID: USERID (all capital letters)
 - Password: PASSWORD (note the zero, not O, in PASSWORD)
3. Follow the instructions that appear on the screen. Be sure to set the timeout value you want for your Web session.

The BladeCenter management and configuration window opens.



Note: The upper left corner of the management and configuration window shows the location and identity of the active management module.



Management and configuration program options

From the management and configuration program main menu, you can select settings that you want to view or change.

The navigation pane (on the left side of the management module window) contains navigational links that you use to manage your BladeCenter unit and check the status of the components (modules and blade servers). Descriptions of the links are as follows:

Monitors

Use the choices in this section to view the status, settings, and other information for components in the BladeCenter unit.










System status

The following links can be used to view the status of different components.

[Blade Servers](#)
[I/O Modules](#)
[Management Modules](#)
[Power Modules](#)
[Blowers](#)
[Front Panel](#)

Blade Servers

Click the icon in the Status column to view detailed information about each blade server.

Bay	Status	Name	Pwr	Owner**		Network		WOL*	Local Control			BSE*	SCOD†
				KVM	MT*	Onboard	Card		Pwr	KVM	MT*		
1		SN#J1SH635Y16N	On	X	X	Eth	--- ---	On	X	X	X		
2		SN#J1SH635Y16J	On			Eth	--- ---	On	X	X	X		
3		SN#J1SH535X109	On			Eth	--- ---	On	X	X	X		
4		SN#J1SH535X112	On			Eth	--- ---	On	X	X	X		
5		SN#J1SH535X11S	On			Eth	--- ---	On	X	X	X		
6		SN#J1PCB70500C	On			Eth	--- ---	On	X	X	X		
7		SN#J1SH535X107	On			Eth	--- ---	On	X	X	X		
8		SN#J1SH635X1A6	On			Eth	--- ---	On	X	X	X		X
9		SN#J1SH7365118	On			Eth	--- ---	On	X	X	X		X

Select this choice to view the overall system status, a list of outstanding events that require immediate attention, and the overall status of each of the blade servers and I/O modules.

Blade Servers:

- **Bay** - The lowest-number bay the blade server occupies.
- **Status** - An icon that indicates good, warning, or bad status for the blade server. Click the icon for more detailed status information.
- **Name** - The name of the blade server.
- **Pwr** - The power state (on or off) of the blade server.
- **Owner** - An indication of whether the blade server is the current owner of the following BladeCenter resources:
 - **KVM** - Keyboard, video, and mouse.
 - **MT** - The CD-ROM drive, diskette drive, and USB port.
- **Network** - An indication of which network interfaces are on the blade server and the I/O expansion option. For example, eth/fibre indicates that the blade server has Ethernet controllers on the system board and a Fibre Channel I/O expansion option.
- **WOL** - An indication of whether the Wake on LAN[®] feature is currently enabled for the blade server. The Wake on LAN feature is enabled by default in blade server BIOS code and cannot be disabled. The BladeCenter management module provides a single point of control for the Wake on LAN feature, enabling the settings to be controlled for either the entire BladeCenter unit or a single blade server. Wake on LAN settings made in the management module override the settings in the blade server BIOS code.
- **Local Control** - An indication of whether the following options are enabled:
 - Local power control
 - Local keyboard, video, and mouse switching

- Local CD-ROM drive, diskette drive, and USB port switching
- **BSE** - An indication of whether a SCSI expansion unit occupies the blade bay.
- **SCOD** - An indication of whether the blade server is an On Demand blade server with a Standby status. You cannot turn on an On Demand blade server until you activate it (**Blade Tasks** → **On Demand**), which changes the status from Standby to Active.

Note: You must contact IBM within 14 calendar days after you activate an On Demand blade server. See your *Agreement for Standby Capacity on Demand* for additional information.

I/O modules:

- **Bay** - The number of the bay the I/O module occupies.
- **Status** - An icon that indicates good, warning, or bad status for the I/O module.
- **Type** - The type of I/O module in the bay, such as Ethernet switch, Fibre Channel switch, or pass-thru.
- **MAC Address** - The medium access control (MAC) address of the I/O module.

Note: Some types of I/O modules, such as a pass-thru module, have no MAC address nor IP address.

- **IP Address** - The IP address of the I/O module.
- **Pwr** - The power state (on or off) of the I/O module.
- **Details** - Text information about the status of the I/O module.

Management module:

- **Bay** - The number of the bay that the management module occupies.
- **Status** - An icon that indicates good, warning, or critical status for the management module. Click the icon for more detailed status information.
- **IP Address** - The IP address of the remote connection (external Ethernet port) on the management module.
- **Primary** - An indication of which management module is the primary, or active, management module.

Power Modules:

- **Bay** - The number of the bay that the power module occupies.
- **Status** - An icon that indicates good, warning, or critical status for the power module.
- **Details** - Text information about the status of the power module.

Blowers:

- **Bay** - The number of the bay that the blower module occupies.
- **Status** - An icon that indicates good, warning, or critical status for the blower module.
- **Speed** - The current speed of the blower module, as a percentage of the maximum revolutions per minute (RPMs). The

blower speed varies with the thermal load. An entry of `Offline` indicates that the blower is not functioning.

Front panel: The temperature status for the front of the BladeCenter unit.

Event log

The screenshot shows the 'Event Log' window with the following components:

- Monitor log state events:**
- Filter Section:**

Severity	Source	Date
E Error	BLADE_D2	06/23/03
W Warning	BLADE_D5	
I Info	SERVPROC	
- Note:** Hold down Ctrl to select more than one option. Hold down Shift to select a range of options.
- Filters:** None
- Event Log Table:**

Index	Sev	Source	Date/Time	Text
1	E	BLADE_D2	06/23/03, 06:16:06	(IBM 867821X SN1) Hard Drive 2 Fault
2	E	BLADE_D5	06/23/03, 06:15:08	(SN#J1RNE34911N) POSTBIOS: 162 Configuration Change Has Occurred
3	E	BLADE_D5	06/23/03, 06:15:08	(SN#J1RNE34911N) POSTBIOS: 1762 Configuration Change Has Occurred
4	I	SERVPROC	06/23/03, 06:14:10	User USERID attempting to restart blade in bay 2.
5	I	SERVPROC	06/23/03, 06:13:55	User USERID attempting to restart blade in bay 5.
6	I	SERVPROC	06/23/03, 06:13:41	System log cleared.
End of Log.				
- Buttons:** Clear Log, Save Log as Text File

Select this choice to view entries that are currently stored in the management module event log. This log includes entries for events that are detected by the blade servers. The log displays the most recent entries first. Information about all remote access attempts is recorded in the event log, and the management module sends out the applicable alerts if configured to do so.

The maximum capacity of the event log is 750 entries. When the log is 75 percent full, the BladeCenter Information LEDs light. When the log is full, new entries overwrite the oldest entries, and the BladeCenter Error LEDs light. If you do not want the management module to monitor the state of the event log, deselect the **Monitor log state events** checkbox at the top of the event log page.

You can sort and filter entries in the event log. See the event log help for more information.

LEDs

The screenshot displays two sections of the BladeCenter management interface:

Front and Rear Panel LEDs

LED	Status	Action
System error		
Information		Off
Temperature		
Location		On Off Blink

Blade Server LEDs

Bay	Name	Pwr ²	Error	Information	KVM	MT	Location		
1	No blade present								
2	IBM 867821X SN1	On			Off				On Off Blink
3									
4	No blade present								
5	SN#J1RNE34911N	On			Off				On Off Blink
6	No blade present								
7	No blade present								
8	No blade present								
9	No blade present								
10	No blade present								
11	No blade present								

Select this choice to view the state of the BladeCenter system LED panel and blade server control panel LEDs. You also can use this choice to turn off the information LED and turn on, turn off, or blink the location LED on the BladeCenter unit and the blade servers.

- **Front Panel LEDs** - The state of the following LEDs on the BladeCenter system LED panel. You can change the state of the information and location LEDs.
 - System error
 - Information
 - Over temperature
 - Location
- **Blade Server LEDs** - The state of the following LEDs on the blade server control panel. You can change the state of the information and location LEDs.
 - Power
 - Error
 - Information
 - Keyboard, video, and monitor select
 - Media (CD-ROM, diskette drive, USB port) select
 - Location

Hardware VPD

BladeCenter System VPD

Type / Model	86771XX
Serial no.	23A0016
UUID	A7FB FB81 DB12 11D6 8D71 C8D6 4BF2 ED0C

[Edit BladeCenter System VPD](#)

BladeCenter Hardware VPD

Move your mouse pointer over a module name to see a description for that module in the status bar of your browser.

Bay(s)	Module Name	Manuf. ID	Machine Type/Model	Machine Serial No.	Hardware Revision	Manuf. Date	Part Number	FRU Number
Chassis and Media Tray								
	Chassis	----	1X23AD	16	04	----	091 59P6	609 27TR
1	Media Tray	----	n/a	n/a	03	3402	32P1936	59P6629
Blade Servers								
2-3	IBM 867821X SN1	SLRM	867821X	23A0016	06	3202	02R1011	59P6610
	Daughter Card	----	n/a	n/a	00	----	48	----
	DASD Daughter Card	----	n/a	n/a	20	----	----	----
5	SN#J1RNE34911N	SLRM	883211Z	23K5202	23	1503	73P9046	71P8857
I/O Modules								
1	Ethernet SM	DLNK	n/a	n/a	02	0000	01R0807	59P6620

Select this choice to view the hardware vital product data (VPD) for the BladeCenter unit. When the BladeCenter unit is started, the management module collects the vital product data and stores it in nonvolatile memory. The management module then modifies the stored VPD as components are added to or removed from the BladeCenter unit. You can also view the log of modules inserted or removed from the BladeCenter unit.

Firmware VPD

Blade Server Firmware VPD

Bay(s)	Name	Firmware Type	Build ID	Released	Revision
2-3	IBM 867821X SN1	BIOS	BRE118AUS	02/13/2003	1.02
		Diagnostics	BRYT04AUS	07/19/2002	1.00
		Blade sys. mgmt. proc.	BR8T14A	n/a	14
5	SN#J1RNE34911N	BIOS	BSE101AUS	04/04/2003	1.00
		Diagnostics	BSYT06AUS	05/01/2003	1.00
		Blade sys. mgmt. proc.	BR8T15A	n/a	15

I/O Module Firmware VPD

Bay	Type	Firmware Type	Build ID	Released	Revision
1	Ethernet SM	Boot ROM	BRESMB4G	01/29/2003	04
		Main Application 1	BRESMR4G	01/29/2003	59

Management Module Firmware VPD

Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	Redundant MM	Main application	BRETZD+	CNETMNU5.PKT	06-18-03	16
		Boot ROM	BRBRZD+	CNETBRUS.PKT	06-15-03	16
		Remote control	BRRGZD+	CNETRGUS.PKT	06-19-03	16
		PS/2 to USB conv.	BREZ14	DUALPS2.PKT	12-03-02	1
		MM to USB intf.	BRPI14	REMODEKM.PKT	11-27-02	1
2	MM#B37CC7034	Main application	BRETZD+	CNETMNU5.PKT	06-18-03	16

Select this choice to view the vital product data (VPD) for the firmware in all blade servers, the I/O modules and the management modules in the BladeCenter unit. The firmware VPD identifies the firmware type, build ID, release date, and revision number. The VPD for the firmware in the management modules includes the file

name of the firmware components. (Selecting this choice takes up to 30 seconds to refresh and display information.)

Blade tasks

Select the choices in this section to view and change the settings or configurations of blade servers in the BladeCenter unit.

Power/restart

Blade Power / Restart

Click the checkboxes in the first column to select one or more blade servers; then, click one of the links below the table to perform the desired action.

<input type="checkbox"/>	Bay	Name	Pwr	Local Pwr Control	Wake on LAN	Console Redirect	SCOD [†]
<input type="checkbox"/>	1	SN#J1SH635Y16N	On	Enabled	On		
<input type="checkbox"/>	2	SN#J1SH635Y16J	On	Enabled	On		
<input type="checkbox"/>	3	SN#J1SH535X109	On	Enabled	On		
<input type="checkbox"/>	4	SN#J1SH535X112	On	Enabled	On		
<input type="checkbox"/>	5	SN#J1SH535X11S	On	Enabled	On		
<input type="checkbox"/>	6	SN#J1PCB70500C	On	Enabled	On		
<input type="checkbox"/>	7	SN#J1SH535X107	On	Enabled	On		
<input type="checkbox"/>	8	SN#J1SH635X1A6	On	Enabled	On		X
<input type="checkbox"/>	9	SN#J1SH7365118	On	Enabled	On		X
<input type="checkbox"/>	10	SN#J1SH535X108	On	Enabled	On		X
<input type="checkbox"/>	11	Lrl 6511-4	On	Enabled	On		X
<input type="checkbox"/>	12	SN#J1SH535X11N	On	Enabled	On		X
<input type="checkbox"/>	13	SN#J1SH535X126	On	Enabled	On		X
<input type="checkbox"/>	14	SN#J1SH535X11B	On	Enabled	On		X

[†] SCOD = Standby Capacity on Demand

Select this choice to perform the following actions on any blade server in the BladeCenter unit.

Note: You cannot perform these actions on an On Demand blade server with a Standby status (identified by an X in the SCOD column). To activate an On Demand blade server, see the **On Demand** choice under **Blade Tasks** and follow the instructions.

- Turn on or turn off the selected blade server (set the power state on or off).
- Enable or disable local power control. When local power control is enabled, a local user can turn on or turn off the blade server by pressing the power-control button on the blade server.
- Enable or disable the Wake on LAN feature.
- Restart the blade server or the service processor in the blade server.

Select the blade servers on which you want to perform an action; then, click the appropriate link below the table for the action you want to perform.

On Demand

On Demand Blade Activation ?

Click the checkboxes in the first column to select one or more On Demand blade servers that have a Standby status; then, click the 'Activate Standby Blade Servers' link below to activate the selected blade servers.

Note: You must contact IBM within 14 calendar days after you activate an On Demand blade server. See your Attachment for Standby Capacity on Demand for additional information.
Activating an On Demand blade server restarts the Blade System Management Processor on the blade server. It will take a few minutes for the status of the activated blade server to change from Standby to Active.

Select	Bay	Name	On Demand
<input type="checkbox"/>	1	SN#J1SH635Y16N	N/A
<input type="checkbox"/>	2	SN#J1SH635Y16J	N/A
<input type="checkbox"/>	3	SN#J1SH535X109	N/A
<input type="checkbox"/>	4	SN#J1SH535X112	N/A
<input type="checkbox"/>	5	SN#J1SH535X11S	N/A
<input type="checkbox"/>	6	SN#J1PCB70500C	N/A
<input type="checkbox"/>	7	SN#J1SH535X107	N/A
<input type="checkbox"/>	8	SN#J1SH635X1A6	Standby
<input type="checkbox"/>	9	SN#J1SH7365118	Standby
<input type="checkbox"/>	10	SN#J1SH535X108	Standby
<input type="checkbox"/>	11	Lrl 6511-4	Standby
<input type="checkbox"/>	12	SN#J1SH535X11N	Standby
<input type="checkbox"/>	13	SN#J1SH535X126	Standby
<input type="checkbox"/>	14	SN#J1SH535X11B	Standby

[Activate Standby Blade Servers](#)

Select this choice to activate an On Demand blade server with Standby status. You must activate an On Demand blade server with Standby status before you can turn it on. When you activate an On Demand blade server, its status changes from Standby to Active and the blade server is available for use.

Select the check boxes in the first column for one or more On Demand blade servers that have a Standby status; then, click the **Activate Standby Blade Servers** link to activate the selected blade servers.

Note: You must contact IBM within 14 calendar days after you activate an On Demand blade server. See your *Agreement for Standby Capacity on Demand* for additional information.

Remote control

Remote Control Status ?

KVM owner:	Blade2 - IBM 867821X SN1 since 06/22/2003 17:53:15
Media tray owner:	Blade2 - IBM 867821X SN1 since 06/24/2003 17:09:43
Console redirect:	In progress by USERID at 160.0.0.42 since 06/23/2003 07:12:43

Redirect Server Console ?

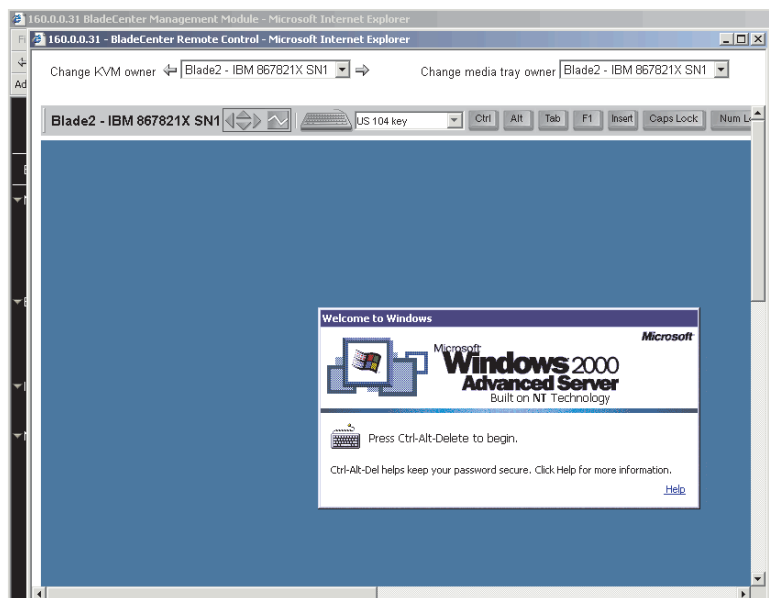
To disable the buttons located on the blade servers for KVM and media tray switching, check the boxes below and click "Save". Click "Redirect Server Console" to start a console redirect session. This session will allow you to access the video console of the KVM owner blade and have full keyboard and mouse control. You can also change KVM and media tray ownership during this session.

Note: An Internet connection is required to download the Java Runtime Environment (JRE) if the Java 1.4 Plug-in is not already installed.

Disable local KVM switching
 Disable local media tray switching

Select this choice to:

- View and change the current owners of the keyboard, monitor, and mouse (KVM), and of the CD-ROM drive, diskette drive, and USB port (Media tray).
- View the details of any remote control session currently active (user ID, client IP address, start time).
- Disable local switching of the KVM and of the media tray for all blade servers until they are explicitly enabled again. This prevents a local user from switching the console display to a different blade server while you are performing remote control tasks.
- Redirect a blade server console to the remote console.



On the remote console, you can:

- View the current blade server display.

- Change the owner of the KVM and of the media tray to the blade server you need to view.
- Control the blade server as if you were at the local console, including restarting the blade server and viewing the POST process, with full keyboard and mouse control.

Remote console keyboard support includes all keys. Icons are provided for keys that might have a special meaning to the blade server. For example, to transmit Ctrl-Alt-Del to the blade server, you must click the Ctrl icon, then press the Alt and Del keys on the keyboard.

Notes:

1. Only one remote control session is allowed at a time. If a remote control session is already active, you can end the current session and start a new one.
2. The timeout value for a remote control session is the same as the timeout value that you set for the Web session when you logged in.
3. When you redirect a blade server Linux X Window System session console to the remote console, the ability of the remote console applet to accurately track the location of the mouse cursor depends on the configuration of the X Window system. Complete the following procedure to configure the X Window System for accurate mouse tracking. Type the commands through the remote console or at the keyboard attached to the BladeCenter unit. Note that the changes require root privileges.
 - a. Enter the following commands:

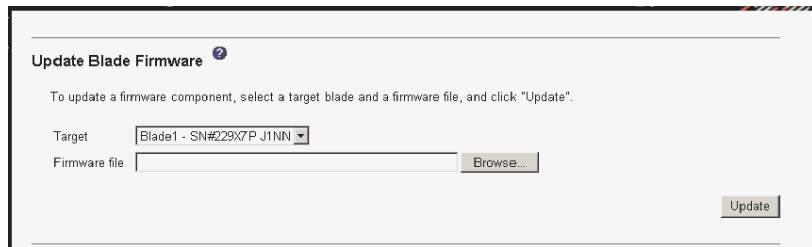
```
init 3 (Switch to text mode if necessary)
rmmod mousedev (Unload the mouse device driver)
```
 - b. Add the following statement to `.xinitrc` in the user's home directory:

```
xset m 1 1 (Turn off mouse acceleration)
```
 - c. Add the following statement to `/etc/modules.conf`:

```
options mousedev xres=x yres=y (Notify the mouse
device driver of the video resolution) where x and y
specify the video resolution
```
 - d. Enter the following commands:

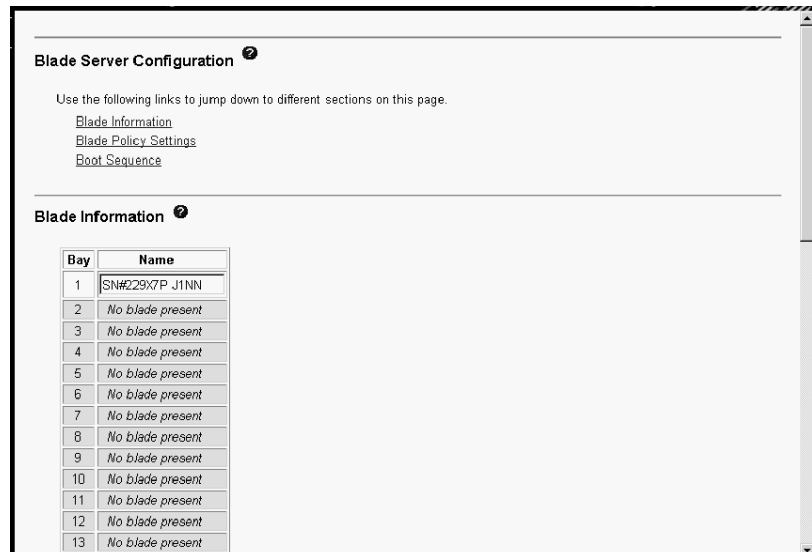
```
insmod mousedev (Reload the mouse device driver)
init 5 (Return to GUI mode if necessary)
```

Firmware update



Select this choice to update the service processor firmware on a blade server. Select the target blade server and the firmware file to use for the update; then, click **Update**. You can obtain the firmware files from the IBM Support Web site at <http://www.ibm.com/pc/support/>.

Configuration



Bay	Name
1	SN#229X7P J1NN
2	No blade present
3	No blade present
4	No blade present
5	No blade present
6	No blade present
7	No blade present
8	No blade present
9	No blade present
10	No blade present
11	No blade present
12	No blade present
13	No blade present

Select this choice to:

- Define a name for a blade server.
- Enable or disable the following items on all blade servers in the BladeCenter unit:
 - Local power control
 - Local KVM control
 - Local media tray control
 - The Wake on LAN feature
- View or define the startup (boot) sequence for one or more blade servers. The startup sequence prioritizes the following boot-record sources for a blade server:
 - IDE drive 1 (HDD1)
 - IDE drive 2 (HDD2)
 - CD-ROM
 - Diskette
 - Network

- **PXE** - Attempt a PXE/DHCP network startup the next time the selected blade server is turned on or restarted.


Note: To use the CD-ROM drive or diskette drive as a boot-record source for a blade server, the blade server must have been designated as the owner of the CD-ROM drive, diskette drive, and USB port. You set ownership either by pressing the CD/diskette/USB select button on the blade server or through the **Remote Control** choice described on page 17.

I/O Module Tasks

Select the choices in this section to view and change the settings or configuration on network-interface I/O modules in the BladeCenter unit.

Note: Some choices do not apply to, and are not available for, some types of I/O modules such as pass-thru modules.

Power/Restart

I/O Module Power/Restart 

Select one or more module(s) using the checkboxes in the first column and then click on one of the links below the table to perform the desired action.

<input type="checkbox"/>	Bay	Type	MAC Address	IP Address	Pwr
<input type="checkbox"/>	1	Ethernet SM	00:05:5D:71:83:B0	160.0.0.34	On
	2		No module		
	3		No module		
	4		No module		

[Power On Module\(s\)](#)
[Power Off Module\(s\)](#)
[Restart Module\(s\) and Run Standard Diagnostics](#)
[Restart Module\(s\) and Run Extended Diagnostics](#)
[Restart Module\(s\) and Run Full Diagnostics](#)

Select this choice to display the power status of the I/O modules and perform the following actions:

- Turn on or turn off an I/O module
- Reset an I/O module

Management

I/O Module Management

Use the following links to jump down to different sections on this page.

[Bay 1](#)
[Bay 2](#)
[Bay 3](#)
[Bay 4](#)

Bay 1 (Ethernet SM)

Current IP Configuration

Configuration method: Static
IP address: 160.0.0.34
Subnet mask: 255.255.0.0
Gateway address: 0.0.0.0

New Static IP Configuration

Status: Enabled

To change the IP configuration for this switch module, fill in the following fields and click "Save". This will save and enable the new IP configuration.

IP address:
Subnet mask:
Gateway address:

[Advanced Management](#)

Select this choice to view or change the IP configuration of the Ethernet or Fibre Channel switch modules; ping a switch module; return a switch module to the default configuration; enable the switch module ports, external management of switch ports, other switch settings; and start the configuration and management firmware that is in the switch module.

Note: The initial user ID and password for the switch module firmware are:

- User ID: USERID (all capital letters)
- Password: PASSWORD (note the zero, not O, in PASSWORD)

See the *IBM @server BladeCenter Type 8677 Installation and User's Guide* for more information about basic configuration of the Ethernet switch module.

See the documentation that comes with the switch module for details about the configuration and management firmware for the switch module. Documentation for the Ethernet switch module is on the *IBM BladeCenter Documentation CD*.

MM Control

Select the choices in this section to view and change the settings or configuration on the management module whose Web interface you are logged into. This includes configuring the following items:

- The name of the management module
- Up to 12 login profiles for logging in to the management module
- How alerts are handled
- The management module Ethernet connections for remote console and for communicating with the I/O modules
- Settings for the SNMP, SMTP, and DNS protocols
- Settings for secure socket layer (SSL) security

This also includes performing the following tasks:

- Backing up and restoring the management-module configuration
- Updating the management-module firmware
- Restoring the default configuration
- Restarting the management module
- Switching from the current active management module to the redundant management module

General Settings

[View Configuration Summary](#)

MM Information ?

Name

Contact

Location

MM Date and Time ?

Date (mm/dd/yyyy):

Time (hh:mm:ss):

[Set MM Date and Time](#)

Select this choice to view or change the following settings:

- The name of the management module
- The name of the contact person responsible for the module
- The physical location of the management module
- The real-time clock settings in the management module

Login Profiles

[View Configuration Summary](#)

Management Module Login Configuration ?

Use the following links to jump down to different sections on this page.

[Login Profiles](#)

[Global Login Settings](#)

Login Profiles ?

To configure a login profile, click a link in the "Login ID" column.

Login ID	Access
1. _USERID	Read/Write
2. _mcalri	Read/Write
3. _tushar	Read/Write
4. _germany	Read/Write
5. _france	Read/Write
6. _spain	Read/Write
7. _japan	Read/Write
8. _korea	Read/Write
9. _taiwan	Read/Write
10. _china	Read/Write
11. ~ not used ~	
12. ~ not used ~	

Select this choice to configure up to 12 login profiles for logging in to the management module, and to specify the lockout period after five unsuccessful login attempts. For each profile, specify the following values:

- Login ID
- Authority level (default is Read Only)

- Password (requires confirmation)

Attention: If you change the default login profile on your management module, be sure to keep a record of your login ID and password in a safe place. If you forget the management-module login ID and password, you must replace the management module.

Alerts

[View Configuration Summary](#)

Management Module Alerts Configuration ?

Use the following links to jump down to different sections on this page.

[Remote Alert Recipients](#)
[Global Remote Alert Settings](#)
[Monitored Alerts](#)

Remote Alert Recipients ?

To configure a remote alert recipient, click a link in the "Name" column.

Name	Notification Method	Status
moalvi	SNMP over LAN	Receives all alerts
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		
~ not used ~		

Select this choice to specify which alerts (from lists of Critical, Warning, and System alerts) are monitored, which alert notifications are sent to whom, how alert notifications are sent (SNMP, e-mail, IBM Director), whether to include the event log with the notification, and other alert parameters.

Note: The IBM Director program is a system-management product that comes with the BladeCenter unit. To configure the remote alert recipients for IBM Director over LAN, the remote alert recipient must be an IBM Director-enabled server.

Network Interfaces

[View Configuration Summary](#)

Management Module Network Interfaces [?]

Use the following links to jump down to different sections on this page.

- [External Network Interface \(eth0\)](#)
- [Internal Network Interface \(eth1\)](#)
- [TCP Log](#)

External Network Interface (eth0) [?]

Interface: Enabled
DHCP: Disabled - Use static IP configuration

*** Currently the static IP configuration is active for this interface.
*** This static configuration is shown below.

Hostname: MM00096BCA32E0

Static IP Configuration

IP address	160.0.0.31
Subnet mask	255.255.0.0
Gateway address	0.0.0.0

[Advanced Ethernet Setup](#) [IP Configuration Assigned by DHCP Server](#)

Select this choice to configure the two Ethernet interfaces: external (remote management and console), and internal (communication with the I/O modules). You can also select this choice to view the TCP log.

Notes:

1. When you use the management module Web interface to update the Ethernet or Fibre Channel switch module configuration, the management module firmware writes its settings for the switch module only to the management module NVRAM; it does not write its settings for the switch module to the switch module NVRAM.

If the switch module restarts when the management module is not able to apply the IP address it has in NVRAM for the switch module, the switch module will use whatever IP address it has in its own NVRAM. If the two IP addresses are not the same, you might not be able to manage the Ethernet switch module any more.

The management module cannot apply the switch IP address from its NVRAM if:

- The management module is restarting
- The management module has failed
- The management module has been removed from the chassis

You must use the Telnet interface to log into the switch module, change the IP address to match the one you assigned through the management module, and save the switch settings in the Telnet session (**Basic Setup** → **Save Changes**).

2. For switch communication with a remote management station, such as the IBM Director server, through the management module external Ethernet port, the switch module internal network interface and the management module internal and external interfaces must be on the same subnet.

- **External Network Interface (eth0)** - This is the interface for the remote management and console port.

Note: If you plan to use redundant management modules and want both to use the same external IP address, disable DHCP and configure and use the static IP address. (The IP configuration information will be transferred to the redundant management module automatically when needed.)

- **Interface** - The status (Enabled or Disabled) of the Ethernet connection. The default is Enabled.
- **DHCP** - Select one of the following choices:
 - **Try DHCP server. If it fails, use static IP config.** (this is the default).
 - **Enabled - Obtain IP config. from DHCP server**
 - **Disabled - Use static IP configuration**
- **Hostname** - (Optional) This is the IP host name you want to use for the management module (maximum of 63 characters).
- **Static IP configuration** - You need to configure this information only if DHCP is disabled.
 - **IP address** - The IP address for the management module. The IP address must contain four integers from 0 to 255, separated by periods, with no spaces or consecutive periods. The default setting is 192.168.70.125.
 - **Subnet mask** - The subnet mask must contain four integers from 0 to 255, separated by periods, with no spaces. The default setting is 255.255.255.0
 - **Gateway address** - The IP address for your network gateway router. The gateway address must contain four integers from 0 to 255, separated by periods, with no spaces.
- **Internal Network Interface (eth1)** - This interface communicates with the network-interface I/O modules, such as the Ethernet switch module or the Fibre Channel switch module.
 - Specify the IP address to use for this interface. The subnet mask must be the same as the subnet mask in the external network interface (eth0).
 - View the data rate, duplex mode, maximum transmission unit (MTU), locally-administered MAC address, and burned-in MAC address for this interface. You can configure the locally-administered MAC address; the other fields are read-only.
- **TCP log** - Select this choice to view entries that are currently stored in the management module TCP log. This log contains error and warning messages generated by the TCP/IP code running on the management module, and might be used by your service representative for advanced troubleshooting. The log displays the most recent entries first.
You can sort and filter entries in the event log.

Network Protocols

The screenshot shows the 'Management Module Network Protocols' configuration page. At the top right is a link for 'View Configuration Summary'. Below the title, there are instructions to use links to jump to different sections: 'Simple Network Management Protocol (SNMP)', 'Domain Name System (DNS)', and 'Simple Mail Transfer Protocol (SMTP)'. The 'Simple Network Management Protocol (SNMP)' section is expanded, showing 'SNMP agent' and 'SNMP traps' both set to 'Enabled'. Below this is a table for community names and host names/IP addresses.

Community Name	Host Name or IP Address
Mastermind	1. 193.0.0.39
	2.
	3.
	1.
	2.
	3.
	1.

Select this choice to view or change the settings for the SNMP, SMTP, and DNS protocols.

Security

The screenshot shows the 'Install SSL' configuration page. It states 'SSL is not currently installed.' and provides instructions: 'To install SSL, go to the BladeCenter firmware update site to obtain the installation key. After downloading and saving the key file, select the saved key file below and click on "Install SSL".' Below the instructions is a file selection field with a 'Browse...' button and an 'Install SSL' button.

Select this choice to view or change the secure socket layer (SSL) settings. You can enable or disable (the default) SSL, and choose between self-signed certificates and certificates provided by a certificate authority (CA).

Note: The first time you select **Security**, you are directed to an IBM Web page for downloading the SSL installation key. After you load the key, the **Security** choice functions as described.

Configuration File

The screenshot shows a web interface for managing the Management Module (MM) configuration. It is divided into two main sections: "Backup MM Configuration" and "Restore MM Configuration".

Backup MM Configuration

To backup the configuration, click "Backup." You can [view the current configuration summary](#) before backing it up.

Backup

Restore MM Configuration

To restore the MM configuration, select a file and click "Restore." To modify the configuration and then restore it, select a file and click "Modify & Restore."

Select configuration file to restore

Browse...

Restore Modify and Restore

Select this choice to back up or restore the management-module configuration file.

Firmware Update

The screenshot shows a web interface for updating the Management Module (MM) firmware. It includes a section for "Update MM Firmware" with a checkbox for automatic updates and a file selection field.

Update MM Firmware

To update a firmware component on the MM, select a firmware file and click "Update". If you want the firmware on the redundant MM to be automatically updated to the same level, select the checkbox below.

Automatically update firmware on redundant MM

Browse...

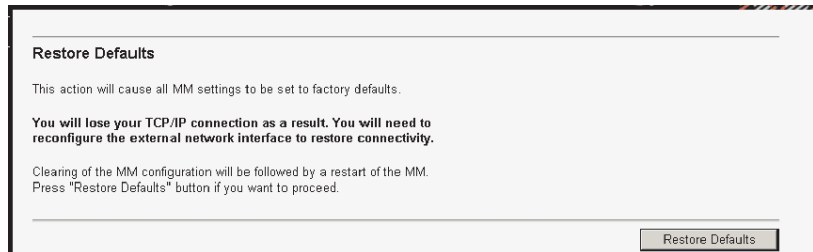
Note: To ensure proper operation of the management module, make sure you update all MM firmware components to the same level.

Update

Select this choice to update the management-module firmware; if a second management module is installed, you can choose to apply the firmware update only to the active management module. Click **Browse** to locate the firmware file you want; then, click **Update**.

You can obtain the firmware files from the IBM Support Web site at <http://www.ibm.com/pc/support/>.

Restore Defaults



Restore Defaults

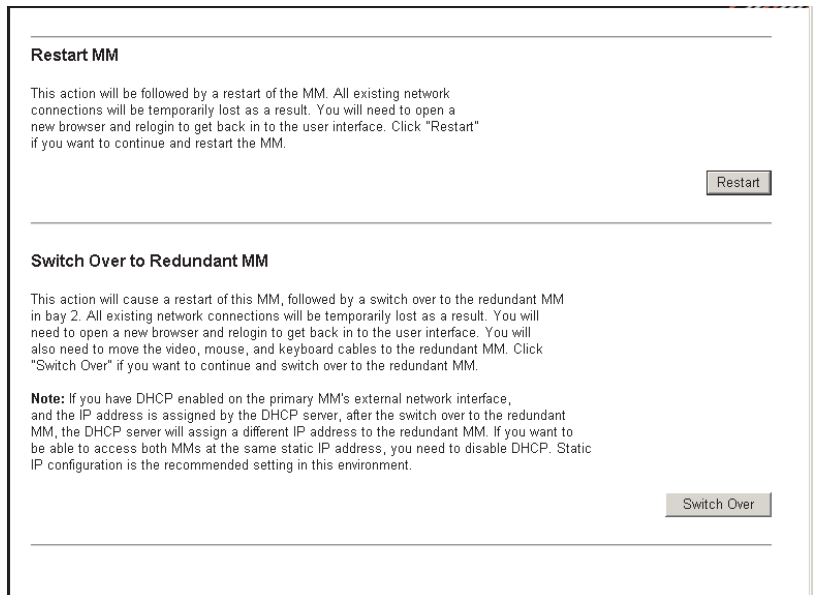
This action will cause all MM settings to be set to factory defaults.

You will lose your TCP/IP connection as a result. You will need to reconfigure the external network interface to restore connectivity.

Clearing of the MM configuration will be followed by a restart of the MM. Press "Restore Defaults" button if you want to proceed.

Select this choice to restore the factory default configuration of the management module.

Restart MM



Restart MM

This action will be followed by a restart of the MM. All existing network connections will be temporarily lost as a result. You will need to open a new browser and relogin to get back in to the user interface. Click "Restart" if you want to continue and restart the MM.

Switch Over to Redundant MM

This action will cause a restart of this MM, followed by a switch over to the redundant MM in bay 2. All existing network connections will be temporarily lost as a result. You will need to open a new browser and relogin to get back in to the user interface. You will also need to move the video, mouse, and keyboard cables to the redundant MM. Click "Switch Over" if you want to continue and switch over to the redundant MM.

Note: If you have DHCP enabled on the primary MM's external network interface, and the IP address is assigned by the DHCP server, after the switch over to the redundant MM, the DHCP server will assign a different IP address to the redundant MM. If you want to be able to access both MMs at the same static IP address, you need to disable DHCP. Static IP configuration is the recommended setting in this environment.

Select this choice to restart (reset) the management module. If a second management module is present, select this choice to change to the redundant management module.

Configuring SNMP

You can query the SNMP agent to collect the sysgroup information and to send configured SNMP alerts to the configured host names or IP addresses.

Note: If you plan to configure Simple Network Management Protocol (SNMP) traps on the management module, you must install and compile the management information base (MIB) on your SNMP manager. The MIB supports SNMP traps. The MIB is included in the management-module firmware update package that you downloaded from the IBM Support Web site.

Complete the following steps to configure your SNMP:

1. Log in to the management module where you want to configure SNMP. For more information, see “Starting the management and configuration program” on page 8
2. In the navigation pane, click **General Settings**. In the management-module information page that opens, specify the following information:
 - **Management module name** - The name that you want to use to identify the management module. The name will be included with e-mail and SNMP alert notifications to identify the source of the alert.
 - **System contact** - The name and phone number of the person to contact if there is a problem with the BladeCenter unit.
 - **System location** - Sufficient detail to quickly locate the BladeCenter unit for maintenance or other purposes.
3. Scroll to the bottom of the page and click **Save**.
4. In the navigation pane, click **Network Protocols**; then, click the **Simple Network Management Protocol (SNMP)** link. A page similar to the one in the following illustration is displayed.

Simple Network Management Protocol (SNMP) ?

SNMP agent

SNMP traps

Community Name	Host Name or IP Address
<input type="text"/>	1. <input type="text"/>
	2. <input type="text"/>
	3. <input type="text"/>
<input type="text"/>	1. <input type="text"/>
	2. <input type="text"/>
	3. <input type="text"/>
<input type="text"/>	1. <input type="text"/>
	2. <input type="text"/>
	3. <input type="text"/>

-
5. Select **Enabled** in the **SNMP agent** and **SNMP traps** fields to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:
 - System contacts must be specified on the General Settings page.

- The system location must be specified on the General Settings page.
- At least one community name must be specified.
- At least one valid IP address or host name (if DNS is enabled) must be specified for that community.

Note: Alert recipients whose notification method is SNMP will not receive alerts unless both the SNMP agent and the SNMP traps are enabled.

6. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:

- Name
- IP address

If either of these parameters is not correct, SNMP management access is not granted.

Note: If an error message window opens, make the necessary adjustments to the fields listed in the error window. Then, scroll to the bottom of the page and click **Save** to save your corrected information. You must configure at least one community to enable this SNMP agent.

7. In the **Community Name** field, enter a name or authentication string to specify the community.
8. In the corresponding **Host Name** or **IP Address** field, enter the host name or IP addresses of each community manager.
9. If a DNS server is not available on your network, scroll to the bottom of the page and click **Save**.
10. If a DNS server is available on your network, scroll to the **Domain Name System (DNS)** section. A page similar to the one in the following illustration is displayed.

Domain Name System (DNS)

DNS	<input type="text" value="Enabled"/>
DNS server IP address 1	<input type="text" value="9.37.0.5"/>
DNS server IP address 2	<input type="text" value="9.37.0.6"/>
DNS server IP address 3	<input type="text" value="0.0.0.0"/>

11. If a DNS server (or servers) is available on your network, select **Enabled** in the **DNS** field. The **DNS** field specifies whether you use a DNS server on your network to translate host names into IP addresses.
12. If you enabled DNS, in the **DNS server IP address** fields, you can specify the IP addresses of up to three DNS servers on your network. Each IP address should contain integers from 0 through 255, separated by periods.
13. Scroll to the bottom of the page and click **Save**.
14. In the navigation pane, click **Restart MM** to activate the changes.

Saving and restoring the configuration file

After you have configured the active management module, you can save the configuration file to a diskette or other external media. Then, if the configuration in the active management module becomes damaged or the only management module is replaced, you can restore the saved configuration file to the management module. Use the management-module Web interface to save and restore the configuration file (**MM Control** → **Configuration File**).

Note: If you cannot communicate with a replacement management module through the Web interface or the IBM Director programs, the IP address might be different from the IP address of the management module just removed. Press the IP reset button to set the management module to the factory default IP addresses; then, access the management module using the factory IP address (see “Configuring the management module for remote access” on page 7 for the factory IP addresses) and configure the management module or load the saved configuration file.

Notices

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

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

IBM 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:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "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. IBM 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 non-IBM Web sites 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 IBM product, and use of those Web sites is at your own risk.

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

Edition notice

© Copyright International Business Machines Corporation 2003. All rights reserved.

U.S. Government Users Restricted Rights — Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Trademarks

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

Active Memory	Predictive Failure Analysis
Active PCI	PS/2
Active PCI-X	ServeRAID
Alert on LAN	ServerGuide
BladeCenter	ServerProven
C2T Interconnect	TechConnect
Chipkill	ThinkPad
EtherJet	Tivoli
e-business logo	Tivoli Enterprise
@server	Update Connector
FlashCopy	Wake on LAN
IBM	XA-32
IntelliStation	XA-64
NetBAY	X-Architecture
Netfinity	Xcel4
NetView	XpandOnDemand
OS/2 WARP	xSeries

Lotus, Lotus Notes, SmartSuite, and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

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

Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD-ROM drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1 000 000 bytes, and GB stands for approximately 1 000 000 000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven[®], including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Product recycling and disposal

This unit contains materials such as circuit boards, cables, electromagnetic compatibility gaskets, and connectors which may contain lead and copper/beryllium alloys that require special handling and disposal at end of life. Before this unit is disposed of, these materials must be removed and recycled or discarded according to applicable regulations. IBM offers product-return programs in several countries. Information on product recycling offerings can be found on IBM's Internet site at <http://www.ibm.com/ibm/environment/products/prp.shtml>.

Battery return program

This product may contain a 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 collection process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and battery packs from IBM equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Have the IBM part number listed on the battery available prior to your call.

In the Netherlands, the following applies.

INSERT D3MM9BAT HERE

Electronic emission notices

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. 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 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 Class A emission compliance statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance 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 nonrecommended 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 CISPR 22/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.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese Class A warning statement

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。

Chinese Class A warning statement

聲 明
此為 A 級產品。在生活環境中，該產品可能會造成無線電干擾。在這種情況下，可能需要用戶對其干擾採取切实可行的措施。

Japanese Voluntary Control Council for Interference (VCCI) statement

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。

Power cords

For your safety, IBM provides a power cord with a grounded attachment plug to use with this IBM product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.

IBM power cords used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).

For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.

For units intended to be operated at 230 volts (U.S. use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.

For units intended to be operated at 230 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.

IBM power cords for a specific country or region are usually available only in that country or region.

IBM power cord part number	Used in these countries and regions
02K0546	China
13F9940	Australia, Fiji, Kiribati, Nauru, New Zealand, Papua New Guinea
13F9979	Afghanistan, Albania, Algeria, Andorra, Angola, Armenia, Austria, Azerbaijan, Belarus, Belgium, Benin, Bosnia and Herzegovina, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo (Democratic Republic of), Congo (Republic of), Cote D'Ivoire (Ivory Coast), Croatia (Republic of), Czech Republic, Dahomey, Djibouti, Egypt, Equatorial Guinea, Eritrea, Estonia, Ethiopia, Finland, France, French Guyana, French Polynesia, Germany, Greece, Guadeloupe, Guinea, Guinea Bissau, Hungary, Iceland, Indonesia, Iran, Kazakhstan, Kyrgyzstan, Laos (People's Democratic Republic of), Latvia, Lebanon, Lithuania, Luxembourg, Macedonia (former Yugoslav Republic of), Madagascar, Mali, Martinique, Mauritania, Mauritius, Mayotte, Moldova (Republic of), Monaco, Mongolia, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Reunion, Romania, Russian Federation, Rwanda, Sao Tome and Principe, Saudi Arabia, Senegal, Serbia, Slovakia, Slovenia (Republic of), Somalia, Spain, Suriname, Sweden, Syrian Arab Republic, Tajikistan, Tahiti, Togo, Tunisia, Turkey, Turkmenistan, Ukraine, Upper Volta, Uzbekistan, Vanuatu, Vietnam, Wallis and Futuna, Yugoslavia (Federal Republic of), Zaire
13F9997	Denmark
14F0015	Bangladesh, Lesotho, Maceo, Maldives, Namibia, Nepal, Pakistan, Samoa, South Africa, Sri Lanka, Swaziland, Uganda
14F0033	Abu Dhabi, Bahrain, Botswana, Brunei Darussalam, Channel Islands, China (Hong Kong S.A.R.), Cyprus, Dominica, Gambia, Ghana, Grenada, Iraq, Ireland, Jordan, Kenya, Kuwait, Liberia, Malawi, Malaysia, Malta, Myanmar (Burma), Nigeria, Oman, Polynesia, Qatar, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Seychelles, Sierra Leone, Singapore, Sudan, Tanzania (United Republic of), Trinidad and Tobago, United Arab Emirates (Dubai), United Kingdom, Yemen, Zambia, Zimbabwe
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Italy, Libyan Arab Jamahiriya

IBM power cord part number	Used in these countries and regions
14F0087	Israel
1838574	Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, Bolivia, Brazil, Caicos Islands, Canada, Cayman Islands, Costa Rica, Colombia, Cuba, Dominican Republic, Ecuador, El Salvador, Guam, Guatemala, Haiti, Honduras, Jamaica, Japan, Mexico, Micronesia (Federal States of), Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Taiwan, United States of America, Venezuela
24P6858	Korea (Democratic People's Republic of), Korea (Republic of)
34G0232	Japan
36L8880	Argentina, Paraguay, Uruguay
49P2078	India
49P2110	Brazil
6952300	Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, Bolivia, Caicos Islands, Canada, Cayman Islands, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guam, Guatemala, Haiti, Honduras, Jamaica, Mexico, Micronesia (Federal States of), Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Thailand, Taiwan, United States of America, Venezuela

Index

C

- cabling
 - remote connection Ethernet port 6
- Class A electronic emission notice 36
- configuration file
 - restoring 31
 - saving 31
- Configuration/Setup Utility program 8
- configuring
 - BladeCenter unit 4
 - DNS 30
 - SNMP 29
- connector
 - Ethernet
 - remote management and console 4
 - input/output 3
 - keyboard 3
 - PS/2 mouse 4
 - remote management 4
 - video 3

D

- difficulty communicating with replacement module 31
- DNS, configuring 30

E

- electronic emission Class A notice 36
- error log.
 - See event log
- Ethernet
 - configuring remote connection 7
 - port, cabling 6
- Ethernet activity LED 2, 6
- Ethernet connector, remote management and console 4
- Ethernet-link status LED 2, 6
- event log 12
- event log in alerts 23
- event log, viewing 12

F

- FCC Class A notice 36

I

- IP reset button 2, 31

K

- keyboard connector 3

L

- LEDs
 - active 2
 - error 2
 - Ethernet activity 2, 6
 - Ethernet-link status 2, 6
 - power-on 2

M

- management module
 - redundant
 - manual changeover 28
- mouse connector 4

N

- network protocols
 - configuring DNS 30
 - configuring SNMP 29
- network, connecting 6
- notes, important 34
- notices
 - electronic emission 36
 - FCC, Class A 36

P

- port
 - See connector
- power cords 37
- power-on LED 2
- protocols
 - DNS 30
 - SNMP 29

R

- remote console 17
- remote control 17
- remote management connector 4
- replacement module, difficulty communicating with 31
- restoring configuration file 31

S

- saving configuration file 31
- SNMP, configuring 29

T

- TCP log 25
- TCP log, viewing 25
- trademarks 34

U

United States electronic emission Class A notice 36
United States FCC Class A notice 36
utility, Configuration/Setup 8

V

video connector 3

W

Web browsers, supported 5



Part Number: 59P6594

Printed in U.S.A.

(1P) P/N: 59P6594

