IBM @server Cluster 1350

Installation and Service Guide

IBM @server Cluster 1350

Installation and Service Guide

Note: Before using this information and the product it supports, read the general information in “Safety” on page vii and Appendix F, “Notices”, on page 93.

Second edition (November 2003)

Contents

Safety

For general information concerning safety, refer to *Electrical Safety for IBM Customer Engineers*, S229-8124. For a copy of the publication, contact your IBM® account representative or the IBM branch office serving your locality.

Enterprise rack safety information: Read the safety notices in the manual provided with the enterprise rack before beginning work. Keep the Enterprise Rack manual near the rack for fast reference.

The procedures described in this document must be performed by qualified service personnel. Safety warnings are contained within these procedures. If you cannot read the language of this document, do not perform any procedures until you receive a translated copy. IBM does not accept responsibility or liability for failure to follow these procedures correctly.

Safety Information

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

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 pečítaje 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.

Important:

All caution and danger statements in this documentation begin with a number. This number is used to cross reference an English caution or danger statement with translated versions of the caution or danger statement in the *IBM NetBAY Rack Safety Information* book.

For example, if a caution statement begins with a number 1, translations for that caution statement appear in the *IBM NetBAY Rack Safety Information* book under statement 1.

Be sure to read all caution and danger statements in this documentation before performing the instructions. Read any additional safety information that comes with your server or optional device before you install the device.

Statement 2:

DANGER

- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **Always install servers and optional devices starting from the bottom of the rack cabinet.**
- **Always install the heaviest devices in the bottom of the rack cabinet.**

Statement 3:

DANGER

- **Do not extend more than one sliding device at a time.**
- **The maximum allowable weight for devices on slide rails is 80 kg (176 lb). Do not install sliding devices that exceed this weight.**

Class 1 Laser Product
Laser Klasse 1
Laser Klass 1
Luokan 1 Laserlaite
Appareil À Laser de Classe 1

Statement 4:

DANGER

Electrical current from power, telephone, and communication cables is hazardous.

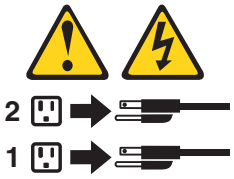
To avoid a shock hazard:

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

Statement 7:

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.



Statement 8:

DANGER

- **Plug power cords from devices in the rack cabinet into electrical outlets that are located near the rack cabinet and are easily accessible.**
- **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.**
- **Install an emergency-power-off switch if more than one power device (power distribution unit or uninterruptible power supply) is installed in the same 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.**

Statement 10:

CAUTION:
Removing components from the upper positions in the Enterprise Rack cabinet improves rack stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building:

- **Reduce the weight of the rack cabinet by removing equipment starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must do the following:**
  - **Remove all devices in the 32U position and above.**
  - **Ensure that the heaviest devices are installed in the bottom of the rack cabinet.**
  - **Ensure that there are no empty U-levels between devices installed in the rack cabinet below the 32U level.**
- **If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.**
- **Inspect the route that you plan to take to eliminate potential hazards.**
- **Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.**
- **Verify that all door openings are at least 760 x 2030 MM. (30 x 80 in.)**
- **Ensure that all devices, shelves, drawers, doors, and cables are secure.**
- **Ensure that the four leveling pads are raised to their highest position.**
- **Ensure that there is no stabilizer bracket installed on the rack cabinet.**
- **Do not use a ramp inclined at more than ten degrees.**
- **Once the rack cabinet is in the new location, do the following:**
  - **Lower the four leveling pads.**
  - **Install stabilizer brackets on the rack cabinet.**
  - **If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.**

If a long distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also, lower the leveling pads to raise the casters off of the pallet and bolt the rack cabinet to the pallet.

Notices and statements in this book

The caution and danger statements used in this book also appear in the multilingual *Safety Information* book provided on the IBM Documentation CD. Each caution and danger statement is numbered for easy reference to the corresponding statements in the safety book.

The following types of notices and statements are used in this book:

- **Note:**These notices provide important tips, guidance, or advice.
- **Important:**These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:**These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.

- **Caution:**These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.
- **Danger:**These statements indicate situations that can be potentially lethal or extremely hazardous to you. A danger statement is placed just before the description of a potentially lethal or extremely hazardous procedure step or situation.

Chapter 1. System overview

This chapter provides information about the operating systems that support the IBM cluster components and related documentation.

The Cluster 1350 supports a maximum of 512 nodes in addition to the one required xSeries™ 345 management node (or an @server 325 for 64-bit processing environments). All nodes must run one of the Linux versions shown in the following table.

Table 1. Linux operating-system support

Microprocessor	Operating-system support
32-bit Professional	Red Hat Linux version 9.0 (CSM), SuSE Linux version 8.2 (XCAT) for Opteron, RHEL version 2.1 and version 3.0 WorkStation for Opteron (XCAT), SuSE Linux version 8.2 (XCAT)
32-bit Enterprise	SLES version 8 (XCAT) for Opteron, RHEL version 3.0 Work Station (XCAT)
64-bit	SLES version 8 for Opteron, RHEL version 3.0 for Opteron (CSM only)

The Cluster 1350 uses a primary cabinet and an expansion cabinet. The primary cabinet contains the management node and console monitor. An expansion cabinet can contain the following components:

- cluster or compute nodes
- storage nodes
- mass storage devices

Note: An expansion cabinet does not contain a management node or console.

Figure 1 on page 2 illustrates a primary cabinet. Figure 2 on page 3 illustrates an expansion cabinet containing cluster nodes. Figure 3 on page 4 illustrates an expansion cabinet containing storage controllers and mass storage.

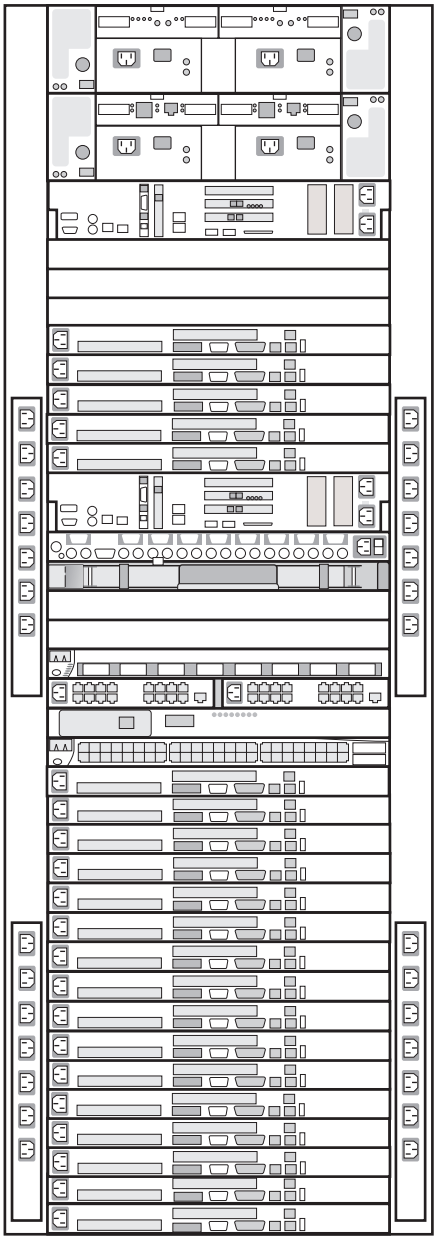


Figure 1. Example of an @server Cluster 1350 primary cabinet

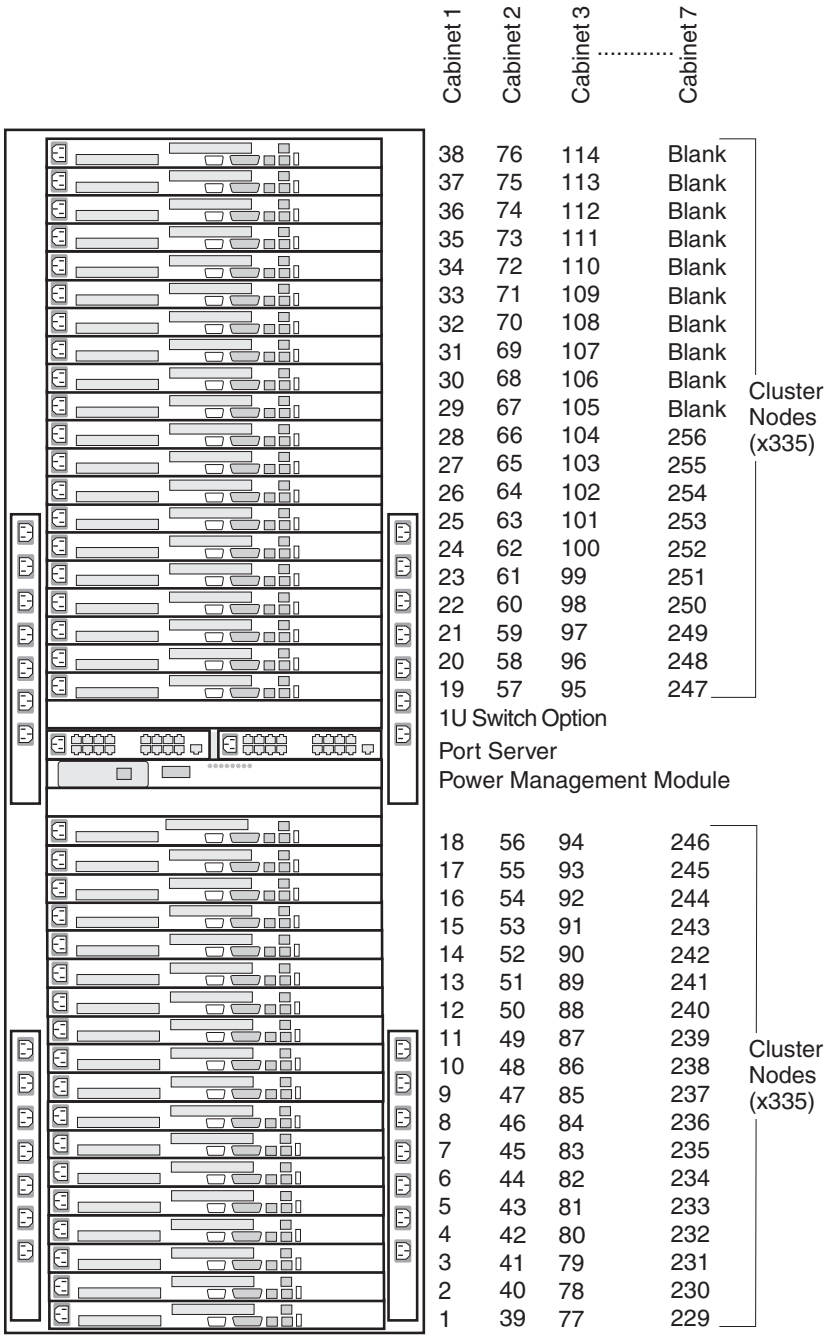


Figure 2. Example of an @server Cluster 1350 expansion cabinet with cluster nodes. This figure also shows how the node numbering scheme maps to other expansion cabinets.

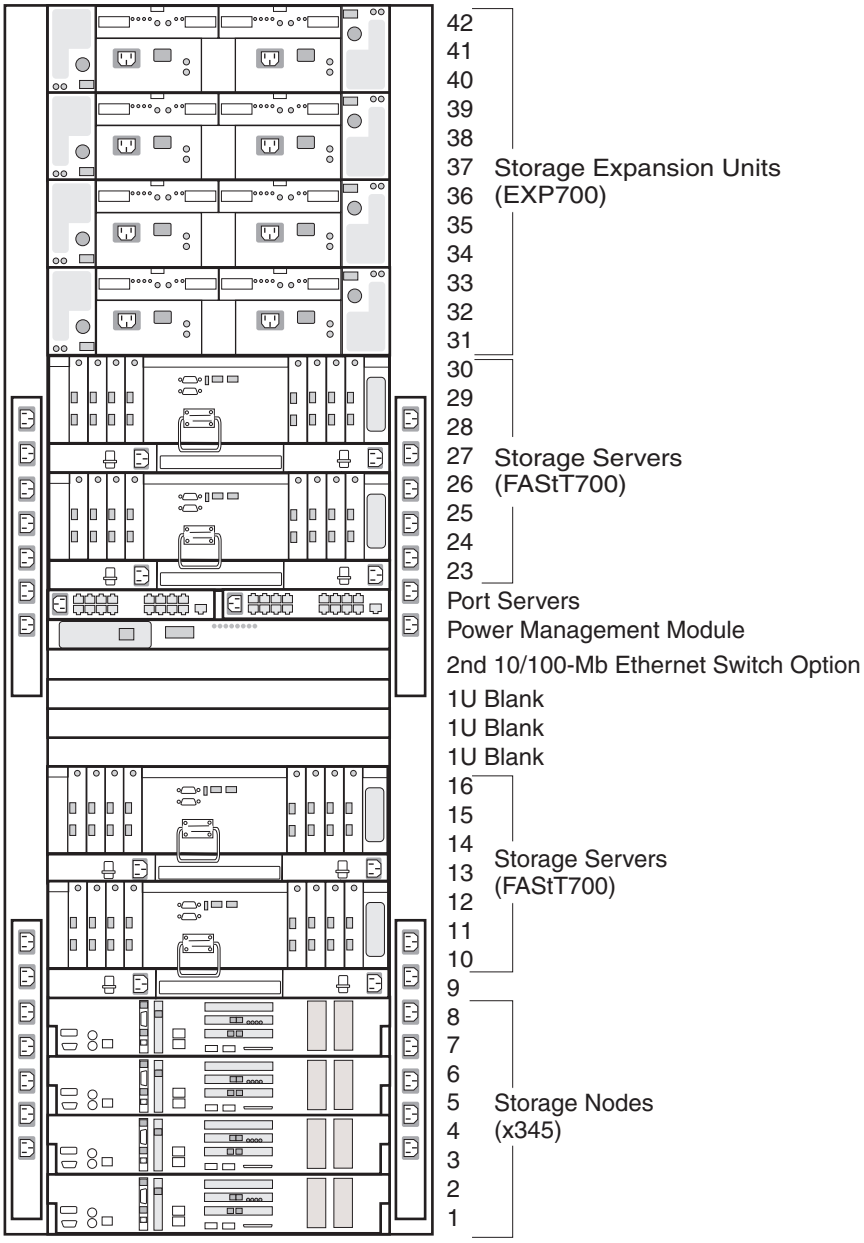


Figure 3. Example of an IBM @server Cluster 1350 expansion cabinet containing storage controllers and mass storage

Cluster components

This section describes the components in the Cluster 1350. Cluster components include:

- Cluster nodes
- Management node
- Storage nodes
- Storage servers
- Storage expansion units
- SCSI/RAID Storage controller adapters

- Console
- KVM switch
- 10/100 Mb Ethernet switch
- 1 Gb Ethernet switch
- Port server
- High-Speed Myrinet switch
- High-Speed Cisco switch
- Power management module
- Power distribution unit (PDU)

Cluster nodes

A cluster must contain at least four cluster nodes. The cluster nodes carry out the computational tasks in the cluster.

The cluster nodes are a combination of the following components:

- @server™ 325
- xSeries 335
- xSeries 345
- @server BladeCenter® populated with HS20 Blade servers

Each node runs a supported version of Linux. Cluster nodes are also known as compute nodes.

Management node

Each cluster contains one management node, which provides system management for all modules in the cluster. The Cluster 1350 management node is typically an xSeries 345 running Linux. You can also use an @server 325 as the management node in a cluster environment running a 64-bit operating system. The @server 325 rack model server processes high-volume network transactions.

Storage nodes

The optional storage nodes manage the mass storage. The cluster supports up to 32 storage nodes. The total number of storage and compute nodes cannot exceed 512.

For tasks that do not require large amounts of mass storage, the storage node has onboard disk storage that is typically sufficient. The storage nodes can be any of the following servers in the primary cabinet running Linux:

- @server 325 - a 1 U storage unit
- xSeries335 - a 1 U storage unit
- xSeries 345 - a 2 U storage unit
- xSeries 360 - a 3 U storage unit
- @server BladeCenter unit populated with HS20 Blade servers

Storage servers

For the storage server option, the Cluster 1350 system communicates over a Fibre Channel connection and uses the RAID-capable controllers:

- FAStT200 Storage Controller (3 U). Each FAStT200 Storage Controller adds up to 10 internal 18 GB 15000 RPM drives or ten 36 GB or 73 GB 10000 RPM drives to the storage capacity of the cluster.

- FAStT600 Storage Controller (3 U). Each FAStT600 Storage Controller supports up to 14 internal disk drive modules, supporting over 2-TBs of storage capacity when using 146 GB drives. Additional storage can be added to the FAStT600 with up to seven FAStT EXP700s using optional EXP700 attachment features.
- FAStT700 Storage Controller (3 U). Each FAStT700 Storage Controller supports up to 224 18 GB 15000 RPM drives or 224 36GB or 73 GB 10000 RPM drives contained in external expansion cabinets.
- FAStT900 Storage Controller (4 U). Each FAStT900 Storage Controller supports up to 16 EXP700 external expansion cabinets. All controllers interface with the cluster so that the storage nodes communicate with large RAID-protected arrays of storage.

Storage expansion units

The cluster supports the following disk storage expansion units:

- Each FAStT200 Storage Server in the cluster controls up to two EXP500 Disk Storage Expansion Units, each of which expands the capacity of the storage server by ten disk drives.
- Each FAStT600 Storage Server in the cluster controls up to two EXP700 Disk Storage Expansion Units, which expands the capacity of the storage server by 224 disk drives.
- Each FAStT700 Storage Server in the cluster controls at least one FAStT EXP700 Disk Storage Expansion Unit drive enclosure that contains Fibre Channel hard disk drives. The FAStT700 Storage Server supports 224 Fibre Channel hard disk drives. The FAStT EXP500 expansion unit supports a maximum of 220 Fibre Channel drives.
- The FAStT900 Storage Server functions with at least one external Fibre Channel drive expansion unit that contains Fibre Channel hard disk drives. The IBM FAStT EXP700 drive supports a maximum of 224 Fibre Channel hard disk drives when using a FAStT900 Storage Server. The EXP500 drive expansion unit supports a maximum of 220 Fibre Channel drives.

SCSI/RAID Storage controller adapters

The Cluster 1350 supports the following SCSI/RAID storage adapters:

- A ServeRAID™-6I Ultra320 SCSI Controller supports up to 16 arrays with support for a maximum of 160 hard disk drives.
- A ServeRAID-6M Ultra320 SCSI Controller supports eight arrays with support for a maximum of 30 hard disk drives.

Console

The console provides the monitor, keyboard, and mouse for the management node. The monitor is a flat-panel display that folds down and retracts into the rack.

KVM switch

The keyboard/video/mouse (KVM) switch enables the console to connect to all the nodes in the cluster from one terminal location. Storage and management nodes are connected directly to the KVM switch. For cluster nodes in the same rack, you can configure multiple nodes on one KVM switch port.

The Cluster 1350 can use the IBM NetBAY™ 2x8 Console Switch or the NetBAY Remote Console Manager (RCM). The RCM is the only supported KVM switch option that can be used with the @server 325.

10/100 Mb Ethernet switch

The 10/100 Mb Ethernet switch provides 10/100 Mb Ethernet connections for the cluster. The Cluster 1350 uses the Cisco Ethernet switch models 3550 XL (24-port) and 3550 XL (48-port). You can partition the switch to set up multiple independent LANs within the same switch.

Each model also provides two 1 Gb Ethernet ports for communication with the management node.

1 Gb Ethernet switch

The 1 Gb Ethernet switch provides a 1 Gb Ethernet trunk line between the management node and the cluster and storage nodes. The Cluster 1350 uses the Cisco Ethernet switch model 3508G-XL (8-port). The 1 Gb Ethernet switch uses an optical cable.

Port server

The port server provides serial connections for cluster modules. The Cluster 1350 can use the iTouch IR-8020–101 (20–port), or the iTouch IR-8040–101 (40–port).

The main purpose of the port server is to assign Ethernet addresses to cluster components. The port server can also act as a backup for Ethernet connections to download firmware and to check information stored in logs of cluster components.

High-Speed Myrinet switch

This is an optional 2 Gb switch for interconnecting cluster nodes and storage nodes. The Cluster 1350 uses the Myrinet models M3-E32 (5-slot), M3-E64 (9-slot), M3-E128 (17), M3F-PC164C-2 (PCI adapter), and M3F-PCIXD-2 (PCI card). The high-speed switch can replace the optional secondary Ethernet. It requires a Myrinet PCI adapter in each cluster node and storage node. The Myrinet switch uses an optical cable.

High-Speed Cisco switch

The Cluster 1350 can also use the Cisco Catalyst 4003 (3-slot) and Cisco Catalyst 4006 (6-slot) switches for a lower-cost high-speed solution.

Power management module

The power management module provides power to the service processors (in xSeries 335) and to the port servers. The Cluster 1350 uses the APC MasterSwitch Model AP9212. The power management module can supply up to eight connections. The power management module lets you shut down and restart a component from a remote site.

Power distribution unit (PDU)

Each rack contains one or more IBM NetBAY Rack Power Distribution Units (PDUs) or Distributed Power Interconnect (DPI) Power Distribution Units (PDUs). The PDUs mount sideways beside the rack space. The cluster supports the following types of PDUs:

- Rack PDU
- Front-end PDU

Rack PDUs provide power to components within a cabinet; front-end PDUs provide the connection to the external power source and distribute the power among the

rack PDUs. To eliminate the need for the front-end PDU, a rack PDU is directly connected to the external power source. Up to four front-end PDUs and up to 12 rack PDUs can be placed in each cabinet.

DANGER

The breaker switch on the PDU is not accessible. To turn off power to the cabinet, you must disconnect all the PDU power cords from the electrical outlets or from the individual PDU inlets.

Related publications

Your cluster might have features that are not described in the documentation that you received with the cluster. The documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in your cluster documentation. These updates are available from the IBM Web site. Complete the following steps to check for updated documentation, related documentation, and technical updates:

1. Go to **http://www.ibm.com/pc/support/**.
2. In the **Learn** section, click **Online publications**.
3. On the“ Online publications” page, in the **Brand** field, select **Servers**.
4. In the **Family** field, select **xSeries ***xxx*****.
5. Click **Continue** and select the online documents for the product.

Chapter 2. Unpacking the Cluster 1350

An IBM support team installs the IBM @server Cluster 1350. Complete the following steps before the IBM support team arrives on site to finish the installation:

1. Review the legal and safety information.
2. Review the physical, environmental, and electrical requirements in the *IBM @server Cluster 1350 Preinstallation Planning Guide* and make sure that the installation site is ready.
3. Unpack the cabinets only but not the other boxes. Depending on the cluster configuration that you order, the heavy cluster components are removed from the racks and packed separately to satisfy shipping requirements.

   Attention: Do not attempt to replace any equipment that was removed from the racks. The IBMsupport team will install all equipment back into its locations as part of the installation process.
4. Using the order that you placed for the cluster, identify the primary cabinet and verify its contents. If equipment is removed prior to shipping, check the bill of materials to make sure that all the equipment that is required for the primary cabinet was shipped with the order.
5. Using the order that you placed for the cluster, identify the expansion cabinets and verify their contents. If equipment was removed prior to shipping, check the bill of materials to make sure that all the equipment that is required for the expansion cabinets was shipped with the order.
6. Dispose of the packing material that comes with the cabinets.
7. Move the cabinets and any boxes containing extra equipment or other material to the installation site. The IBM support team completes the final cabinet placement.
8. Arrange for a phone line near the cabinets.

The IBM support team performs the final cabling and installation steps. After theIBM support team installs the cluster, connect the network cables.

Chapter 3. Proper placement of the cabinets

This chapter discusses the placement of your cluster cabinets and how to install the frame stabilizer foot to physically support each cabinet.

Customer responsibilities

Once the contents of all the cabinets of the Cluster 1350 are verified, you should move the cabinets and any boxes containing extra equipment and other materials to the location prepared for the installation.

Physical, environmental, and electrical requirements are outlined in the *IBM @server Cluster 1350 Preinstallation Planning Guide*. Do not move the cabinets to their final location if proper preparations are still being made to the space.

The Cluster 1350 is manufactured according to information provided at the time the order is placed. The side-to-side and front-to-back clearances for each cabinet are directly related to the load carrying capability of the floor in the location of the installation. Cabinet-to-cabinet cabling harnesses are custom made for each order to consider proper spacing of the cabinets. If the location of the installation changes from the location at the order time you should review the physical, environmental, and electrical requirements outlined in the preinstallation manual to make sure there are no incompatibilities.

Using the packing slip enclosed with the Cluster 1350, place the cabinets in their approximate final location. Each cabinet has installation labels to help you in this process.

The IBM support team determines the final cabinet placement and completes the necessary cabling and installation steps.

Cabinet placement

The IBM support team performs the remaining installation activities.

Use the following guidelines when placing cabinets:

- Cabinets can be placed side-by-side in contact with one another. Remember that to service any Power Distribution Unit (PDU) in a cabinet, you must remove the side covers. At least 30 inches of *working clearance* is required to make sure safe removal of a side cover and permit access to the PDU. If the cabinets are placed side-by-side in contact with one another you should have enough extra space around the cluster to make sure safe movement of the cabinets in the event a PDU needs service.

  Cabinet placement must not exceed floor loading limits.
- Cabinet placement must allow for access to both the front and back panels. At least 36 inches of *working clearance* is needed to remove or insert a module into the rack.
- Cables and cable harnesses are custom made to fit the order. If the location of the installation has changed since the time the order was placed, review the physical, environmental, and electrical requirements outlined in the preinstallation manual to make sure there are no incompatibilities.
- Make sure that the cabinets are arranged properly and adjust if needed. Refer to the packing slip and the cabinet labels to verify that all cabinets are in their proper location.

DANGER

Ensure that all rack-mounted units are fastened in the rack frame. Do not extend or exchange any rack-mounted units when the stabilizer is not installed.

To finish the cabinet placement, perform following steps:

1. Inspect the cabinets, components, and cable connections for shipping damage.
2. Install the cabinet stabilizer on each cabinet as required. Refer to Figure 4 for stabilizer kit installation.

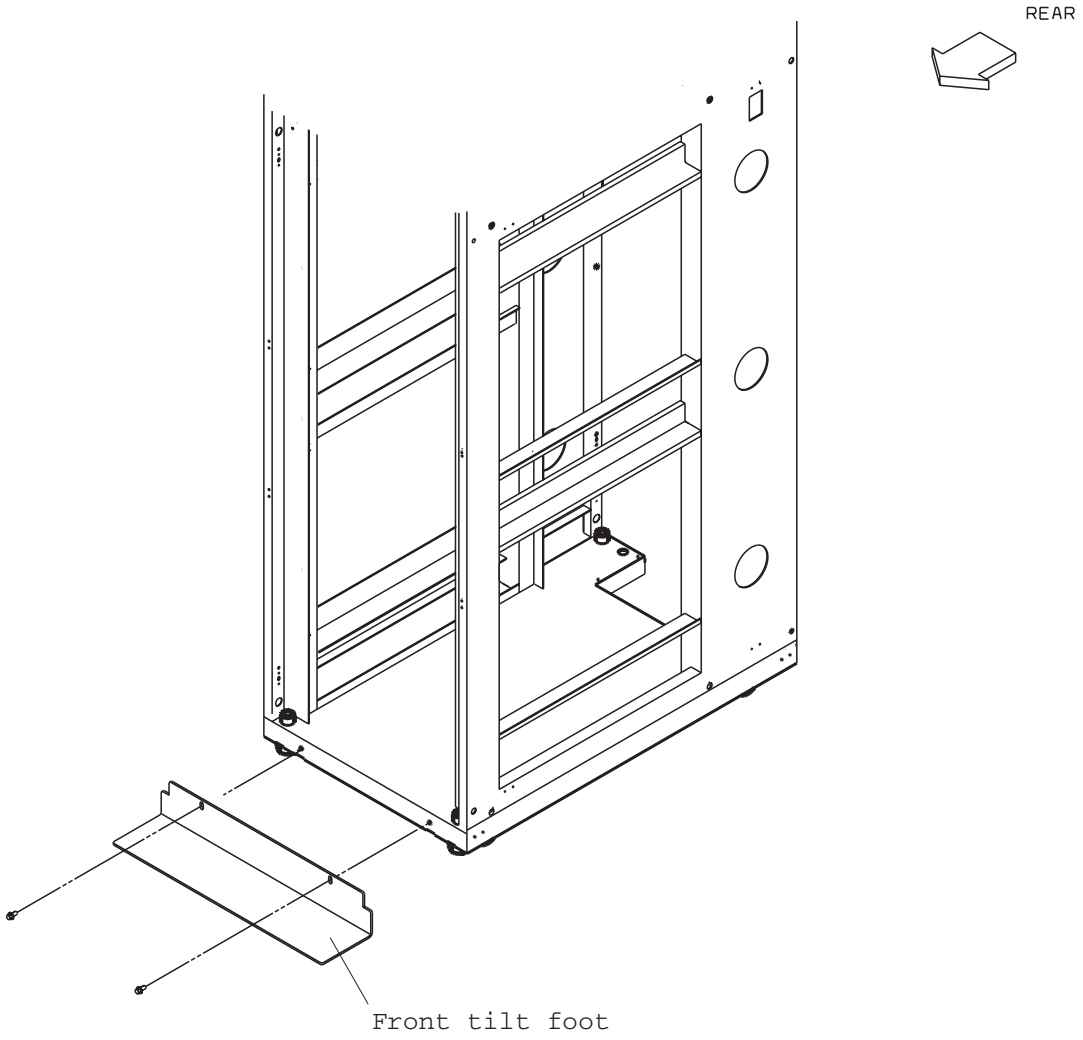


Figure 4. Frame stabilizer (tilt) foot installation

Chapter 4. Cabling

Overview of the Cluster 1350 cabling

The various types of cables in the Cluster 1350 system perform functions such as providing serial and Ethernet connections to cluster components.

Management VLAN

The management VLAN provides the private virtual LAN (VLAN) to manage the components in the cluster. This VLAN includes the following connections:

- RS485 connections to all cluster nodes and storage nodes through the Remote Supervisor Adapter (RSA) cards. These enable diagnostics and monitoring for the cluster and storage nodes.
- Serial connections to all cluster components. These provide a path for configuration of components in the cluster.
- 10/100 Ethernet connections from the RSA card in the management node to the 10/100 Ethernet switch.

Primary cluster VLAN

The primary cluster VLAN provides a 10/100 or a 10/100/1000 Ethernet (depending on the VLAN type selected) for communications with cluster nodes and storage nodes. This VLAN includes the following connections:

- A 10/100 or 10/100/1000 Ethernet to all cluster and storage nodes and other components. This provides the primary communications between the management node and the other components in the cluster.
- A gigabit Ethernet trunk line (shared with the management VLAN) for certain VLAN types only. This serves as a high-speed trunk line for all Ethernet communications within the cluster.

Optional secondary cluster

The optional secondary cluster provides a second 10/100/1000 Ethernet or 2 Gb Myrinet switch for communications with cluster and storage nodes. There are several options for the secondary cluster VLAN:

- A 10/100/1000 Ethernet using a Cisco 4003 or 4006 switch.
- A 2 Gb Ethernet using a high-speed Myrinet switch. The Myrinet switch uses optical cables for communication with cluster and storage nodes.

Keyboard/Video/Monitor

The keyboard/video/mouse (KVM) connects the keyboard/video/mouse (KVM) ports on all nodes (cluster, storage, and management) to a single console through a central switch.

Fiber channel

The Fibre channel provides Fibre channel connections between the storage nodes and the storage servers, and between the storage servers and the Storage Expansion Units.

Power Distribution Units

The power distribution unit provides the power to the cluster components. This includes both the AC power provided to the entire cabinet through the PDUs and

remote power provided to the Remote Supervisor Adapter (RSA) boards and the port servers through the Power Management Module.

VLAN options

The Cluster 1350 supports a variety of VLAN options. Currently, there are six basic configurations. Point-to-point wiring information is printed on each cable. Check the information on the cables in the primary rack and refer to the following tables to determine which VLAN option was used in the cluster.

Table 2. Type 1 VLAN 10/100 Ethernet

Device	Management VLAN	10/100 Primary Cluster VLAN	Comments
Management node	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 3508 GBIC	
KVM switch	Connects to Cisco 3550		
Cisco 3508 Gb switch		GBIC connects to management node Ethernet 1	
iTouch port server	Connects to Cisco 3550		
APC switch	Connects to Cisco 3550		
Cisco 3550 10/100 switch		GBIC connects to Cisco 3508	
Cluster nodes		Ethernet 0 connects to Cisco 3550	
Storage nodes	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 3508 GBIC	
FAStT200HA	Connects to Cisco 3550		Uses both jacks
FAStT600	Connects to Cisco 355		Uses both jacks
FAStT700	Connects to Cisco 3550		Uses both jacks
FASt900	Connects to Cisco 3550		Uses both jacks

Table 3. Type 2 VLAN 10/100/1000 Ethernet

Device	Management VLAN	Gbit Primary Cluster VLAN	Comments
Management node	• Ethernet 1 connects to Cisco 400x • Ethernet 2 connects to Sup I or Sup III		06P3701 or 22P7801
KVM switch	Connects to Cisco 400x		
iTouch port server	Connects to Cisco 400x		
APC switch	Connects to Cisco 400x		
Cisco 4003 and/or 4006 switch	• Sup I connects to management node • Sup III connects to management node	• Gbit connects to management node Ethernet1 • Sup III uplink connects to management node PCI card	

Table 3. Type 2 VLAN 10/100/1000 Ethernet (continued)

Cluster nodes		Ethernet 0 connects to Cisco 400x	
Storage nodes	Ethernet 2 connects to Cisco 400x	Ethernet 1 connects to Cisco 400x	
FAStT200HA	Connects to Cisco 400x		Uses both jacks
FAStT600	Connects to Cisco 400x		Uses both jacks
FAStT700	Connects to Cisco 400x		Uses both jacks
FAStT900	Connects to Cisco 400x		Uses both jacks

Table 4. Type 3 VLAN. 10/100 Ethernet with 10/100/1000 public high speed VLAN

Device	**Management VLAN**	**10/100 Primary Cluster VLAN**	**Gbit customer public high speed VLAN**
Management node	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 3508 GBIC	
KVM switch	Connects to Cisco 3550		
Cisco 3508 (4003) Cisco 3508 (4006)		Copper GBIC connects to management node Ethernet 1 Copper GBIC connects to management node Ethernet 1	Copper GBIC connects to Cisco 4003 Gbit Fiber GBIC connects to Sup III uplink
iTouch port server	Connects to Cisco 3550		
APC switch	Connects to Cisco 3550		
Cisco 3550 10/100 switch		Copper GBIC connects to Cisco 3508	
Cisco 4003 and/or 4006 switch	SupI connects to Cisco 3550 SupIII connects to Cisco 3550		Gbit connects to 3508 copper GBIC SupIII uplink connects to Cisco 3508 fiber GBIC
Cluster nodes		Ethernet 0 connects to Cisco 3550	Ethernet 2 connects to Cisco 400x Gbit
Storage nodes	Ethernet 1 Alias connects to Cisco 3508 copper GBIC	Ethernet 1 Alias connects to Cisco 3508 copper GBIC	Ethernet 2 connects to Cisco 400x Gbit
FAStT200HA	Connects to Cisco 3550		
FAStT600	Connects to Cisco 3550		
FAStT700	Connects to Cisco 3550		
FAStT900	Connects to Cisco 3550		

Table 5. Type 4 VLAN. 10/100/1000 Ethernet with 2 Gbit public high speed VLAN

Device	Management VLAN	10/100 Primary Cluster VLAN	Myrinet customer public high speed VLAN
Management node	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 3508 copper GBIC	
KVM switch	Connects to Cisco 3550		
3508 Gbit switch		Copper GBIC connects to management node Ethernet 1	
iTouch port server	Connects to Cisco 3550		
APC switch	Connects to Cisco 3550		
Cisco 3550 10/100 switch		Copper GBIC connects to Cisco 3508	
Myrinet 32, 64, or 128 (both jacks), D card	Connects to Cisco 3550		
Cluster nodes		Ethernet 0 connects to Cisco 3550	Myrinet adapter
Storage nodes	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to copper Cisco 3508 GBIC	Myrinet adapter
FAStT200HA	Connects to Cisco 3550		
FAStT600	Connects to Cisco 3550		
FAStT700	Connects to Cisco 3550		
FAStT900	Connects to Cisco 3550		

Table 6. Type 5 VLAN 10/100/1000 Ethernet with 10/100/1000 Ethernet public high speed VLAN

Device	Management VLAN	Gbit Primary Cluster VLAN	Gbit customer public high speed VLAN
Management node	• Ethernet 1 Alias connects to Cisco 400x • Ethernet 2 connects to Sup I or Sup III	• Ethernet 1 connects to 4003 • Fiber Channel PCI card connects to 4006 SupIII uplink	Copper or Fiber Channel PCI connects to public network
KVM switch	Connects to Cisco 400x		
iTouch port server	Connects to Cisco 400x		
APC switch	Connects to Cisco 400x		
Cisco 4003 and/or 4006 switch	• Sup I connects to management node Ethernet 2 • Sup III connects to management node Ethernet 2	• Gbit connects to management node Ethernet 1 • Sup III uplink 1 connects to Fiber Channel PCI card	SupIII uplink 2 connects to public network

Table 6. Type 5 VLAN 10/100/1000 Ethernet with 10/100/1000 Ethernet public high speed VLAN (continued)

Cluster nodes		Ethernet 0 connects to Cisco 400x	Ethernet 2 connects to Cisco 400x
Storage nodes	Ethernet 1 Alias connects to Cisco 400x	Ethernet 1 Alias connects to Cisco 400x	Ethernet 2 connects to Cisco 400x
FAStT200HA (both jacks)	Connects to Cisco 400x		
FAStT700 (both jacks)	Connects to Cisco 400x		

Table 7. Type 6 VLAN.10/100/1000 Ethernet with 2 Gbit Myrinet public high speed VLAN

Device	**Management VLAN**	**Gbit Primary Cluster VLAN**	**Myrinet customer public high speed VLAN**
Management node	• Ethernet 1 Alias connects to Cisco 400x • Ethernet 2 connects to Sup I or Sup III	• Ethernet 1 Alias connects to Cisco 400x • Fiber Channel PCI card (06P3701 or 22P78021) connects to Cisco 4006 Sup III uplink	
KVM switch	Connects to Cisco 400x		
iTouch port server	Connects to Cisco 400x		
APC switch	Connects to Cisco 400x		
Myrinet 32, 64, 128, or PCI card (both jacks)	Connects to Cisco 400x		
Cluster nodes		Ethernet 0 connects to Cisco 400x	Myrinet adapter
Storage nodes	Ethernet 2 connects to Cisco 400x	Ethernet 1 connects to Cisco 400x	Myrinet adapter
FAStT200HA	Connects to Cisco 400x		
FAStT700	Connects to Cisco 400x		

For large clusters that use VLAN types 2, 5 or 6 it is necessary to add additional Cisco 400x switches. If the cluster has more than one Cisco 400x switch in the primary rack then refer to the following tables.

Table 8. Type 2 VLAN with multiple Cisco 400x switches

Device	**Management VLAN**	**Gbit Primary Cluster VLAN**	**Comments**
Management node	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 3508 copper GBIC	
KVM switch	Connects to Cisco 3550		

Table 8. Type 2 VLAN with multiple Cisco 400x switches (continued)

iTouch port server	Connects to Cisco 3550		
3508 Gbit switch		Connects to 3550 copper GBIC	
APC switch	Connects to Cisco 3550		
3550 10/100 switch		Cisco 3550 copper uplink to Cisco 3508	
Cisco 4003 and/or 4006 switch	• Sup I connects to 3550 • Sup III connects to 3550	• Gbit connects to 3508 copper GBIC • Sup III uplink connects to 3508 fiber GBIC	
Cluster nodes		Ethernet 0 connects to Cisco 400x	
Storage nodes	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 400x	
FAStT200HA	Connects to Cisco 3550		Uses both jacks
FAStT700	Connects to Cisco 3550		Uses both jacks

Table 9. Type 5 VLAN with multiple Cisco 400x switches

Device	**Management VLAN**	**Gbit Primary Cluster VLAN**	**Gbit customer public high speed VLAN**
Management node	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 3508 copper GBIC	Fiber Channel PCI connects to public network
KVM switch	Connects to Cisco 3550		
iTouch port server	Connects to Cisco 3550		
3508 Gbit switch	Connects to Cisco 3550 copper uplink	Connects to management node Ethernet 1	Fiber GBIC connects to management node
APC switch	Connects to Cisco 3550		
3550 10/100 switch	Connects to management node Ethernet 2		
Cisco 4003 and/or 4006 switch	• Sup I connects to 3550 • Sup III connects to 3550	• Gbit connects to 3508 copper GBIC • Sup III uplink 1 connects to 3508 fiber GBIC	• Gbit connects to 3508 copper GBIC • Sup III uplink 2 connects to 3508
Cluster nodes		Ethernet 0 connects to Cisco 400x	Ethernet 2 connects to Cisco 400x
Storage nodes	Ethernet 1 Alias connects to Cisco 400x	Ethernet 1 Alias connects to Cisco 400x	Ethernet 2 connects to Cisco 400x
FAStT200HA (both jacks)	Connects to Cisco 3550		

Table 9. Type 5 VLAN with multiple Cisco 400x switches (continued)

FAStT700 (both jacks)	Connects to Cisco 3550		

Table 10. Type 6 VLAN with multiple Cisco 400x switches

Device	**Management VLAN**	**Gbit Primary Cluster VLAN**	**Myrinet customer public high speed VLAN**
Management node	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 3508 copper GBIC	Fiber Channel PCI connects to public network
KVM switch	Connects to Cisco 3550		
iTouch port server	Connects to Cisco 3550		
3508 Gbit switch	Connects to Cisco 3550 GBIC	Connects to management node Ethernet 1	
APC switch	Connects to Cisco 3550		
3550 10/100 switch	Connects to management node Ethernet 2		
Cisco 4003 and/or 4006 switch	• Sup I connects to Cisco 3550 • Sup III connects to Cisco 3550	• Gbit connects to Cisco 3508 copper GBIC • Sup III uplink connects to Cisco 3508 fiber GBIC	
Myrinet 32, 64, 128, or PCI card (both jacks)	Connects to Cisco 3550		
Cluster nodes		Ethernet 0 connects to Cisco 400x	Myrinet adapter
Storage nodes	Ethernet 2 connects to Cisco 3550	Ethernet 1 connects to Cisco 400x	Myrinet adapter
FAStT200HA	Connects to Cisco 3550		
FAStT700	Connects to Cisco 3550		

General information

Most of the cabling in a Cluster 1350 system is installed during manufacturing. However, there are three instances where cables must be installed at a customer site:

- Cables between cabinets
- Replacements for faulty cables
- Cables to replacement components

Any cable that fails at the customer site or is connected to components that must be replaced must be reconnected at the customer site.

Attaching the cables

Cables and the cable harnesses in each cabinet are labeled with information that tells where to connect each end of the cable. Each label will identify the device or node it connects to, and where appropriate, its port number.

Depending on the country of manufacture the label scheme will vary. Before you begin attaching cables take some time to familiarize yourself with the information on the labels.

When initially installing a Cluster 1350 start with the primary cabinet. Once you have attached the intracabinet cables inside the primary cabinet, move on to each expansion cabinet and use the information printed on each cable label to properly attach the cables found there.

Once you have reattached any cables in the primary cabinet and expansion cabinets you can move on to attaching the cables that run between cabinets. This is called the intercabinet cabling and the following types of cables are involved:

- 1 Gb or 2 Gb Fibre Channel (optical)
- 1 Gb Ethernet (optical)
- 2 Gb Myrinet (optical)
- 10/100/1000 Ethernet (copper)
- KVM (copper)

For a complete listing of all available cables and their part numbers refer to the Cluster 1350 information contained on the IBM InfoTips web site.The same information is also available in the IBM Current Object Repository (CORE) system.

1 Gb Ethernet cabling

The 1 Gb Ethernet provides a high-speed optical trunk line for VLAN communications with the management node. Figure 5 on page 21 schematically shows a possible intercabinet cabling for a large cluster configuration. VLAN types 1, 3, and 4 would follow this model.

Attention: All intercabinet cables have labels at both ends of each cable. You can use the information on the label to create a site map to document all cable routing.

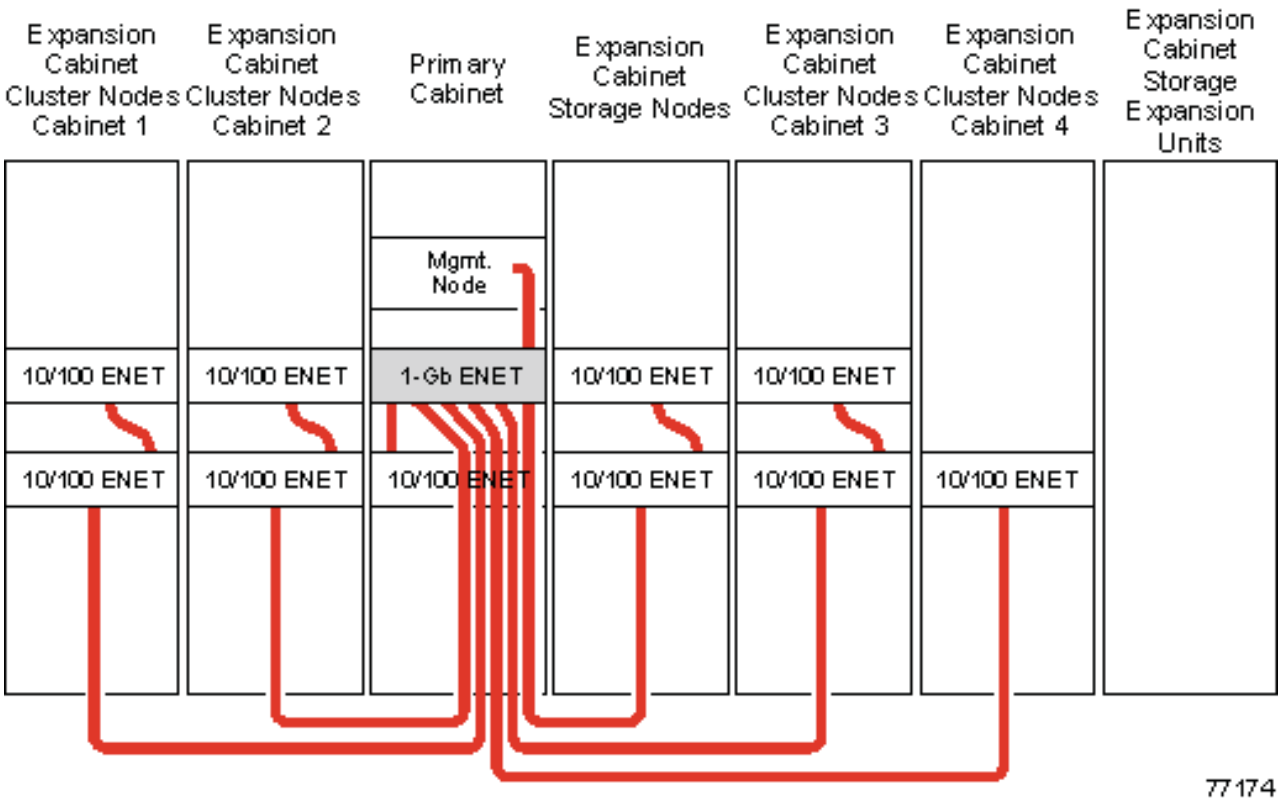


Figure 5. Intercabinet cabling for the 1 Gb Ethernet connections (VLAN types 1, 3 and 4)

High-speed (Myrinet) switch cabling

The Myrinet high-speed switch provides an optional 2 Gb optical network for communications between cluster nodes and storage nodes. Figure 6 on page 22 shows a schematic of the Myrinet optical cabling in a large cluster. VLAN types 2, 5, and 6 would follow this model.

Attention: All intercabinet cables have labels at both ends of each cable. You can use the information on the label to create a site map to document all cable routing.

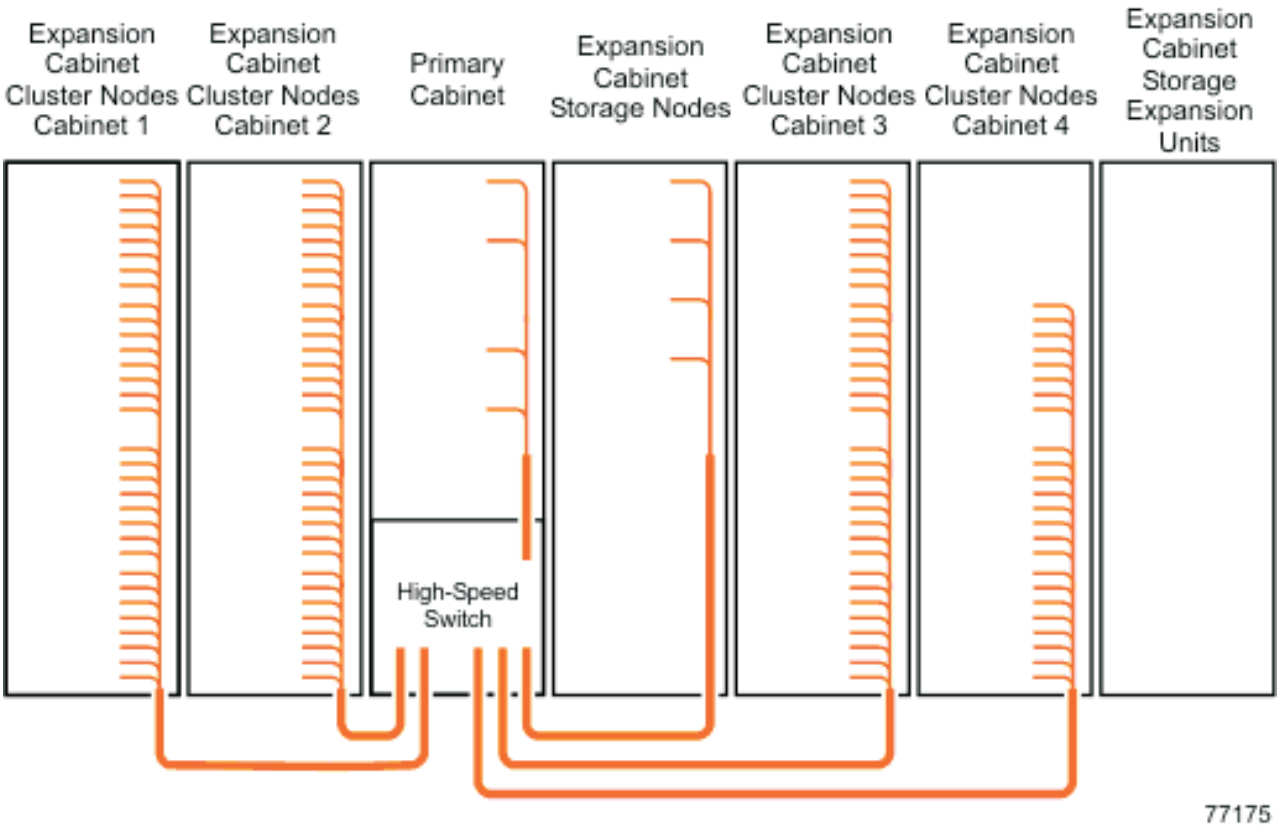


Figure 6. Intercabinet cabling for Myrinet connections (VLAN types 4 and 6)

10/100/1000 Ethernet cabling

The 10/100/1000 Ethernet switch provides an optional 10/100/1000 network for communications between cluster nodes and storage nodes. Figure 6 shows a schematic of the cabling in a large cluster. VLAN types 2, 3,5 and 6 would follow this model.

Attention: All intercabinet cables have labels at both ends of each cable. You can use the information on the label to create a site map to document all cable routing.

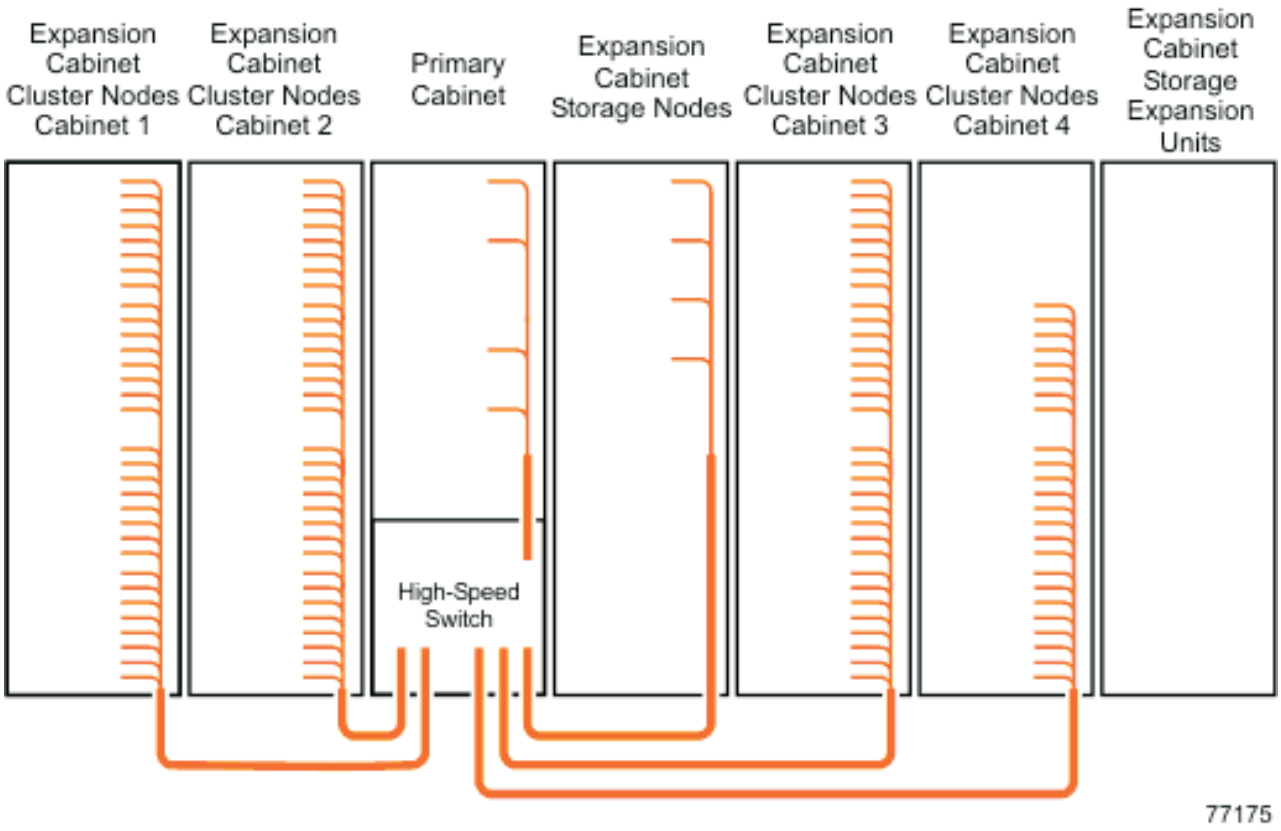


Figure 7. Intercabinet cabling for Gbit Ethernet connections (VLAN types 2,3,5 and 6)

Fibre Channel cabling

Fibre Channel is used to connect storage nodes to storage servers, and to connect storage servers to storage expansion units. Figure 8 on page 24 shows a schematic diagram of Fibre Channel cabling in a large cluster.

Attention: All intercabinet cables have labels at both ends of each cable. You can use the information on the label to create a site map to document all cable routing.

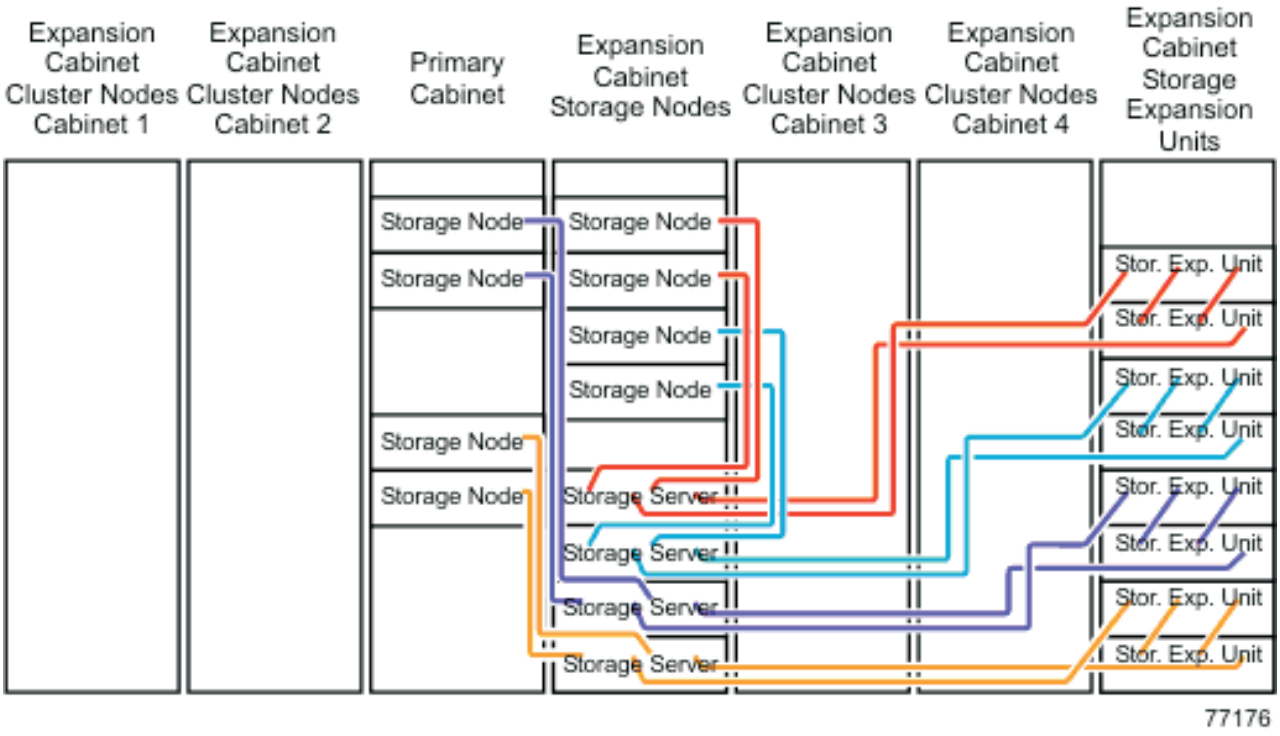


Figure 8. Intercabinet cabling for Fibre Channel connections. To avoid making the storage node a single point of failure, connect two storage nodes to each storage server, as shown.

KVM cabling

The KVM switch allows a maximum of eight connections. Figure 9 on page 25 shows an example of KVM cabling for a cluster configuration. Use the following guidelines for cabling the KVM switch:

- Use the information on each end of each cable to create a site map.
- When routing a KVM cable from a cabinet containing cluster nodes to another cabinet containing the KVM switch, connect a C2T-to-KVM cable to the cluster nodes and use a KVM extension cable to add sufficient length to reach the KVM switch.
- Multiple KVM switches can be connected in series. Cluster nodes (xSeries 335) can be connected in series to a single KVM switch port (up to 40 cluster nodes). But the management node and all the storage nodes each require a separate KVM switch port. Certain systems may require a second KVM switch. The second switch should be located in the expansion cabinet that contains the additional storage nodes.
- When using two KVM switches, connect Port A (the console port) of Switch 2 to Port 8 of Switch 1. Use a KVM extension cable to make the connection between the two cabinets. If more length is needed, use two KVM extension cables linked together.

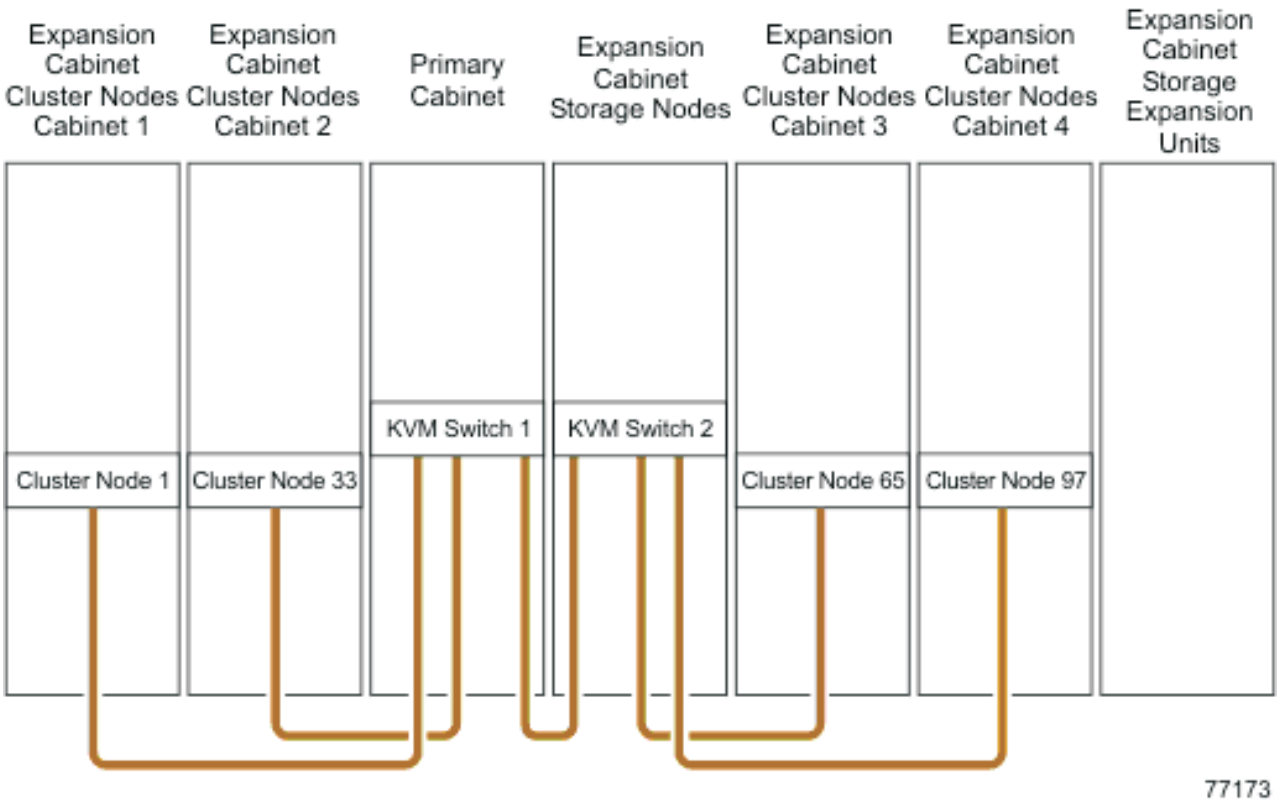


Figure 9. Intercabinet cabling for KVM connections

Remote Console Manager cabling

The Remote Console Manager (RCM) switch has sixteen ACT connections (KVM over RJ45/CAT5) along with one KVM connection for the console. Use the following guidelines for cabling the RCM switch:

- Use the information on each end of each cable to create a site map.
- When routing a CAT5 KVM cable from a cabinet containing cluster nodes to the cabinet containing the RCM, use a CCO cable and a CAT5 cable sufficiently long enough to reach the RCM switch.
- Multiple KVM switches can be connected in series.
- Up to 40 cluster nodes (xSeries 335) can be connected in series to each ACT port on the RCM. The management node and all the storage nodes may also be daisy-chained, with up to sixteen per ACT port. Multiple RCMs may not be daisy-chained together. The RCM may be connected to an Ethernet network to allow for remote access to the consoles of the servers over the network.

Replacing a defective cable in a harness

If a cable in a harness is defective, replace the cable as follows:

1. Disconnect both ends of the defective cable from their ports. Do not remove any other connectors from their ports.
2. If possible, remove the cable from the harness. If that can not be done, use a pair of wire cutters to cut off the connectors at both ends of the defective cable. This prevents someone from mistakenly reconnecting the cable, thinking that it has accidentally been left unconnected.

3. Install a single cable between the two empty ports. Use a wire tie to attach the cable to the harness that contains the defective cable. This identifies the replacement cable as belonging to this harness.
4. Label the replacement cable so it is clearly identified as a replacement.

Chapter 5. Turning on the cluster

Initial Cluster 1350 procedure

The IBM @server Cluster 1350 is shipped without an operating system installed. Before turning on an entire Cluster 1350 system, first check all the connections in the expansion cabinets and primary cabinet. Once you have verified that all connections are secure, turn on the expansion cabinets containing storage nodes, storage servers, and storage expansion units. Turn on the primary cabinet last.

Checking connections in the expansion cabinets

1. Verify that the breaker switches for the source power are all turned off.
2. Open the side and rear doors of the cabinet.
3. From the side of the cabinet check that all the power cables between the rack PDUs and the front-end Power Distribution Units (PDUs) are fully seated.
4. From the back of the cabinet, push on all the power plugs running from the rack-mounted devices to the PDUs to verify that the cables are fully seated.
5. Connect power to the PDUs.
   a. Plug the power cable into the PDU.
   b. Draw the power cable through the opening at the base of the cabinet.
   c. Plug the power cable into the wall outlet or other appropriate receptacle.
   d. Turn on the breaker switch for the source power.
   e. Make sure the PDU circuit breakers are turned on.
6. Verify that all internal PDUs are turned up by viewing the power LEDs on components that are connected to the PDUs.
   - Servers display a blinking green LED on the front panel when power is applied.
   - The following devices have no power switch and will turn on automatically when the PDUs are turned on. Verify that these components have power applied.
     – KVM Switch
     – Cisco 10/100 switch
     – Cisco Gigabit switch
     – In-Reach Port server

   All rack-mounted devices are powered by the internal PDU.

Checking connections in the primary cabinet

1. Verify that the source power breaker switches are all turned off.
2. Open the side and rear doors of the cabinet.
3. From the side of the cabinet check that all the power cables between the rack Power Distribution Units (PDUs) and the front-end PDUs are fully seated.
4. From the back of the cabinet, push on all the power plugs running from the rack-mounted devices to the PDUs to verify that the cables are fully seated.
5. Connect power to the PDUs. Use the NEMA L6-20, 280VAC, single-phase power cable.
   a. Plug the power cable into the PDU.
   b. Draw the power cable through the opening at the base of the cabinet.
   c. Plug the power cable into the wall outlet or other appropriate receptacle.
   d. Turn on the breaker switch for the source power.
   e. Make sure the PDU circuit breakers are turned on.
6. Verify that all internal PDUs are switched on by viewing the power-on LEDs on the components that are connected to the PDUs.
   - Servers display a blinking green LED on the front panel when power is applied.

- The following devices have no power switch and switch on automatically with the PDUs. Verify that these components have power:
  - KVM switch
  - Cisco 10/100 switch
  - Cisco Gigabit switch
  - In-Reach Port server

  All rack-mounted devices are powered by the internal PDU.

Switching on the expansion cabinets

1. Switch on the cluster nodes manually with the power switch.
2. Verify that every Remote Supervisor Adapter (RSA) card has power. A green LED on the card will light when the card has power.
3. Once an expansion cabinet is turned on, verify that all front panel LEDs on the cluster nodes are steady ON, otherwise you will not see all the nodes in the configuration.

Repeat the procedure for every expansion cabinet in the cluster before moving on to the primary cabinet.

Switching on the primary cabinet

Switch on the following devices in the order listed:

1. Storage expansion units - switch the circuit breakers on the back of the device to the **On** position.
2. Storage controllers - Switch the circuit breakers on the back of the device to the **On** position.
3. Management node, perform the following steps:
   a. Turn the power switch on the front of the device to the **On** position.
   b. Verify that the system passes POST with no errors. During the boot process verify that the PXE BOOT attempts to run. If not, press F1 to enter the Setup utility and add **Network** as a third boot option.
   c. Once the system boot has completed the screen will show the *No operating system* icon. If there are any yellow warning LEDs on the management node, fix the underlying condition before continuing.
4. Cluster nodes
   - Turn on the cluster node 1 and verify that the system passes POST with no errors.
5. Storage nodes
   - Turn the power switch on the front of the device to the ON position.
   - During the boot process verify that the PXE BOOT attempts to run. If not, press F1 to enter the Setup utility and add **Network** as a third boot option.
   - Once the system boot completes, the monitor screen displays the *No operating system* icon. If there are any yellow warning LEDs on the cluster node, fix the underlying condition before continuing. Repeat the procedure for all cluster nodes in the cluster.
   - In order for the storage nodes to see the peripheral devices, these devices must be turned on and online before you turn on the storage nodes.
6. Verify that all CAT-5 and fibre connections have a green link LED.
7. Verify that every Remote Supervisor Adapter (RSA) card has power applied. A green LED on the card faceplate will light up when power is applied to the card. Connect your laptop to the Cisco 10/100 switch and configure it to use IP address **172.22.30.20** with a net mask of **255.255.0.0**. Sign in to each RSA card using the Web browser and verify that each is present. `Ping` each communication device (Cisco switches, In-Reach port server, power management module, and KVM switch).

If the system appears to be functionally sound, theIBM support team will turn control over to the party installing the software.

Verifying the installation of the Linux Cluster Installation Tool

The installation materials include a LCIT startable CD. With your 1350 Cluster, you also receive tab files that detail the rack hardware configuration. To make sure that you install the cluster components correctly, run the installation diagnostics to generate a new set of tab files. Compare the new tab files to the tab files that came with your cluster to make sure that both sets of tab files are identical. Complete the following steps to run the diagnostic installation tool:

1. Turn the power on the management node and insert the LCIT CD into the CD-ROM drive. Workspace 1 opens as a gray screen.
2. Anywhere in the open Workspace window, right-click and select **LCIT 3.0**. The LCIT window opens.
3. Click **Enable** for each interface, then click **Next** to start the Discovery wizard. The Discovery wizard polls all devices configured in the applicable search ranges and populates the LCIT IP Addresses tab with all device IP and MAC addresses found in the cluster.
4. Click **Cluster View** and click **Refresh View**. This updates your network configuration with all discovered devices.
5. Click an RSA device and click **Power Off**, then click **Power On** to restart all the nodes in the selected RSA. Repeat this step for each RSA device.
6. Click **Tab Files** and click **Write Tab Files** to update the tab files in the /LCIT/bin directory.

Lights out or brown out

The following sequence should occur during a lights out or brown-out scenario.

1. The system is up and running typical applications.
2. A lights out or brown out event occurs. The system turns off then turns back on via an external source.
3. All nodes turn on to the last known state (on/off). If the last known state is on, then the nodes boot to a login prompt.
4. Log files show system restart events on nodes and on RSA cards. Check the following log files.
   - */var/log/messages*
   - */var/log/csm/installnode.log*
   - Remote Supervisor Adapter (RSA) event log
   - BIOS event log

Related topics

Appendix B, “Error and event logs”, on page 79

Chapter 6. Installing the software

These installation steps are used by IBM Global Services or the customer's agent for the initial software setup of a Cluster 1350. There are five basic steps to complete:

1. Install a supported distribution of Linux. Refer to Table 11 for all supported versions of Linux and other supported versions of Cluster 1350 software and firmware.
2. Install Cluster Systems Management (CSM).
3. Configure the storage nodes.
4. Push the system image to all nodes in the cluster.
5. Test the configuration.

The installation time is about 8 hours per cabinet.

Before you begin the software installation process, refer to "Software version matrix" to verify that you have all the required material.

Attention: The Cluster 1350 should be maintained only by system administrators experienced with Red Hat Linux, DHCP, NFS, and Linux networking and administration.

Software version matrix

The Cluster 1350 requires certain levels of a supported Linux distribution and Cluster System Management (CSM) in order to operate correctly. Before you begin the software installation process, make sure you have collected all the appropriate levels of operating system kernel, management software, device drivers, and other firmware needed for building a working system image. Table 11 shows the supported software and firmware versions.

Changing the versions of any components will adversely affect IBM's ability to service and support the cluster.

Table 11. Cluster 1350 supported software and firmware versions - October 2003

Product	Versions
Red Hat Linux	v9.0
Red Hat Linux Advanced Server	v2.1
SuSE Linux	v8.2 Professional
SuSE Linux Enterprise Server (SLES)	v8.0
RHEL	• A0.0.12 • v3.0 WorkStation
Cluster System Management (CSM)	csm v1.3.2
Cisco 3508 Gb switch	• v12.1(9)EA1c • 3500L-C3H25-MZ-120-5.2-xv.1.bin
Cisco 35xx Ethernet switch	• v12.1(9) • 3500L-C3H25-MZ-120-5.3-wc.1.bin
Cisco 400x Ethernet switch	v12.1(13)EW1

Table 11. Cluster 1350 supported software and firmware versions - October 2003 (continued)

Product	Versions
Broadcom Gigabit Ethernet	bcm5700-ver 6.0.2
Ethernet Intel Single Port 10/100 Adapter	e1000-4.3.17.tar.gz
Fiber FAStT Adapter	• BIOS: v 3.01.31 • Driver: v6.01.00-fo
FAStT 700Raid Controller	v5.4
APC power switch	• SNMP AOS v3.03 • Masterswitch App v2.20
IBM NetBAY console switch	• S2.0.0.I • F1.1.0 • H0.0.10.02.00 • A0.0.12
Myrinet 2000 Fiber PCI-2B card	GM-v1.6.4
@server 325	• BIOS: v1.17 • Diagnostics: v2.0.1267A • Processor: v1.2.2
xSeries335	• BIOS: v1.05 • ISMP: v1.03 • Diagnostics: v1.00 • Remote Supervisor Adapter F/W: v1.03
BladeCenter	• BIOS: v1.03 • ISMP: v15 • Diagnostics: v1.00
xSeries 345	• BIOS: v1.17 • ISMP: v1.08 • Diagnostics: v1.04 • Remote Supervisor Adapter F/W: v1.17
xSeries 360	• BIOS: v1.08 • Diagnostics: v3.01
ServeRAID Driver	6.10.20

Downloading drivers and firmware

If drivers and firmware are needed, go to http://www-3.ibm.com/pc/support/site.wss/multiplefiledownload.do.

Installing a supported version of Linux

The Cluster 1350 is shipped without an operating system. The customer or the customer's agent is responsible for securing a valid copy of the operating system for installation. Refer to Table 11 on page 31 for more information on the supported distributions of Linux.

Use the detailed installation instructions provided with your software kit to install the Linux software. If you are missing your documentation for installing Linux, refer to the following web site: http://www.redhat.com/docs/manuals/linux/

Installation of the operating system begins with the management node in the primary cabinet.

Installing Cluster System Management software

To install Cluster System Management (CSM), refer to the installation instructions provided with your CSM software kit. You can also access software installation information from the following URL:

http://www-1.ibm.com/servers/eserver/clusters/library/am7LXstp.pdf

Installing General Parallel File System system management software

To install the General Parallel File System (GPFS) software, refer to the installation instructions provided with your GPFS software kit. You can also access software installation information from the following URL:

http://www-1.ibm.com/servers/eserver/clusters/library/gpfs.html.

Configuring the storage nodes

Prerequisites

The procedure assumes the following prerequisites:

- Red Hat Linux version 9.0 is installed and running from a local drive.
- The FAStT Storage Server is properly configured and connected to a Host Bus Adapter (HBA).
- The FAStT drives in the storage server are configured into different RAID groups, storage groups, and LUNS via the software provided with the FASTt Storage Server.

Issues

Because of the way the Red Hat Linux version 9 loads SCSI drivers and assigns them to */dev/sda*, */dev/sdb*, problems can result if more than one SCSI host adapter board (Adaptec SCSI controller for local drives and Qlogic HBA for Triton connection) is installed on the system and you use the `scsi_hostadapter` alias. When the system is rebooted, the operating system will detect the Qlogic controller prior to detecting the Adaptec, which will cause the system to panic. To avoid this issue, follow the Installation procedure and modify the order of the contents of the /etc/modules.conf file.

Installation procedure

1. If not already done, turn off the storage controllers or disconnect the fibre cable running to each storage controller.
2. For Red Hat Linux version 9, edit the */etc/modules.conf* file to put the host adapters in the correct order and to add the parameter `scsi_mod max_scsi_luns` to the file.

Attention:

- Because the system is running a modular kernel, the Adaptec SCSI device driver (″alias scsi_hostadapter aic7xxx″) must be probed before any other SCSI adapters so that the kernel will be able to find the root device during the initialization phase. Also, the Qlogic Qla driver (″alias scsi_hostadapter2 qla2x00″) must be the last SCSI host adapter listed in the file.
- If there are other SCSI host adapter boards installed on your system and the scsi_hostadapter alias is used, define a different alias for the qlogic Qla driver and make sure to add it after the other SCSI modules so this doesn't cause the SCSI devices names already in use to be renumbered on next boot. You can do this by appending a number at the end of the scsi_hostadpter word, for example, *alias scsi_hostadapterN qla2x00* [where *N* is an alphanumeric number from 1-9].

For example:

```
Original modules.conf:
alias eth0 e1000
alias scsi_hostadapter qla2x00
alias scsi_hostadapter1 aic7xxx
alias scsi_hostadapter2 ips
alias eth1 e1000
alias parport_lowlevel parport_pc
alias scsi_hostadapter3 aic7xxx
alias scsi_hostadapter4 aic7xxx
alias usb-controller usb-ohci

Modified modules.conf:
alias eth0 e1000
alias scsi_hostadapter1 aic7xxx
alias scsi_hostadapter2 ips
alias eth1 e1000
alias parport_lowlevel partport_pc
alias scsi_hostadapter3 aic7xxx
alias scsi_hostadapter4 aic7xxx
alias scsi_hostadapter5 qla2x00
alias usb-controller usb-ohci
options scsi_mod max_scsi_luns=128
```

For SuSE Linux 8.2 and SLES 8.0: edit the /etc/modules.conf file to make sure it contains the following lines:

```
alias scsi_hostadapter ips
alias scsi_hostadapter1 qla2300
options scsi_max_scsi_luns=128
```

For SuSE Linux 8.2 append the /etc/sysconfig/kernel file with the following information line:

```
INITRD_MODULES="ips qla2300 reiserfs"
```

For SLES 8.0 edit the /etc/rc.config file to contain the following line:

```
INITRD_MODULES="ips qla2300"
```

3. For Red Hat Linux version 9 rebuild the two `initrd` images. `mkinitrd` will not allow you to make a ramdisk image if it detects one already present with the same name, so the first two commands will rename the old images:

```
mv /boot/initrd-2.4.2-2.img /boot/initrd-2.4.2-2_orig.img
mv /boot/initrd-2.4.2-2smp.img /boot/initrd-2.4.2-2smp_orig.img
mkinitrd initrd-2.4.2-2.img 2.4.2-2
mkinitrd initrd-2.4.2-2smp.img 2.4.2-2smp
```

For SuSE 8.2 and SLES 8.0 run the `mkinitrd` command to create a *boot/initrd* directory and then run *lilo*.

4. If a Remote Supervisor Adapter (RSA) card was installed, reboot and load the setup floppy or CD to configure the network. Assign the same configuration information for the RSA adapter (name, IP, host name) as used before. Go to the following site to download the RSA and ASM Process or Firmware Update Diskette utility: http://www.pc.ibm.com/qtechinfo/MIGR-4JTS2T.html
5. If you have custom modifications, configure the kernel.
6. Reboot the node.

Defining nodes

Before you can copy (push) the system image to all nodes in the Cluster 1350, you must first define the nodes for which you do not know the IP address.

Defining nodes using CSM

You can either use a node-definition file to define the nodes, console servers, and service processors to the cluster, or you can enter the information from the command line.

1. At the command prompt, use a node definition file in order to define the nodes, console server information, and service processors, by typing:

   ```
   definenode -f nodedef
   ```

2. To review the arguments that you need to enter from the command line, type:

   ```
   definenode -h
   ```

3. To define the node host name, type:

   ```
   definenode -n hostname
   ```

   where *hostname* is the name of the node being defined. The command prompts for missing information when some or all of the arguments are not provided.

See the man page or *IBM Cluster Systems Management for Linux Technical Reference* for details on `definenode` or `addnode` command-line syntax and more examples of the usage of the command.

Defining nodes using GPFS

Use the `mmaddnode` command to add nodes to an existing GPFS nodeset. On each new node, a mount point directory and character mode device is created for each GPFS file system.

Syntax: mmaddnode [-C NodesetId] {-n NodeFile | NodeName[:manager | client][,NodeName[:manager | client]...]}

Parameters:

__ `C NodesetId`

The identifier of the GPFS nodeset you want to add nodes to. If this option is not specified or a period (.) is used for the `NodesetId`, the nodes are added to the `nodeset` from which the `mmaddnode` command was issued. To determine the nodeset of the node you are running on, at the command prompt, type:

```
mmlsnode -C
```

__ `-n NodeFile`

Specifies the file containing the list of node descriptors, one per line, to be added to the nodeset. Node descriptors are of the same format as the `NodeName[:manager | client]` parameter, and follow the same rules.

__ `NodeName[:manager | client][,NodeName[:manager | client]...]`

A comma-separated list of nodes to be added to the nodeset. Nodes are specified by a NodeName and may be optionally followed by a use designation. A designation of manager specifies that the node should be included in the pool of nodes from which the file system manager node is chosen. For further information on the role of a node as the file system manager, see the *General Parallel File System for Linux(R): Concepts, Planning, and Installation Guide* and search for file system manager.

The hostname or IP address must refer to the communications adapter. Alias interfaces are not allowed. Use the original address or a name that is resolved by the host command to that original address. You may specify a node using any of these forms:

```
Short hostname k145n01
Long hostname k145n01.kgn.ibm.com
IP address 9.119.19.102
```

Security

You must have root authority to run the `mmaddnode` command. You may issue the `mmaddnode` command from any node in the GPFS cluster.

When using `rcp` and `rsh` for remote communication, a properly configured *.rhosts* file must exist in the root user's home directory, normally `/root`, on each node in the GPFS cluster. If you have designated the use of a different remote communication program on either the `mmcrcluster` or the `mmchcluster` command, you must ensure:

- Proper authorization is granted to all nodes in the GPFS cluster.
- The nodes in the GPFS cluster can communicate without the use of a password.

Examples

1. To add nodes k145n04 and k145n05, designating k145n04 to be available as a manager node only, and by default add the nodes to the GPFS nodeset on which you are running, type:

   ```
   mmaddnode k145n04:manager,k145n05
   ```

2. To confirm the addition, type: `mmlsnode -C` .
3. To add nodes k145n06 and k145n07 to the GPFS `nodeset set1` , type:

   ```
   mmaddnode -C set1 k145n06,k145n07
   ```

4. To confirm the addition, type: `mmlsnode -C set1`

Rules to follow when adding nodes: You must follow these rules when adding nodes to a GPFS nodeset:

- A node may belong to only one nodeset at a time.
- The nodes being added to the nodeset must belong to a GPFS cluster (issue the `mmlscluster` command to display available nodes).
- The existing nodeset must meet quorum for the nodes to be added. For example, if GPFS is currently configured on eight nodes, all of which are up and running, the quorum value is met and the new nodes join the nodeset.
- Conversely, if GPFS is currently configured on eight nodes and only four are up and running, a quorum of five does not exists and the new nodes may not join the nodeset. When five of the original eight nodes are up and running, the new nodes are added.

- After the nodes have been added and GPFS is started on the new nodes, the quorum value for the nodeset is adjusted accordingly. This allows new nodes to join a running nodeset without causing quorum to be lost.
- Issue the `mmstartup` command to start GPFS on the new nodes.
- When adding nodes to a nodeset using the single-node quorum algorithm, the GPFS daemon must be stopped on all of the nodes. If after adding the nodes, the number of nodes in the nodeset exceeds two, the quorum algorithm is automatically changed to the multi-node quorum algorithm.

Pushing the system image to all nodes in the cluster

Because of the way the Red Hat version 9.0 loads SCSI drivers and assigns them to */dev/sda*, */dev/sdb* partitions, problems can result if more than one SCSI host adapter board (Adaptec or LSI SCSI controller for local drives and Qlogic HBA for Triton connection) is installed on the system. The QLogic HBA will typically be seen first by the installation process. Follow the “Installation procedure” on page 33 and modify the order of the contents of the */etc/modules.conf* file.

Attempting to push the system image out to the nodes while a FAStT controller is still turned on and connected may cause data corruption on the first logical disk device in FAStT subsystem. Make sure the FAStT controllers are turned off or all fibre cables for the FAStT controllers are disconnected from the back of each controller before starting the install process.

To push the system image to all nodes in the cluster, perform the following steps:

1. Open an `rconsole` window for each node being installed so you can monitor the install process:

   ```
   rconsole -n {node list}
   ```

2. Run the `installnode` command for each node being installed:

   ```
   installnode {node list}
   ```

Once the operating system is installed on the storage nodes, reconnect the fibre cable to the FAStT controllers. Reboot the storage nodes to see any configured LANs.

Testing the configuration

1. Boot and log on to the management node as user `root`.
2. Log on to the storage nodes and verify disk configuration:
   `fdisk -l`
3. If present, configure the modem according to the modem instructions.
4. The system is now ready for the customer to connect their network cables.

Chapter 7. Cluster administration

IBM Cluster systems management provides a powerful way to administer the daily operations of a Cluster 1350. This chapter includes administration information about:

- accessing the cluster from a remote location
- accessing each node before the operating system is installed
- shutting down the system components
- lights out or brown out scenario

For more information on such topics as monitoring, remote control, set-up, and technical references, refer to the following URL:
http://www.ibm.com/servers/eserver/clusters/library/linux.html

Remote power

Using the command `rpower` boots and resets hardware, powers hardware on and off, and queries node power state. The syntax is:

```
rpower [-a] [-h] [-n host[,host...]] [-N Node_group[,Node_group...]]
 [-v] on | off | reboot | query | resetsp
```

Remote console

The remote console function is provided using the serial ports of the xSeries 335 servers and terminal servers. This provides remote access to nodes before the operating system is installed or when network access to the servers is unavailable or failed. The terminal servers are required by the installation function in CSM and must be included to enable the remote console function.

Each rack in the configuration includes one or two terminal servers to connect each node in the rack via a DB9 to RH45 serial cable. The terminal servers are LAN connected to the Management VLAN.

The Remote console function is accessed via the `rconsole` command. This command opens a remote console for each node specified with the command. The syntax is:

```
rconsole [-a] [-h] [-n host[,host...]] [-N Node_group[,Node_group...]
```

Shutting down the system components

Because the operating system is installed on each node, the shut down procedures are relatively simple. Complete the following steps to shut down the cluster nodes:

1. Log off the cluster nodes and the storage nodes.
2. To turn the cluster nodes off with Cluster System Management (CSM) installed on the management node, at the command prompt, type:

   ```
   rpower off -A
   ```

   Note: If CSM is not installed on the management node, manually turn off the power switch for each individual cluster node.
3. Turn off the power for the following devices in the order listed:
   a. storage nodes
   b. management node
   c. storage controllers

d. storage expansion units

4. Turn off the power switch for the Power Distribution Units (PDUs) or unplug, from the PDU, the devices that have no power switch.
   - To turn off the PDUs, unplug them from the wall outlet.

   Note: The following devices have no power switch and must be unplugged if the PDUs are not turned off:
   - KVM switch
   - Cisco 10/100 switch
   - Cisco Gigabit switch
   - iTouch terminal server

5. Unplug the PDU power cords from the wall outlet.

Lights out or brown out

In the event of a lights out or brown out scenario, the following sequence occurs:

- The system is up and running typical applications.
- A lights out or brown out event occurs. The system shuts down then restarts via an external source.
- All nodes turn on to the last known state (on/off). If the last known state is on, then the nodes will boot to a console login prompt.
- Log files will show system restart events on nodes and on Remote Supervisor Adapter (RSA) devices. Check the following log files.
  - *`/var/log/messages`*
  - *`/var/log/csm/installnode.log`*
  - RSA event log.
  - BIOS event log

Related topics

- Chapter 5, “Turning on the cluster”, on page 27
- Appendix B, “Error and event logs”, on page 79

Chapter 8. Troubleshooting hardware and software problems

How to use this information

This chapter helps diagnose problems associated with the Cluster 1350. The Cluster 1350 is an integrated Linux cluster that includes IBM and third party hardware and software components like server nodes and associated service processors, storage and networking subsystems, plus Cluster Systems Management (CSM) and General Parallel File System (GPFS) software.

Problem resolution involves identifying the likely problem cluster component and following the relevant problem resolution steps for that component.

This chapter aids in the diagnosis of problems down to the component level. Once a failing component is identified you should see the specific product documentation for further actions. Links to product web sites and online product documentation are provided in this chapter as appropriate.

Diagnosing hardware and software problems in a cluster environment requires a basic understanding of how the components of the Cluster 1350 function together.

The cluster consists of:

- One or more 19″ racks.
- From 4 to 512 cluster nodes. The nodes of the cluster may be an @server 325, an xSeries 335, or BladeCenter containing at least four Blade servers. The nodes are configured to execute customer applications or provide other services required by the customer - such as file server, network gateway, or storage server.
- One management node (xSeries 345 or @server 325) for cluster systems management and administration.
- A management Ethernet VLAN used for secure traffic for hardware control.

  The management Ethernet VLAN is used for management traffic only. It is logically isolated for security using the VLAN capability of the Cisco Ethernet switches, and is only accessible from the management node. The cluster VLAN and management VLANs share the same physical Cisco switches.
- A cluster VLAN used for other management traffic and user traffic. Cisco switches integrated with the cluster are used for the management Ethernet VLAN and the cluster Ethernet VLAN.
- Service processor networks. All nodes in the cluster are connected via serial service processors (xSeries 335) and/or Remote Supervisor Adapter (RSA) cards. The first node in a serial connection must have a RSA which is connected via Ethernet to the management Ethernet VLAN.
- A terminal server network for remote console, using the MRV In-Reach terminal server. Optionally, the customer might elect to include an additional network.
- A high-performance Myrinet 2000 cluster interconnect, or an additional 10/100 Ethernet.
- The customer may elect to configure a subset of cluster nodes with additional external storage. This can also be a Fiber Channel solution (using a FAStT storage subsystem).
- A supported distribution of the Linux operating system.
- Cluster management software such as CSM.

CSM maintains a database of configuration information (tab files) about the nodes that are configured in the Cluster 1350. To display the node configuration information, use the following CSM command on the management server console:

```
Isnode -Al
```

The output provides information about each node, such as, the node type, model number, serial number, and host name. The tab file output also provides information that corresponds each node to its terminal server network and service processor network. For the terminal server network, the output includes the console server host name and the console port number to which the node is connected. For the service processor network, the output includes the host name of the Remote Supervisor Adapter card to which the node is connected and the internal service processor name for the node.

CSM distinguishes between a management node, a pre-managed node, and a managed node. A pre-managed node is a node that has been added to the configuration but is not yet ready to be managed, for example, because it has not yet been installed. To display a list of pre-managed nodes on the management server, at the console prompt type:

```
Isnode -P
```

To display a list of managed nodes on the management server, at the console prompt type:

```
Isnode
```

To display the management server, at any node console prompt type:

```
mgmtsvr
```

Isolating network, node, and Linux problems

Cluster 1350 nodes are connected over a 10/100 Mb Ethernet cluster network. A Cluster 1350 may also have a second network, either an additional Ethernet network or a Myrinet 2000 network.

As a preliminary diagnostic step, ping all the nodes over all available networks.

Compare the error to possible symptoms in Table 12.

Table 12. Troubleshooting the shared VLAN

Symptom	Action
• Can `ping` the storage node from the management node but cannot `ping` the cluster nodes. • Can `ping` the cluster nodes from the management node but cannot `ping` the storage nodes. • Cannot `ping` either the storage nodes or the cluster nodes. • Cannot `ping` the cluster nodes in one of the expansion cabinets.	1. Verify links between the management node, storage nodes, Cisco 3550, 3500, and 400x switches. 2. Reboot the management node and press F1 to enter Setup. Verify that Ethernet devices are turned on. 3. Verify the correct driver level for 1Gb fibre Ethernet. To verify the status, at the console prompt, type: `ifconfig` 4. Check the Cisco (3500, 4003, or 4006) switch for green status lights or system and status LEDs. If the green lights are lit the switch is OK. 5. Verify 1 Gb fibre Ethernet connections are good by swapping a known good cable to isolate the failing device. 6. Replace the failing fibre cable, GBIC, or network interface card.

If following the steps in Table 12 did not correct the problem, continue with the steps shown in “Clustering with one network” on page 43.

Clustering with one network

Ping failure on one or some nodes: If one or more nodes experience a ping failure, this indicates a problem with the node hardware or software. Complete the following steps to resolve the problem:

1. `Telnet` to the node via the serial console or KVM and verify the node is operational.
   a. If telnet succeeds, check the *syslog* for errors.
      1) If there are errors, go to "Isolating software problems" on page 51 and complete the steps in that table to resolve the problem.
      2) If there are no errors, it indicates a network problem. See Table 13 and complete the steps in that table to resolve the problem.
   b. If telnet fails, it indicates a node hardware problem. See "Isolating hardware problems" on page 45 for problem resolution.

Ping failure on all nodes: If all nodes experience a ping failure, it indicates a problem on one of the following:

- Network. Go to Table 13 and complete the listed actions to resolve the problem.
- Network adapter on the management node
- DHCP configuration
- Network configuration
- Cisco blade failure

Table 13. Network troubleshooting for a cluster with one network

Symptom	Action
Cannot `ping` a node or nodes on the cluster network from the management node, yet the `rconsole` command and access from the KVM work correctly.	1. At the console prompt, type the `ifconfig` command to verify that the IP settings are correct. 2. Verify that the cables are fully plugged into the switch and node, and that everything else is plugged into the correct port. Refer to the cabling information printed on each cable label and "VLAN options" on page 14 if you are unsure where a cable belongs. Verify that the link LEDs are lit. 3. Swap ports on the Ethernet switch with a cluster node port that you know is working. 4. Verify the Ethernet switch port is configured for the Management VLAN.

Clustering with two networks

Ping failure on one or more nodes: If one or more nodes experience a `ping` failure, it indicates a problem with the node hardware or software. Complete the following steps to resolve the problem:

- `Telnet` to the suspect node via the serial console or KVM and verify the node is operational. If `telnet` succeeds, check the *syslog* for errors.
  1. If there are errors, go to "Isolating software problems" on page 51 and complete the listed actions to resolve the problem.
  2. If there are no errors, it indicates a network problem. Go to Table 15 on page 44 and complete the listed actions to resolve the problem.
- If `telnet` fails, this indicates a node hardware problem. Go to "Isolating hardware problems" on page 45 and complete the listed actions to resolve the problem.

Ping failure on only one network: If `ping` failures occur on one network but not on the other network, this indicates a problem on the network adapter on the management node for the failing network.

Ping failure on one or both networks:

1. Verify that all communication devices on the network are turned on and that each device has a green status LED lit on both ends of the connection.
2. Verify with support the correct IP Address, Net Mask, and Gateway settings for each device that fails to function in the network.
3. To determine the IP Address scheme of each node, at the console prompt, type, `ifconfig` and compare this output to the factory defaults shown in Table 14.

Table 14. Factory defaults

Device	IP address	Host name
Management node	172.20.0.1 172.30.0.1	eth0–mgtnode.cluster.net eth1–mgtnode-eth1
Storage node	172.20.1.1	storage001
First FAStT storage	172.20.2.1	
Second FAStT storage	172.20.2.2	
xSeries 335 cluster nodes	172.20.3.1	node001...node*xxx*
BladeCenter Ethernet switch module	172.20.90.1	
Myrinet switch	172.20.10.1	myri001
First iTouch port server	172.30.20.1	ts001
Second iTouch port server	172.30.20.2	ts002
RSA cards (bottom card)	172.30.30.1	rsa001
RSA cards (next card)	172.30.30.2	rsa002
RSA cards (Myrinet switch)	172.30.30.3	
Cisco 4003 switch (console management)	172.30.80.1	cisco4003–001
Cisco 10/100 switch	172.30.40.1	cisco3550–001
Cisco Gb switch	172.30.50.1	cisco3508–001
APC Master switch	172.20.60.1	apc001
Remote Console Manager	172.30.70.1	rcm001

Ping failure on all nodes on both networks: If all nodes on both networks experience a ping failure, it indicates a problem with the system software or a user application. Telnet to the node via the serial console:

1. If `telnet` succeeds, check the *syslog* for errors.
   a. If there are errors, go to “Isolating software problems” on page 51 for software problem resolution.
   b. If there are no errors, it indicates a user application problem.
2. If `telnet` fails, connect to the node using a serial communications program like Hyperterminal. If you still cannot connect it indicates a node hardware problem. Go to “Isolating hardware problems” on page 45 for problem resolution.

Table 15. Network troubleshooting for a cluster with two networks

Symptom	Action

Table 15. Network troubleshooting for a cluster with two networks (continued)

Cannot `ping` a node or nodes on the cluster network from the management node, yet the `rconsole` command and access from the KVM work correctly.	1. Use the `ifconfig` command to verify that the IP settings are correct. 2. Verify that the cables are fully plugged into the switch and node, and that everything is plugged into the correct port. Refer to the cabling information printed on each cable label and“VLAN options” on page 14if you are unsure where a cable belongs. Verify that the link LEDs are lit. 3. Swap ports on the Ethernet switch with a cluster node port you know is working. 4. Verify the Ethernet switch port is configured for the management VLAN.

Isolating hardware problems

Node checks

Table 16. Troubleshooting the remote console network

Symptom	Action

Table 16. Troubleshooting the remote console network (continued)

1. Cannot execute a `rconsole` command to any cluster node. 2. Cannot execute any `rconsole` commands to get an active terminal session.	1. Verify the Ethernet connections between the terminal server and the Cisco switch are OK. Also check the connections between the Cisco switch and the management node. 2. Check the cables, dongles, and connectors at the node and the terminal server. Verify that the serial port at the node is attached to the correct port on the terminal server by using the CSM command `lsnode -aI <NodeName>`. Refer to the `ConsolePortNum` information later in this section. 3. Follow steps 1 through 9 of Chapter 11, "Port server configuration after device replacement", on page 63, then at the `IN-Reach_Priv>` prompt type, `show port <portnumber>` to verify the settings of all suspect ports against ports that are working correctly. 4. Verify the iTouch terminal server is turned on and connected to the network by pinging the unit at 172.30.20.1 5. To make sure the serial port (COM 1) is configured to redirect output to the terminal server, complete the following steps: a. Restart the node and review the console screen. b. When the message, `Press F1 for Configuration/Setup` opens, press **F1**. c. From the main menu, select **Devices and I/O Ports** then press **Enter**. d. Verify that Serial Port A is set to **Port 3F8, IRQ 4**. e. Select **Serial Port A**. f. Select **Remote Console Redirection**. g. Verify the following settings: Remote Console Active [Enabled] Remote Console Com Port [COM1] Remote Console Baud Rate [9600] Remote Console Data Bits [8] Remote Console Parity [None] Remote Console Stop Bits [1] Remote Console Emulation [VT100] Remote Console Active After Boot [Enabled] h. Save the settings and exit. 6. For the xSeries 335 and xSeries 345 only, run diagnostics against the serial port to validate network connectivity. 7. Swap out the cables and dongle with new cables and dongle.

If the procedures in Table 16 on page 45 do not correct the issue you may have a problem with a port on the terminal server. Complete the following steps to test a different port:

1. Issue the CSM command `lsnode –AI <nodename> lgrep` and record the port information.
2. Move the cable to a new port and change the port number using the CSM command `chnode <nodename> ConsolePortNum=`*xx* where *xx* is the new port number.

If the symptom persists, go to “Checking service processor logs” on page 53 and check the service processor log.

Hardware problem in service processor log: Go to “Node checks” on page 45 for node problem resolution.

Amber LED lit on node: Service processor log may be full. The log is cleared by connecting to the service processor via the Remote Supervisor Adapter card. Otherwise, go to “Node checks” on page 45 for node problem resolution.

`rpower` ***to node fails:***

- Check the service processor connection.
- At the console prompt, type `rpower -a on`.
- Go to “Checking service processor logs” on page 53 and check the service processor log.
- Use the Web interface or `telnet` to each Remote Supervisor Adapter card on the cluster and then connect to the service processor on each cluster node individually through the Remote ASM Access menu.
- If the cluster node is not in listed, insert the node firmware diskette and try to diagnose the problem.

Service processor network

Table 17. Troubleshooting the service processor network

Symptom	Action

Table 17. Troubleshooting the service processor network (continued)

1. The `rpower –a query` command does not return with the status of all nodes 2. Cannot see all the nodes when managing remote Advanced System Management (ASM) service processors. 3. Cannot connect to individual Remote Supervisor Adapter (RSA) cards using browser.	1. Check the physical connections on the RS485 network and check for errors. 2. From the management node, use the Web browser and try to connect to the failing node through that node's RSA card. 3. Check that the RSA network is properly terminated. When more than one node is connected, terminators should be plugged into the empty port on the dongle and in the second RS485 port of the last node in the chain. 4. Swap the internodal CAT5 cable on the unresponsive node with a known good cable. Also, replace the dongle if a problem is suspected. 5. Swap the KVM/RS485 cable (on the xSeries 335 only) with a known good cable. Also, replace the dongle if a problem is suspected. 6. Verify the RSA configurations and IP settings with support. 7. Verify the 10/100 Ethernet link between the RSA card and the Cisco 3550 or 400x switch. 8. Flash the ASM service processors to the latest firmware level. 9. Flash the RSA to the latest firmware level. 10. Check RSA configurations using the firmware update diskette.

If following the steps in Table 17 on page 47 did not correct the problem, continue with the steps shown in "Remote Supervisor Adapter card connection failure".

Remote Supervisor Adapter card connection failure:

1. To verify the node has power, type: `rpower query`.
   a. If the node has power, `ping` the Remote Supervisor Adapter (RSA) card using the `HWControlPoint` field in the `lsnode` output.
      1) If `ping` succeeds, reset the RSA card. If the adapter connection continues to fail after it has been reset contact IBM support.
      2) If the `ping` fails, check the network connection.
   b. If the node does not have power, check the power connections.
2. If the network connection LED is lit for the RSA card at the Ethernet switch, go to "Resetting the Remote Supervisor Adapter card" on page 53 and reset the RSA adapter.

Node connection or command failure: If the Remote Supervisor Adapter (RSA) card connection is working, but the node connection or commands issued to the node failed:

- Connect to the RSA card and verify node list.
- Verify all cabling.
- Go to "Node checks" on page 45 and perform node checks.

Checking storage

Table 18. Troubleshooting the Fibre Storage network

Symptom	Action

Table 18. Troubleshooting the Fibre Storage network (continued)

Cannot see disk drives from the storage node.	1. Reboot the storage node and press the **Alt/Q** keys to go into Qlogic setup. Verify that the 700 FastT is a listed device. 2. Check the Fibre connections between the server HBA and the hubs on the 700 FastT. The green connection LED should be lit. 3. Check cabling on the 1742 FastT outbound hubs to the storage expansion units. Look for link lights and proper cabling. Also verify that all transfer rate speed switches are set to 2 Gigabytes. 4. Check the Blade Server and Enhanced System Manager (ESM) firmware levels and update to current levels.

If following the steps in Table 18 on page 48 did not correct the problem, continue with the steps shown in “File system failure”.

File system failure:

Check disks using `fdisk -l`:
- If `fdisk -l` completes without error, go to “GPFS checks” on page 52 and continue with the file system problem resolution.
- If `fdisk -l` reports missing disks, check that the adapter device driver is configured:
  - If the adapter device driver is configured, go to “Checking storage” on page 48 and continue with storage subsystem problem resolution.
  - If the adapter device driver is not configured, check the adapter hardware and then refer to the applicable documentation that came with your software and complete the problem resolution process.

PFA alert indicates internal disk: Go to “Checking storage” on page 48 and perform disk problem resolution.

I/O errors in syslog: Execute problem resolution for the indicated disk, adapter, or storage subsystem.

Ping failure over the Ethernet

Check the nodes using the `rconsole` command or `ping` nodes using the Myrinet switch:
- If the node responds, refer to the applicable documentation that came with the switch and complete the problem resolution process.
- If the node does not respond, go to “Node checks” on page 45 and continue with Node checks.

Ping failure over a Myrinet switch

Check the nodes using the `rconsole` command or `ping` nodes via the Ethernet:
- If node responds, go to “Configuring SNMP alerts from Myrinet” on page 53 and continue with Myrinet problem resolution.
- If the node does not respond, go to “Node checks” on page 45 and continue with Node checks.

Checking the terminal server

Check the terminal server nodes using the `telnet` command or `ping` the nodes via the Ethernet:

- If node communication fails, go to “Node checks” on page 45 and continue with Node checks.
- If following the steps in Table 19 do not correct the problem, continue with the steps shown in “Isolating network, node, and Linux problems” on page 42..

Table 19. Troubleshooting the terminal server network for the Remote Console

Symptom	Action
Unable to execute `rconsole` commands to get an active terminal session.	1. Check connection of cables and connectors at the nodes and the iTouch terminal server. 2. Verify that the iTouch terminal server is turned on and connected to the network by pinging the unit at 172.30.20.1. 3. Follow steps 1 through 9 of Chapter 11, “Port server configuration after device replacement”, on page 63, then at the `*IN-Reach_Priv>*` prompt, type, *`show port <portnumber>`* to verify the settings of all suspect ports against ports that are working correctly. 4. Verify the iTouch terminal server is powered up and functional by pinging the unit at 172.30.20.1 5. Verify that the serial port (COM 1) is configured to redirect the output to the terminal server: • Restart the node and watch the monitor screen. • When indicated, press **F1**. • From the main menu, select **Devices and I/O Ports**, then press **Enter**. • Verify that Serial Port A is set to **Port 3F8, IRQ 4**. • Select **Serial Port A**. • Select **Remote Console Redirection**. • Verify the following settings: Remote Console Active [Enabled] Remote Console Com Port [COM1] Remote Console Baud Rate [9600] Remote Console Data Bits [8] Remote Console Parity [None] Remote Console Stop Bits [1] Remote Console Emulation [VT100] Remote Console Active After Boot [Enabled] • Save settings and exit. 6. Swap out cables and dongle with known good units. 7. Run diagnostics against the serial port to verify connectivity.

Troubleshooting the KVM network

Table 20. Troubleshooting the KVM network

Symptom	Action

Table 20. Troubleshooting the KVM network (continued)

The Keyboard/Video/Mouse (KVM) switch selector shows some or all systems are non-active (indicated by a red X) but the system is turned on.	1. Check that the connections for the KVM harness on the back of the system are securely plugged in. 2. Check the connection of the inbound/outbound CAT5 connections on the KVM switch conversion dongle. 3. Check that the link LED on the dongle is lit. If the LED is lit, a good connection exists with the node keyboard port. If no link LED is lit and you are having problems with KVM connectivity, replace the dongle (FRU 32P1654). 4. Verify that the terminator is in place at the first dongle on the KVM chain. 5. Use a known good CAT5 (straight through) cable to direct connect or bypass possible bad cables. 6. Reboot the failing node to reset connection to the KVM switch.

File system failure

To check the disks, at the command prompt, type: `fdisk -l`

- If `fdisk -l` completes, go to "GPFS checks" on page 52 and continue with the file system problem resolution.
- If `fdisk -l` reports missing disks, check that the adapter device driver is configured:
  - If the adapter device driver is configured, go to "Checking storage" on page 48 and continue with storage subsystem problem resolution.
  - If the adapter device driver is not configured, check the adapter hardware and then go to the applicable Linux documentation that came with your software and resolve the configuration issue.

PFA alert indicates internal disk

Go to "Checking storage" on page 48 and perform disk problem resolution.

I/O errors in syslog

Execute problem resolution for the indicated disk, adapter or storage subsystem.

Isolating software problems

Operating system checks

Node non-responsive: If the node does not respond to `ping` or the serial console, and there are no relevant entries in the `syslog` or hardware logs, refer to the applicable Linux documentation that came with your software to continue with the problem resolution process.

Adapter device driver not configured: If the device driver is not configured, and there are no adapter hardware problems reported, refer to the applicable Linux documentation that came with your software and continue with the problem resolution process.

CSM checks

Events not logged or actions not taken: Using the ERRM command line interface, monitor the `AnyNodeProcessorsIdleTime` condition on specific managed nodes with the `LogEventsAnyTime` response while causing arm and rearm events. If arm and rearm events are not observed at the management server, this is

configuration or network problem. Refer to the applicable documentation that came with CSM and complete the problem resolution process.

Differences in node lists: Output from the command `CT_CONTACT=<ManagedNodeName> lsrsrc IBM.[Host|FileSystem]` when run on the management node is not the same as when run on the managed node. This is configuration or network problem, refer to the applicable documentation that came with CSM and complete the problem resolution process.

netstat output incomplete: The command `netstat -an | grep rmc` on the management server does not show *ESTABLISHED TCP* connections for each managed node that is currently turned on. This is configuration or network problem, refer to the applicable documentation that came with CSM and complete the problem resolution process.

RMC not running: The command `lssrc -ls ctrmc` shows that RMC is not running on the management server. Refer to the applicable documentation that came with CSM and complete the problem resolution process.

lsrsrc reports errors: The command `lsrsrc -ab IBM.[Host|FileSystem]'` which checks that HostRM and FSRM will run on the management server reports errors. Refer to the applicable documentation that came with CSM and complete the problem resolution process.

lsaudrec reports errors: The command `lsaudrec` which checks that AuditRM will run on the management server reports errors. Refer to the applicable documentation that came with CSM and complete the problem resolution process.

Predefined conditions not shown: The `lscondition` and `lsresponse` commands when run on the management server do not show pre-defined conditions and responses. Refer to the applicable documentation that came with CSM and complete the problem resolution process.

Commands or file replication fails: CSM commands fail or CFM file replication fails. Refer to the applicable documentation that came with CSM and complete the problem resolution process.

rpower or rconsole commands fail: CSM `rpower` and `rconsole` commands fail. Refer to the applicable documentation that came with CSM and complete the problem resolution process.

GPFS checks

Performance problems: Refer to GPFS problem resolution and GPFS Performance White papers included with your software.

GPFS file system failure: Refer to GPFS problem resolution and GPFS Performance White papers included with your software.

SNMP monitoring

The service processor network, Ethernet switches, and Myrinet switch can be monitored using SNMP. All devices should be configured to send their SNMP traps to the management server. The management server should be configured to use `trapd` so that SNMP traps can be translated to a human readable form and added to the `syslog`.

Use the `lsnode -Al` command to determine the host name for the Remote Supervisor Adapter card and the service processor name associated with the failing node. Use the `telnet` command or a Web browser to connect to the Remote Supervisor Adapter using the adapters host name, and select options to configure SNMP.

Configuring SNMP alerts from Myrinet

The Myrinet 2000 network in the Cluster 1350 is installed with adapter cards. One can use a graphical user interface, Mute, to monitor the entire network for events, which are logged and reported by the monitoring cards. You can configure an SNMP client or use a Web browser to access the monitoring card information. You can configure the monitoring cards to notify you of events by email.

The following Myrinet software packages are required:

- GM software is the base software required to use Myrinet 2000 network. It is the message-passing system for Myrinet networks, and includes a driver, Myrinet interface control program, a network mapping program, the GM API, library, and header files.
- m3-dist package, which provides the source for building the SNMP library for the GM layer.
- Mute (GUI) tool, which monitors the Myrinet network.

Use the following order to build the software:

- GM including the mt tools
- m3-dist (has dependency on GM)
- Mute (has dependency on GM and m3-dist)

Comprehensive details on how to build the software is described in the:

- Linux README file
- GM mt/README file
- m3-dist README file
- mute software README file

Currently m3-dist and Mute compile against GM version 1.5. With GM version 1.4 the SNMP library does not build m3-dist or Mute. Build the software using GM version 1.5.

You can access Myrinet software from: http://www.myri.com/scs/index.html (for GM, select the *LANai9* software).

Resetting the Remote Supervisor Adapter card

The Remote Supervisor Adapter (RSA) card is typically connected to a remote power control strip. To reset the RSA, plug the remote power control strip of the failing RSA card into another power source and issue the `power off` and `power on` commands to the RSA port.

Checking service processor logs

At the console prompt, type, `lsnode -Al` to determine the host name for the Remote Supervisor Adapter (RSA) card and the service processor name associated with the node. At the console prompt,`telnet` or open a Web browser to connect to the RSA card using the host name, and select **View Log**.

Management, cluster, and storage node problems

The IBM components used for management, cluster, and storage nodes are shown in Table 21:

Table 21. IBM components used for management, cluster, and storage nodes

Node type	IBM component used
Management node	• xSeries 345 • @server 325 (64-bit operating system environment)
Cluster node	• @server 325 • xSeries 335 • xSeries 345 • BladeCenter
Storage node	• @server 325 • xSeries 335 (do not use in a Fibre Channel storage configuration) • xSeries 345 • xSeries 360

While the @server 325, xSeries 335, BladeCenter, xSeries 345, and xSeries 360 are all high-reliability units, occasionally a component may fail. Two areas that might cause problems are:

1. Disk drives
2. System board

The following section includes information about:

- Disk drive failures
- System board failures
- xSeries 335 problems
- BladeCenter problems
- Power problems

Disk drive failures

The following section discusses issues with disk drive failures.

Disk drive failure on the management node

The xSeries 345 supports hot swapping of hard disks. To replace a failing hard disk on the management node:

1. Remove the failing hard disk by sliding it out through the front panel opening.
2. Slide the replacement disk drive into the open slot. The drive will rebuild automatically on a mirrored system. If the system is not mirrored a complete re-install of the management node is required. See Chapter 6, “Installing the software”, on page 31 for detailed instructions.

Disk drive failure on a cluster node

The xSeries 335 supports hot swapping of hard disks, but BladeCenter does not. To replace a failing hard disk on an xSeries 335:

1. Remove the failing hard disk by sliding it out through the front panel opening.
2. Slide the replacement disk drive into the open slot.

3. At the management node, issue the following command:

   `installnode x`

   where *x* is the number of the node being rebuilt. If needed, have the customer contact support to assist with the correct naming conventions and IP addresses.

If a hard drive fails on a Blade server in the BladeCenter, first power down the Blade server. Next, remove the Blade server from the BladeCenter and replace the hard drive as outlined in *IBM eServer BladeCenter Hardware Maintenance Manual and Troubleshooting Guide*. Once the drive is replaced and the Blade server is returned to the BladeCenter issue the following command at the management node:

`installnode x`

where *x* is the number of the node being rebuilt. If needed, have the customer contact support to assist with the correct naming conventions and IP addresses.

Disk drive failure on a storage node

The xSeries 345 and xSeries 360 support hot swapping of hard disks. To replace a failing hard disk on the storage node:

1. Remove the failing hard disk by sliding it out through the front panel opening.
2. Slide the replacement disk drive into the open slot. The drive will rebuild automatically on a mirrored system. To rebuild the storage node, if the system is not mirrored, enter the following command at the management node command line prompt:

   `installstorage 1`

System board failures

1. Replace the system board.
2. Flash the system BIOS to the level used in the installation. Refer to “Software version matrix” on page 31 for a listing of the software and firmware levels used in the Cluster 1350.
3. Flash the Diagnostics to match the BIOS level. Refer to “Software version matrix” on page 31 for a listing of the software and firmware levels used in the Cluster 1350.
4. Flash the onboard ASM to the current level. Refer to “Software version matrix” on page 31 for a listing of the software and firmware levels used in the Cluster 1350.
5. Perform the following configuration settings:
   - Devices and I/O Ports: `PORT 3F8, IRQ4`
   - Remote Console Redirection: Enabled, COM1, 9600, 8, None, 1, VT100, Enabled
   - Boot sequence: Diskette Drive, CD ROM, Network, Hard Drive 0, Boot Fail Count: DISABLED
   - Set the remote control password if a Remote Supervisor Adapter card is installed in this node (xSeries 335, xSeries 345, xSeries 360 only).
   - If you are replacing an HS20 BladeCenter with a serial port option, make sure that switch 7 in the switchblock is turned **on**.
   - Update the cluster software with the new MAC address associated with the new system board or Blade card you installed.
     - To get the MAC address of eth0 for the new component, use the CSM command: `ifconfig`
     - To update the cluster software, use the CSM command: `chnode <nodename> InstallAdaptorMacaddr=<new MAC (xx:xx:xx:xx:xx:xx)>,Any System`.

Contact support for any setup or IP configurations that need to be performed.

6. Turn the customer over to support for any additional tasks needed to restore the node to full functionality.

xSeries 335 problems

In a xSeries 335 with an Remote Supervisor Adapter (RSA) over C2T connection make sure that the cluster node at the beginning of the C2T chain has an RSA card, external dongle, and connection to the onboard RSA processor.

BladeCenter problems

When the serial port option is used on a blade server in the BladeCenter it is important to make sure that switch number 7 in the switchblock is set to the **on** position, that the card is fully seated in the option card slot, and that the cable is plugged into the serial header port. An improper switchblock setting, loose option card, or unplugged cable will cause the blade server to become unresponsive to `rconsole` commands.

When two processors are installed, take special care not to pinch the cable under the metal standoff on the inside of the cover.

If the Ethernet Switch Module (ESM) is replaced in the BladeCenter then you must reassign the IP address for the external ports to work. Make sure the address is in the range reserved for the cluster LAN (.20 address) and not the management LAN.

Make sure that the PDUs in the cluster are connected to 220V source power. BladeCenters connected to PDUs plugged into 115V power will not function properly.

Power problems

The following section includes information about:

- No power to multiple devices
- No power to an individual device

No power to multiple devices

1. Check that the 30 amp twist lock plugs are locked into the customer supplied receptacles.
2. Check the main power breakers at the customer breaker panel and make sure they are on.
3. Measure the voltage on the power out side of the Frame Power Block. If no voltage is present have the customer's electrician check for power issues. If no problems are found with the customer's power then replace the Input Power Block (FRU 32P1077). If the correct voltage is present, continue with the next step.
4. Verify the Power Distribution Unit (PDU) breakers are in the ON position.
5. Verify the PDU plugs are securely seated into the Power Out sockets on the Frame Power Blocks.
6. Verify voltage at the Power Out ports on the PDU using a Multimeter. If no power is present replace the PDU (FRU 9N9671). Otherwise, continue with the next step.
7. Swap out the power cable on the failing unit. If power LEDs do not light up on the failing unit, replace the power supply, or replace the complete unit if the power supply cannot be replaced.

No power to an individual device

1. Verify the PDU plugs are securely seated into the Power Out sockets on the Frame Power Blocks.
2. Verify voltage at the Power Out ports on the PDU using a Multimeter. If no power is present replace the PDU (FRU 9N9671). Otherwise, continue with the next step.
3. Swap out the power cable on the failing unit. If power LEDs do not appear on the failing unit, replace the power supply or complete unit if the power supply cannot be replaced.

Related publications

Additional hardware maintenance and problem resolution information relating to the xSeries 335 and xSeries 345 was included with the documentation shipped with the Cluster 1350.

Your cluster might have features that are not described in the documentation that you received with the cluster. The documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in your cluster documentation. These updates are available from the IBM Web site. Complete the following steps to check for updated documentation and technical updates:

1. Go to **http://www.ibm.com/pc/support/**.
2. In the **Learn** section, click **Online publications**.
3. On the ″Online publications″ page, in the **Brand** field, select **Servers**.
4. In the **Family** field, select **xSeries ***xxx*****.
5. Click **Continue** and select the online documents that best fit your needs.

Chapter 9. KVM Switch configuration

There are two possible KVM switch options for the Cluster 1350:

- IBM NetBAY 2x8 console switch
- IBM NetBAY Advanced Connectivity Technology Remote Console Manager (RCM)

Configure and setup the console switch after device replacement

1. Connect a laptop computer running a terminal emulation program (such as HyperTerminal) to the configuration port on the back panel of the console switch using a RS232 DB9 null modem cable.
2. Configure the terminal settings to:
   - **9600 baud**
   - **8 bits**
   - **1 stop bit**
   - **no parity**
   - **no flow control**
3. Plug the supplied power cord into the back of the console switch and then into the Power Distribution Unit (PDU) supplying power to the cabinet.
4. Turn on the power to the console switch. The power indicator on the front of the unit will blink for 30 seconds while the console switch performs a self-test. Approximately 10 seconds after it stops blinking, press the **Enter** key to access the main menu.
5. At the Terminal Applications menu, select **option 1** *Network Configuration*.
6. Select option 1 and set your network speed. Whenever possible, set your connection speed manually without relying on the auto-negotiation feature. Once you have entered your selection you will be returned to the *Network Configuration* menu.
7. Select option 2 and specify if you are using a static or BootP IP address. Use a static IP address for ease of configuration. If you are using a BootP address, configure your BootP server to provide an IP address to the console switch and skip the next four steps.
8. From the Terminal Applications menu, select option 3 and specify the IP address for the console switch.
9. From the Terminal Applications menu, select option 4 and specify the Netmask for the console switch.
10. At the Terminal Applications menu select option 5 and specify the Default Gateway address for the console switch.
11. Enter 0 to return to the main menu. You must now update the FLASH level on the console switch.

Upgrading the console switch FLASH level

To perform this update you will need a TFTP server. If you don't already have a TFTP server, there are several you can download from the Internet. You will need to download the latest FLASH firmware from Avocent at http://www.avocent.com/support or copy the FLASH upgrade file (.fl file extension) from the CD shipped with the console switch. Save the FLASH upgrade file to the appropriate directory on the TFTP server. Once this is complete, the following steps will upload the new FLASH file onto the console switch:

1. If you haven't already done so, connect a laptop computer running a terminal emulation program (such as HyperTerminal) to the configuration port on the back panel of the console switch using a RS232 DB9 null modem cable.

2. Set the console terminal to:
   - **9600 baud**
   - **8 bits**
   - **1 stop bit**
   - **no parity**
   - **no flow control**
3. Connect the LAN port in the console switch to an Ethernet hub that is also connected to the PC being used as the TFTP server. Launch both the server software and the terminal emulation software.
4. Verify that the console switch is turned on. After approximately 40 seconds, the console switch will send out a message reading: `Avocent AutoView 1000R/2000R Ready_Press any key to continue.` Press any key to access the AutoView 1000R/2000R main menu.
5. Get the IP address of the TFTP server. If you are using the SolarWinds TFTP server, the IP address is shown in the lower right-hand corner of the server pane. Otherwise, you must extract the IP address using the OS tools.
6. Right-click on **Network Neighborhood**, and select the **Properties**.
7. Click the **Protocols** tab, and select **TCP/IP protocol**.
8. Select **Properties**, and make note of the IP address.
9. If needed, assign the IP address for the console switch:
   a. To select the Network Configuration, in the terminal emulation window, type `1`.
   b. Compare the IP address shown for the console switch to the IP address of the TFTP server. The first three numbers of both IP addresses must be the same, but the last number must be different. If the console switch IP address is incorrect, type `3` to select the IP address, and then enter the correct address.
   c. To exit the Network Configuration menu, type `0` and follow the prompts to upgrade the FLASH level on the console switch.

Replacement of NetBAY Advanced Connectivity Technology RCM

Detailed removal, replacement, and configuration information for the RCM is addressed in the applicable service manual that you received with your unit.

Chapter 10. KVM control

The KVM Switch allows the use of a single keyboard, mouse, and monitor for multiple servers. You can switch between nodes and a console through the KVM Switch interface, known as OSCAR.

The Switch provides on-screen configuration and activity reporting, programmable scanning, NVRAM for saving configuration parameters, and an external reset switch.

Saving the KVM Switch settings

Device settings need to be saved in the KVM Switch's nonvolatile memory (NVRAM) when any of the following occurs:

- The KVM Switch is initially powered up.
- Nodes are added to or removed from the cabinet.
- There is a change in the keyboard, mouse, or monitor.

Attention: If device settings are not saved and the power to the KVM Switch is lost, it may be necessary to reboot each node in the system to re-establish keyboard and mouse communications.

To save the device settings in the KVM Switch NVRAM, perform the following steps:

1. On the keyboard, press **Print Screen**. The OSCAR selection window opens.
2. Press **F2**. The Advanced menu window opens. The Commands menu is highlighted.
3. Use the arrow keys (↑ and ↓) to highlight **Snapshot**, and press **Enter**. The device settings are now saved to NVRAM.

Connecting components with the KVM Switch power turned on

You can connect additional servers to the KVM Switch while the system is running. When you power up the newly connected node, the KVM Switch recognizes it, and you can switch to the new node without taking any additional steps.

You can also connect the mouse, keyboard, and/or monitor to the KVM Switch while the system is powered up. When you connect a new device, the KVM Switch recognizes it and configures it to the settings of the currently selected node. This allows replacement of failed devices without having to restart the system.

Switching between nodes and the console

The KVM Switch lets you disconnect the keyboard, mouse, and monitor from the currently selected node or from the console. You can also connect the keyboard, mouse, and monitor to another node or to the console.

Perform the following to switch between nodes or the console:

1. Press **Print Screen**. The OSCAR selection window opens.

   Attention: The servers and the console are listed in order by port or by name, depending on the user-definable settings in OSCAR menu attributes.
2. To select a node or the console, perform one of the following:
   a. Use the arrow keys (↑ and ↓) to select the node or the console; then press **Enter**.

b. Press the numeric key that corresponds to the node port number or the console port number, then press **Enter**.
c. Double-click the node or the console that you want to select.

3. Press the **Esc** key to exit OSCAR and close the OSCAR selection. The status flag window opens to indicate the currently connected node or the console.

Security features

The KVM Switch provides for system security through the OSCAR interface. This security provides a simple keyboard and screen lock.

Open the security screen by selecting, **Advanced Menus>Setup>Security**. You must always provide a password to access the fields on the screen. The default password is **oscar**.

You can change passwords, set wait-time for locking to take effect, and set low-power mode for monitors so configured.

Resetting the mouse and keyboard

If the mouse and keyboard are not working properly (for example, no cursor response), you may need to reset the mouse and keyboard to restore the correct settings for the selected node. Perform the following steps to reset the mouse and keyboard:

1. Press the **Print Screen** key. The OSCAR selection window opens.
2. Press **F2**. The Advanced menu window opens. The Commands menu is selected.
3. Use the arrow keys (↑ and ↓) to select **Reset**, and press **Enter**. The mouse and keyboard are now reset.

If the mouse or keyboard are still locked up, you can push the reset button on the back panel to reset the KVM Switch. Pressing the reset button might allow you to recover the device settings without unplugging and replugging the power cable for the node.

Chapter 11. Port server configuration after device replacement

If you can successfully `ping` the iTouch port server, no further action is needed. The port server has been properly configured. If you cannot `ping` the port server, then complete the following steps to configure the device:

1. Connect a laptop computer running a terminal emulation program (such as HyperTerminal) to the command port on the back panel of the port server using a DB9 to RJ45 Serial cable.
2. Set the terminal configuration to the following settings:
   - **9600 baud**
   - **8 bits**
   - **1 stop bit**
   - **no parity**
   - **no flow control**
3. Attach a serial terminal to the command port. The default command port is the last port, either port 20 or port 40 depending on the size of the port server.
4. Turn on the port server and press **Enter** repeatedly until you see the `*Login>*` command prompt, and type `access`. No readable characters are visible.
5. Press **Enter**.
6. At the `*Username>*` command prompt, type `system` and press **Enter**. The iTouch directory prompt displays.
7. At the *iTouch>* command prompt, type `set priv` and press **Enter**.
8. At the `*Password>*` command prompt, type `system .`
9. At the `*iTouch>*` command prompt, type `show ip` to see the current network settings.
10. To set the IP address, type `define ip address xxx.xxx.xxx.xxx`.
11. To set the gateway address, type `define ip primary gateway address xxx.xxx.xxx.xxx`.
12. To set the subnet mask, type `define ip subnet mask xxx.xxx.xxx.xxx`.
13. To save the configuration and restart the port server, type `init delay 0`.

If the port server does not already have an IP address, it might need further configuration so the serial ports can operate properly. Complete the following steps:

1. Telnet to the IP address assigned to the port server.
2. At the `*Login>*` command prompt, type `access`.
3. At the `*Username>*` command prompt, type `system`.
4. At the `*iTouch>*` command prompt, type `set priv`.
5. At the `*Password>*` command prompt, type `system .`
6. At the `*iTouch_Priv>*` command prompt, define the ports by entering the following:

```
iTouch_Priv>define port 1-20 access remote
iTouch_Priv>define port 21-40 access remote
iTouch_Priv>define port 1-20 flow control enable
iTouch_Priv>define port 21-40 flow control enable
iTouch_Priv>define port 1-20 speed 9600
iTouch_Priv>define port 21-40 speed 9600
iTouch_Priv>define port 1-20 que disable
iTouch_Priv>define port 21-40 que disable
iTouchh_Priv>lo port 1-20
iTouch_Priv>lo port 21-40
iTouch_Priv>init delay 0
```

Note: Do not try to define ports 21–40 on a port server with only 20 ports. The last command will cause the port server to save any configuration changes and restart. The port server should now be fully operational.

Chapter 12. Cisco 10/100 Switch replacement and configuration

To replace the Cisco 24-port 10/100 switch, see the instructions that came with your switch.

Configuration and setup after device replacement

To replace the Cisco 24-port 10/100 switch, see the instructions that came with your switch.

To set up the new 10/100 Switch you will need the following:
- Laptop computer
- Hyper Terminal program
- DB9 to RJ45 serial cable

Take the following steps:

1. Connect the RJ45 side of the serial cable to the port on the front of the Cisco switch marked ″CONSOLE.″
2. Connect the other end of the cable to the laptop computer.
3. Start the Hyper Terminal application. Configure the terminal to:
   - 9600
   - 8
   - N
   - 1
   - No Flow Control
   - VT100 Emulation
4. At the command prompt in the terminal emulation window, type: `enable`. This will put you in administrative mode.
5. At the command prompt, type `ibm` and press **Enter**. The prompt will change from a **>** to a **#** to indicate you are in administrative mode.
6. At the command prompt, type `show run` to show the current configuration information. Make note of the current settings.

   You need the following information to set up the new switch:
   - Switch IP address
   - IP mask
   - Default gateway IP address
   - Switch host name
   - Cluster name
7. At the **#** prompt, type `configure terminal`.
8. Type, `interface vlan1`.
9. Type, `ip address 172.xxx.xxx.xxx 255.255.xxx.xxx`.
10. Type, `exit`.
11. Type, `ip default-gagteway 172.xxx.xxx.xxx`.
12. Type, `end`.
13. Type, `show run-config` to verify the IP settings.
14. Type, `copy running-config startup-config`.
15. Logoff from the session.

The setup procedures are documented in the Cisco Quick Start Guide Catalyst 3500 Series XL Switches:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/3500.htm

After completing the First Time Setup section in the Cisco Quick Start guide, save it to the *startup* file so the switch can be rebooted without losing the setup configuration. At the `telnet` prompt, enter the command:`copy run start`

The Quick Start guide also describes how to obtain the JAVA plug-in and configure your browser to support the HTML interface.

Attention: There is an SNMP vulnerability for various versions of switch firmware.

Refer to http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml for specific firmware patches to download.

Setup troubleshooting

Once the initial setup is complete, there should be a network connection between the PC and the switch. If a `ping` to the switch fails, verify the IP address and gateway to make sure the subnet and gateway addresses match:

- On the PC, at the command prompt, type: `ipconfig`
- On the switch, at the command prompt, type: `show running x`

Additional information

Catalyst 5000 Family Ethernet and Fast Ethernet Switching Modules Installation and Configuration Note (including Translated Safety warnings 10 languages):
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/cnfg_nts/ethernet/5014etsm.htm#20508

Catalyst 3500 Series XL Hardware Installation Guide Includes Troubleshooting:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc/3500ig/index.htm

Catalyst 2900 Series XL and 3500 Series XL Cisco IOS Release 12.0(5.3)XU:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc/rn53/1061505.htm

Quick Start Guide Catalyst 3500 Series XL Switches:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/3500.htm

Chapter 13. Cisco gigabit switch replacement and configuration

Replacement procedure

To replace the Cisco gigabit switch, see the instructions that came with your switch, or go to: http://www.cisco.com/en/US/products/hw/switches/index.html.

Configure and setup after device replacement

To set up the new switch you need the following:
- Laptop computer
- Hyper Terminal program
- DB9 to RJ45 serial cable

Take the following steps:

1. Connect the RJ45 side of the serial cable to the port on the front of the Cisco switch marked ″CONSOLE.″
2. Connect the other end of the cable to the laptop computer.
3. Start the Hyper Terminal application. Configure the terminal settings to:
   - 9600
   - 8
   - N
   - 1
   - No Flow Control
   - VT100 Emulation
4. At the command prompt in the terminal emulation window, type `enable`. This will put you in administrative mode.
5. At the prompt, type `ibm` and press **B**. The prompt will change from a **>** to a **#** to indicate you are in administrative mode.
6. Type `show run` to show the current configuration information. Make note of the current settings and then logoff from the session.

You need the following information to set up the new switch:
- Switch IP address
- IP mask
- Default gateway IP address
- Switch host name
- Cluster name

The set up procedures are documented in the Cisco Quick Start Guide Catalyst 3500 Series XL Switches:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/3500.htm

After completing the First Time Setup section in the Quick Start Guide, save it to the startup file so the switch can be rebooted without losing the setup. At the `telnet` prompt, type: `copy run start`

The Quick Start Guide also describes how to obtain the JAVA plug-in and configure your browser to support the HTML interface.

Attention: There is an SNMP vulnerability for various versions of switch firmware.

Go to: http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml for specific firmware patches to download.

Setup troubleshooting

Once the initial setup is complete, there should be a network connection between the PC and the switch. If a `ping` to the switch fails, verify the IP address and gateway to make sure the subnet and gateway addresses match:

- On the PC, at the command prompt, type: `ipconfig`
- On the switch, at the command prompt, type: `show running`

Nodes on the same VLAN can communicate via `ping and telnet`. They cannot communicate to nodes on different VLANs. To verify VLANs:

- Connect node1 and node2 to the same VLAN and `ping` node2 from node1. This ping should succeed.
- Connect node1 to VLAN1 and node2 to VLAN2 and `ping` node2 from node1. This ping should fail.

Additional information

Catalyst 5000 Family Ethernet and Fast Ethernet Switching Modules Installation and Configuration Note (including Translated Safety warnings 10 languages):
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/cnfg_nts/ethernet/5014etsm.htm#20508

Catalyst 3500 Series XL Hardware Installation Guide Includes Troubleshooting:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc/3500ig/index.htm

Catalyst 2900 Series XL and 3500 Series XL Cisco IOS Release 12.0(5.3)XU:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc/rn53/1061505.htm

Quick Start Guide Catalyst 3500 Series XL Switches:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/3500.htm

Chapter 14. Cisco 4000 Series switch replacement

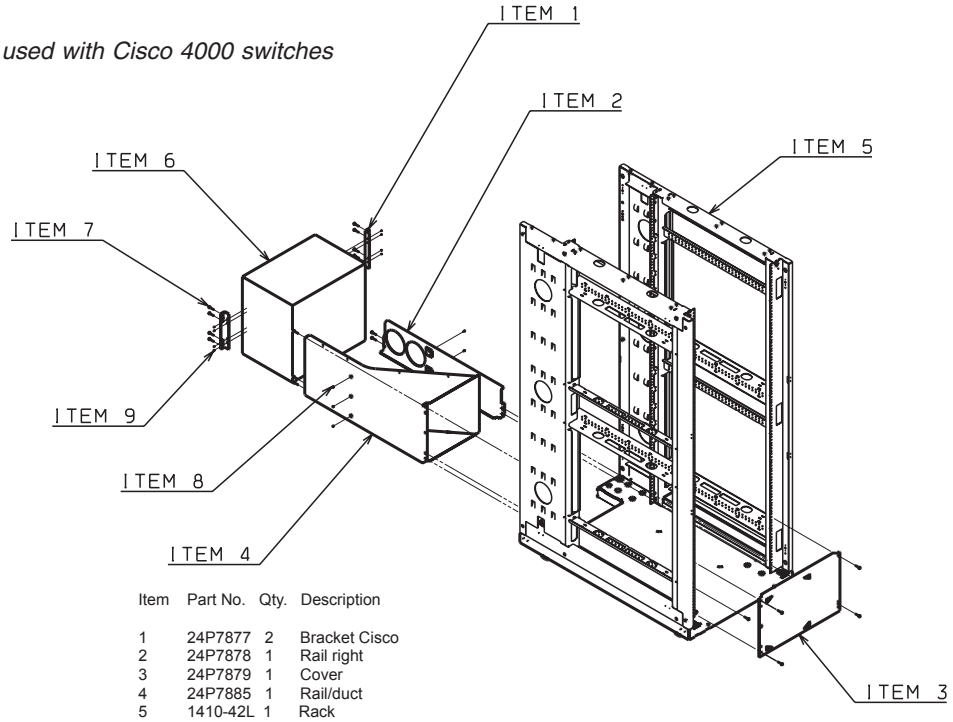
Installation, removal, replacement, and troubleshooting procedures

Detailed hardware maintenance information covering installation, removal, and replacement procedures for the Cisco 4000 series switch is found at:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/hw_doc/install/

Detailed troubleshooting procedures for the Cisco 4000 Series switch are found at:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/trbl_ja.htm

Additionally, IBM has included with each Cisco 4000 Series switch a specially designed thermal duct to make sure proper airflow around the switch. Figure 10 shows an exploded view of the thermal duct and how it fits within the cabinet and attaches to the switch.

Figure 10. Thermal duct used with Cisco 4000 switches



Item	Part No.	Qty.	Description
1	24P7877	2	Bracket Cisco
2	24P7878	1	Rail right
3	24P7879	1	Cover
4	24P7885	1	Rail/duct
5	1410-42L	1	Rack
6	Ref. only	1	Cisco 400x switch
7	12J5289	1	M6 Hex flange screw
8	1621811	5	M4 Hex flange screw
9	N/A	6	M4 Flat head screw

If the Cisco 4000 Series switch is ever removed for maintenance make sure the thermal duct is reinstalled whenever the switch is returned to the cabinet. Failure to reinstall the thermal duct could create temperature management problems within the cabinet.

Additional information

Additional information on a variety of topics (including software configuration) for the Cisco 4000 series switches is available at:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/

Chapter 15. Myrinet 2000

The 2Gb Myrinet switch is a customer option that provides high-speed communication between the storage nodes and cluster nodes, over an optical cable. It requires a Myrinet switch chassis in the primary cabinet and a Myrinet PCI adapter in each storage node and cluster node.

Myrinet PCI board

The Myrinet PCI board resides in the cluster and storage nodes. Use the installation procedures in the applicable server documentation to replace a Myrinet PCI board.

The GM software for running the Myrinet board resides on the cluster and storage nodes, so no new installation of software is required when a Myrinet PCI board is replaced.

Myrinet switch chassis

The Myrinet switch contains the following replaceable components:

8-port line card
Provides the connections to the storage and cluster nodes. The line cards plug into slots in the switch chassis.

Management Module
Manages and routes the Myrinet traffic, polling the ports and building tables to control the addressing of messages.

Blower module
Cools the Myrinet Switch Chassis

All of these components can be hot-swapped. The Myrinet documentation discusses installation of these components.

The three Myrinet Chassis sizes available are described in Table 22.

Table 22. Myrinet Chassis Sizes and Capacities

Slots in switch	Line cards	Nodes supported	EIA slots consumed
5	1-4	4-32	4
9	1-8	4-64	6
17	1-16	4-128	10

If the backplane fails in the Myrinet switch, you must replace the entire switch chassis. Use the following steps to replace the chassis:

1. Make sure that the cluster is not running critical applications.
2. If the optical cables connected to the switch are not labeled, place labels on the cables so they can be located to their respective connectors when the new chassis is installed.
3. Disconnect the optical cables from the connectors on the Myrinet switch. You do not need to power down or change the configuration of the switch before doing this.

   Note: Be sure to install dust caps on all the connectors after the cables are removed.

4. Disconnect the power cord from the Myrinet switch. This powers down the switch.
5. Remove the rack-mount screws from the chassis; then remove the chassis from the rack.
6. Install the new chassis and fasten the rack-mount screws.
7. Connect the optical cables to the connectors on the switch.

   Note: Save the dust caps for future use.
8. Connect the power cord to the Myrinet switch. This powers up the switch.

Configure and setup after device replacement

The Myrinet switch automatically remaps all the PCI boards, so no manual configuration is needed.

IBM Customer Support personnel will update the firmware if necessary.

Additional information

Additional installation and troubleshooting information is available online from Myricom at the following URL: http://www.myri.com/scs/#documentation

Chapter 16. Power Management Module replacement and configuration

Replacing the Power Management Module

The current Power Management Module is the APC MasterSwitch Power Distribution Unit, Model AP9212. We call it the Power Management Module in order to avoid confusion with the IBM Netfinity® Power Distribution Unit (PDU), the fourteen-outlet power distribution bars that fit into side pockets on the mounting rack and plug into the main power supply for the site. In this document, PDU will refer exclusively to the power distribution bars.

To replace the Power Management Module, see the detailed instructions that came with your module.

Configuring after device replacement

1. Configure the new Power Management Module with the same IP address of the Power Management Module you removed.
2. Verify that the firmware level is correct.
3. IBM Customer Support personnel will update the firmware if necessary.
4. For firmware versions prior to 2.2, an SNMP patch must be applied to maintain security. The SNMP patch for the AP9212 is available for download at: http://apcc.com/tools/download/.
5. To reinstall power bricks for the Remote Supervisor Adapter (RSA) cards, see the applicable documentation that came with your power bricks and RSA card.

Related topics

Your cluster might have features that are not described in the documentation that you received with the server. The documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in your server documentation. These updates are available from the IBM Web site. Complete the following steps to check for updated documentation and technical updates:

1. Go to **http://www.ibm.com/pc/support/**.
2. In the **Learn** section, click **Online publications**.
3. On the ″Online publications″ page, in the **Brand** field, select **Options**.
4. In the **Family** field, select **Power Supplies/UPS**.
5. Click **Continue** and select the online documents that best fit your needs.

Chapter 17. Removing and replacing the Power Distribution Unit

The Power Distribution Unit (PDU) provides AC power within the cabinet. The PDUs are mounted sideways beside the regular rack space. Two types of PDUs are used:

- Rack PDUs
- Front-end PDUs

Rack PDUs provide power to components within a cabinet, while front-end PDUs provide the connection to the external power source and distribute the power among the rack PDUs. A rack PDU can also be directly connected to the external power source to eliminate the need for the front-end PDU. Up to four front-end PDUs can be placed in each cabinet and up to twelve rack PDUs.

To remove the Power Distribution Units take the following steps:

1. Shut down all devices.
2. Remove the side cover on the side of the rack that the failing PDU is located on.
3. Turn off each rack PDU using the breaker switch.
4. Unplug each rack PDU from the front-end PDU or customer supplied power source.
5. If present, unplug the front-end PDU from the customer supplied power source.
6. Remove the four screws holding the plate the PDUs are mounted on.
7. Turn the plate over to access the screws that hold the rack PDUs and the front-end PDU (if present) on the plate.
8. Remove the screws holding the failing component to the plate.
9. Replace the failing component (front-end PDU or rack PDU) and reverse the steps shown above to re-install the PDUs.

Appendix A. Frequently asked questions

Here are some frequently asked questions about the IBM @server Cluster 1350.

Q: Why do I sometimes get the error message *"2651-689 Java interface error for method "query": SPException"?*

A: This is due to a defect in the Remote Supervisor Adapter (RSA) firmware that is currently being investigated by xSeries development. This problem occurs after making between 100 and 200 connections to the RSA through the ASM library. The work around is to reset the RSA using the web or telnet interface. Until this defect is fixed, you may want to increase the polling interval for each hardware control point using the command: `chrsrc -s 'Name like "%"' IBM.HwCtrlPoint PollingInterval=86400`

Q: When I issue an `'rpower -n <node> reboot` command why does the node not reboot?

A: Sometimes the Remote Supervisor Adapter (RSA) cards get hung. They can be reset via the web interface, telnetting to the RSA card, or issuing the command `rpower -n <node>resetsp_hcp`.

Q: During installation process tftp hangs on the installing node. What's going on?

A: tftp is not loaded/configured on the management node.

Q: Why doesn't the xSeries 345 boot PXE correctly?

A: You cannot have a PCI ethernet card that uses the e1000 driver in the xSeries 345 when installing. Take the card out and retry the installation.

Q: Why does the dhcp server run out of leases?

A: The problem may be that you have two networks going to the same switch fabric. This causes both *eth0* and *eth1* to see the dhcp requests. To fix this create separate VLANs in the switches, one for each network attached to the switch.

Q: Why did PXE boot not get an IP address using dhcp, but the operating system can?

A: Check the switch. All ports connected to nodes (management, compute, and storage) should have spinning-tree turned off.

Q: Why doesn't the storage node see the drives on the FastT700, but the orange light on the host adapter card still blinks?

A: The qla2300 driver did not load properly. Make sure the proper version of the driver is installed.

Q: What is causing Suse/Sles to continuously install the nodes?

A: Check that fully qualified names (host.domainname) are used in the */etc/hosts* file and that the command `dnsdomainname` returns the correct domain name. Also make sure that */etc/dhcpd.conf* file contains the line: *'option domain-name "cluster.net";'* Once these changes have been made run the `csmsetupsis`command

and then rerun the `installnode` command. If the install still cycles then edit the */csminstall/Linux/SIS/scripts/<hostname>.sh* file and comment out the shutdown line near the bottom of the file. Now using the console watch the boot and the error messages should be on the console when the process has completed.

Q:Why do SuSE/SLES installs take forever?

A: Issue the `installnode` command and then on the management node immediately edit the */tftpboot/pxelinux.cfg/AC** files. Take out *`console= portion`* from the APPEND line. Now all messages will go to the KVM console and the install will be quicker.

Q: Why do SuSE/SLES installs fail but issue no error message?

A: Modify the */tftpboot/pxelinux.cfg/*.sis* file for the node you are trying to install and remove the *`console=ttyS0,9600`* line. Then use the KVM and switch to that node and you can see the error msg.

Appendix B. Error and event logs

There are multiple log files available to help monitor and troubleshoot the cluster:

Linux log

The Linux OS log can be viewed in */var/log/messages*

The system logging daemons are *syslogd* and *klogd*. They are configured via */etc/syslog.conf*.

Log files are automatically rotated by the `logrotate` command. To rotation is configured with the */etc/logrotate.conf* file.

Node log

PC Doctor 2.0 is a ROM-based Diagnostic resident on the servers made available by selecting F2 on boot up. PC Doctor error logs are in the diagnostic portion of the boot up. Press F2 to run diagnostics, then F3 to view log file.

POST/BIOS errors can be read by pressing F1 key during boot process and then selecting View Error Logs from menu. This gives a POST code and description of the error. For example:

```
301 Keyboard Input Error 164 Memory size has changed
```

Cluster System Management log

Cluster System Management (CSM) log files can be viewed in the */var/log/csm/installnode.log* file.

Remote Supervisor Adapter log

Remote Supervisor Adapter (RSA) Adapter log files can be viewed by using `telnet` into the adapter and selecting the *View Log File* from the menu.

American Power Conversion log

You can view the American Power Conversion (APC) event log via Web, FTP or local console I/F:

1. `Telnet` to the switch.
2. From main menu, you will see CTL-L for Event Log.
3. Events are logged in descending order by date, time and event.

Linux Cluster Installation Tool event log

You can view the Linux Cluster Installation Tool (LCIT) event log through a local or remote console or terminal window:

1. Open a console window on the management node.
2. From the root directory, type: `tail -f /var/log/messages`.

Appendix C. Known problems

Node

Amber light on node

There is an amber warning light on the node to indicate the log file is either at 75% or 100% full. To turn off the LED, clear the log.

There is a setting to wrap the log file so the LED never registers if the file is full:

1. Boot using the xSeries 335 Service Processor Firmware diskette.
2. In the Main Menu, select **Configuration Settings**.
3. In the Configuration Menu, select **General Settings**.
4. Set the `75% Full and Log Full` setting to **No**.

COM port settings in BIOS

The COM Port settings for the cluster node should be:

COM Port 1/A
2E8

COM Port 2/B
2F8

Move the serial port jumper from port A to port B on cluster nodes.

CSM

Stale NFS mounts

Existing NFS mounted file systems are inaccessible after a CSM installation on a cluster node.

1. Remount the NFS file systems.
2. If there is an existing */tftpboot* partition on cluster nodes, an error is displayed on the console during CSM installation on the cluster node. Even though an error is displayed, the CSM installation was still successful

rpower hard shut down

The `rpower` command performs a hard shut down. To shut down the OS prior to issuing the `rpower` command issue the following command:

```
dsh -a '/sbin/init 0'
```

Storage

Driver module ordering

During a standard install on the storage nodes the system will attempt to boot from disk located in the FAStT storage device connected to the Qlogic Fibre Channel (FC) Controller instead of the local SCSI drive connected to the internal Adaptec SCSI controller. Why this happens is as follows:

When the modules are loaded, the order ends up in such a way that the driver for the Qlogic FC controller gets loaded before the driver for the Adaptec SCSI Controller. This causes the probing for the devices to occur such that the Fabric

gets assigned *sda*, *sdb*, and so on followed by the local SCSI disks. Make the following modifications to make sure that the SCSI module is loaded before the Fibre module. This will validate that the probing and naming assigns the *sda* device to the first local disk.

1. First, modify the */etc/modules.conf* file by adding the line, `options scsi_mod max_scsi_luns=128` to the end of *modules.conf*. Also remove unnecessary information and reorder the way the modules are loaded. An example of an edited file is as follows:

   Original **modules.conf**:

   ```
   alias eth0 e1000
   alias scsi_hostadapter qla2x00
   alias scsi_hostadapter1 aic7xxx
   alias scsi_hostadapter2 ips
   alias parport_lowlevel parport_pc
   alias scsi_hostadapter2 qla2x00
   alias usb-controller usb-ohci
   alias scsi_hostadapter4 aic7xxx
   ```

   Edited **modules.conf**:

   ```
   alias eth0 e1000
   alias scsi_hostadapter aic7xxx
   alias scsi_hostadapter1 ips
   alias eth1 e1000 alias eth1 e1000
   alias parport_lowlevel parport_pc
   alias scsi_hostadapter3 aic7xxx
   options scsi_mod max_scsi_luns=128
   ```

2. Next, rebuild the two **initrd** images:

   mkinitrd `initrd-2.4.2-2.img 2.4.2-2 -f`

   mkinitrd `initrd-2.4.2-2smp.img 2.4.2-2smp -f`

3. Reboot the node.

KVM

GUI does not appear on first node

If the GUI display does not appear on the first node of the C2T chain, use the text mode.

2x8 Switch powers on with console port B

To remedy this go into the menu settings and change from cooperative to preemptive mode, reselect port 2 and console A will appear. When working properly do a Snapshot to save the setting.

Cluster port 1 reboots

The cluster Port 1 may reboot on power up, and either boots up in text mode blinking every 5 seconds or boots up with a white screen. There are two methods to remedy this situation:

1. Manually select the other ports in the C2T string, then reselect node 1.
2. Unplug the server connections from the port, reattach them in order, and re-plug in the server.

Subsequent KVMs unresponsive

Make sure the KVM switch that was added is in default settings mode.

RSA and Service Processor

If there are any Remote Supervisor Adapter (RSA) errors, check to make sure the RSA is in PCI slot 2.

RSA unable to load firmware

This condition is indicated by error FFFF, 0007. Power cycle the RSA adaptor to clear this condition. The RSA may need to be replaced if this condition persists.

RSA/Service Processor invalid naming

There cannot be any spaces when assigning names of the RSA and Service Processor. If a name is not recognized, verify that there are no trailing blanks after the name.

Light path points to PCI LED

If Light Path diagnostics points to PCI LED, reseat the PCI boards.

Myrinet communication fails

If communication fails over Myrinet then check the following:

- If the Myricom adapter card green LED light is not on, check the cable connector for correct polarity (transmit/receive).
- Check to see that the GM module is installed by running the `lsmod` command.
- Check to see if the Myricom adapter is up and running by using the `ifconfig` command.

Appendix D. Configuring network switches

General networking notes

When setting up switches in the 512 mode or any time there intentionally are multiple connections between switches you must designate one of the core switches as the spanning tree root. In the case of the 512 node configuration it must be one of the 4006's.

When setting up VLANs on a 4006 running Catos make sure to set the vtp domain name. This can be any name since we are not using vtp to maintain the VLANs.

3508/3524 switches only have 1 virtual Ethernet port. This can be assigned to any VLAN on the switch. Which ever VLAN it is assigned to should be designated as the Management VLAN for the switch.

4006 running IOS can have an IP connection for each VLAN. However the management port on the SUP card can only be used for recovery situations. 1 port in the Management VLAN can be dedicated to hook up the management network to the 4006.

4006 running Catos has one port that can be used for an Ethernet connection. It is sc0 and can be in any VLAN. For our purposes it should be assigned to the Management VLAN. Again one port assigned to the Management VLAN needs to be reserved to make the connection to the switch itself. It is the same story as above for the management port on the SUP card.

Load balancing across Etherchannels is an important performance point. This is something that would be unique to the jobs that the customer intends to run on the cluster.

To split networks, creating a primary cluster VLAN and a Management VLAN in the switches, requires an extra connection between the 3550 and the 3508.

RJ45 (copper) adapter GBICS must be connected to a gigabit port or it will not link. Those GBICS will not negotiate speed.

The Linux kernel by default supports proxy arping. This can cause problems on a shared media network. If you have more that one NIC in the same broadcast domain the problem will happen. Proxy arping allows either interface in the broadcast domain to respond to an arp request. This can cause IP traffic to be handled by an interface other than the intended one. The only way to prevent this is to create separate VLANs in the switches.

Switch commands

Use the following section for information on switch commands.Use the command line interface for executing commands.

Switch commands for 3508/3550 running IOS

These commands will work with a 4006 running IOS as well. To set up VLANs, at the command prompt, type:

```
vlan database
vtp transparent
vlan <id>  name <string>
exit
```

To assign ports to the VLAN, type:

```
conf t
int mod/port
switchport access vlan <id>
end
```

To set Ethernet address for switch assign to Management VLAN, type:

```
conf t
int vlan <id>
ip address <ip address> <netmask>
managment
end
```

To assign a name to the switch, type:

```
set system name <some string>
conf t
hostname <string>
end
```

To see the VLAN setup, type:

```
show vlan
```

To see spanning tree information on a port by port basis, type:

```
show spanning-tree brief //
```

Switch commands for 4006 running IOS

These commands will work with 3550 running IOS as well. To set up VLANs, at the command prompt, type:

```
conf t
vlan <id>
name <management network>
end
```

To assign ports to the VLAN, type:

```
conf t
vlan <id>
name <management network>
end
```

To set Ethernet address for switch assigned to Management VLAN, type:

```
conf t
int vlan <id>
ip address <ip address> <netmask>
end
```

To assign a name to the switch, type:

```
set system name <some string>
conf t
hostname <string>
end
```

To create an Etherchannel, type:

```
conf t
int range <mode/port> - <port>
channel-group <id> mode desirable non-silent
end
```

To remove an Etherchannel, type:

```
conf t
int range <mode/port> - <port>
no channel-group
end
```

For the following command to work make sure all ports in the group are set up identically.

```
conf t
int range <mode/port> - <port>
channel-group <id> mode desirable on
end
```

This command generates an error message about port differences. Once the command completes, set it back to the desirable mode.

To turn off the spanning tree on ports going to cluster and storage nodes, type:

```
conf t
int range <mode/port> - <port>
switchport host
end
```

To see the VLAN setup, type:

```
show vlan
```

To set the switch as the spanning tree root. Run the command once for each VLAN:

```
conf t
spanning-tree <id> root primary
end
```

To set the switch as the spanning tree root secondary. Run the command once for each VLAN:

```
conf t
spanning-tree <id> root secondary
end
```

See spanning tree root information on a port by port basis:

```
show spanning-tree brief
```

See Etherchannels that are up and running:

```
show etherchannel
```

Switch commands for 4006 running CATOS

To set up VLANs, type:

```
set vtp domain <string>
set vlan <2> name <management-network>
```

To assign ports to the VLAN, type:

```
set vlan <2> 2/1-10
```

To set Ethernet address for switch assigned to Management VLAN, type:

```
set interface sc0 <2> <172.30.50.3/255.255.0.0>
```

To set switch interface to a VLAN, type:

```
set interface sc0 <2>
```

To create an Etherchannel, type:

```
set port channel mod/port mode desirable non-silent
```

To assign a name to the switch, type:

```
set system name <some string>
```

For the following command to succeed make sure all ports in the group are set up identically. If an Etherchannel does not form, type:

```
set port channel <mod/port> mode on
```

This command generates an error message about port differences. Once the command succeeds, set it back to the desirable mode.

To turn off the spanning tree on ports going to compute and storage nodes, type:

```
set port host
```

To see the VLAN setup, type:

```
show vlan
```

To set the switch as the spanning tree primary, type:

```
set spantree root <vlanid>
```

To set the switch as the spanning tree secondary, type:

```
set spantree root secondary <vlanid>
```

To view spanning tree root information on a port by port basis, type:

```
show spantree
```

To view Etherchannels that are up and running, type:

```
show channel
```

To disable and reenable an Etherchannel that fails to link up, type:

```
set port disable <mod/port>
set port enable <mod/port>
```

Miscellaneous CISCO switch commands for CATOS

To clear configuration information from all modules in the switch, type:

```
clear config <all>
```

To clear configuration information from a module, type:

```
clear config <mod>
```

To view what ports are blocked by spanning tree, type:

```
show spantree
```

Miscellaneous CISCO switch commands for IOS

To view the ports that are blocked by the spanning tree, type:

```
show sp br
```

Appendix E. International License Agreement for Non-Warranted Programs

Part 1 - General Terms

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE PROGRAM. IBM WILL LICENSE THE PROGRAM TO YOU ONLY IF YOU FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY USING THE PROGRAM YOU AGREE TO THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PROGRAM TO THE PARTY (EITHER IBM OR ITS RESELLER) FROM WHOM YOU ACQUIRED IT TO RECEIVE A REFUND OF THE AMOUNT YOU PAID.

The Program is owned by International Business Machines Corporation or one of its subsidiaries (IBM) or an IBM supplier, and is copyrighted and licensed, not sold.

The term ″Program″ means the original program and all whole or partial copies of it. A Program consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings, or pictures), and related licensed materials.

This Agreement includes **Part 1 - General Terms**, **Part 2 - Country-unique Terms**, and **License Information** and is the complete agreement regarding the use of this Program, and replaces any prior oral or written communications between you and IBM. The terms of **Part 2** and **License Information** may replace or modify those of **Part 1**.

1. **License**

   Use of the Program: IBM grants you a nonexclusive license to use the Program. You may 1) use the Program to the extent of authorizations you have acquired and 2) make and install copies to support the level of use authorized, providing you reproduce the copyright notice and any other legends of ownership on each copy, or partial copy, of the Program. If you acquire this Program as a program upgrade, your authorization to use the Program from which you upgraded is terminated. You will make sure that anyone who uses the Program does so only in compliance with the terms of this Agreement. You may not 1) use, copy, modify, or distribute the Program except as provided in this Agreement; 2) reverse assemble, reverse compile, or otherwise translate the Program except as specifically permitted by law without the possibility of contractual waiver; or 3) sublicense, rent, or lease the Program. Transfer of Rights and Obligations You may transfer all your license rights and obligations under a Proof of Entitlement for the Program to another party by transferring the Proof of Entitlement and a copy of this Agreement and all documentation. The transfer of your license rights and obligations terminates your authorization to use the Program under the Proof of Entitlement.

2. **Proof of Entitlement**

   The Proof of Entitlement for this Program is evidence of your authorization to use this Program and of your eligibility for any future upgrade program prices (if announced), and potential special or promotional opportunities.

3. **Charges and Taxes**

   IBM defines use for the Program for charging purposes and specifies it in the Proof of Entitlement. Charges are based on extent of use authorized. If you

wish to increase the extent of use, notify IBM or its reseller and pay any applicable charges. IBM does not give refunds or credits for charges already due or paid.

If any authority imposes a duty, tax, levy or fee, excluding those based on IBM's net income, upon the Program supplied by IBM under this Agreement, then you agree to pay that amount as IBM specifies or supply exemption documentation.

4. **No Warranty**

   SUBJECT TO ANY STATUTORY WARRANTIES WHICH CAN NOT BE EXCLUDED, IBM MAKES NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THE WARRANTY OF NON-INFRINGEMENT AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY. IBM MAKES NO WARRANTY REGARDING THE CAPABILITY OF THE PROGRAM TO CORRECTLY PROCESS, PROVIDE AND/OR RECEIVE DATE DATA WITHIN AND BETWEEN THE 20TH AND 21ST CENTURIES.

   The exclusion also applies to any of IBM's subcontractors, suppliers, or program developers (collectively called ″Suppliers″).

   Manufacturers, suppliers, or publishers of non-IBM Programs may provide their own warranties.

5. **Limitation of Liability**

   NEITHER IBM NOR ITS SUPPLIERS WILL BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST SAVINGS, OR ANY INCIDENTAL, SPECIAL, OR OTHER ECONOMIC CONSEQUENTIAL DAMAGES, EVEN IF IBM IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

6. **General**

   Nothing in this Agreement affects any statutory rights of consumers that cannot be waived or limited by contract.

   IBM may terminate your license if you fail to comply with the terms of this Agreement. If IBM does so, your authorization to use the Program is also terminated and you must immediately destroy the Program and all copies you made of it.

   You agree to comply with applicable export laws and regulations.

   Neither you nor IBM will bring a legal action under this Agreement more than two years after the cause of action arose unless otherwise provided by local law without the possibility of contractual waiver or limitation.

   Neither you nor IBM is responsible for failure to fulfill any obligations due to causes beyond its control. The laws of the country in which you acquire the Program govern this Agreement, except 1) in Australia, the laws of the State or Territory in which the transaction is performed govern this Agreement; 2) in Albania, Armenia, Belarus, Bosnia/Herzegovina, Bulgaria, Croatia, Czech Republic, Federal Republic of Yugoslavia, Georgia, Hungary, Kazakhstan, Kirghizia, Former Yugoslav Republic of Macedonia (FYROM), Moldova, Poland, Romania, Russia, Slovak Republic, Slovenia, and Ukraine, the laws of Austria govern this Agreement; 3) in the United Kingdom, all disputes relating to this Agreement will be governed by English Law and will be submitted to the exclusive jurisdiction of the English courts; 4) in Canada, the laws in the Province of Ontario govern this Agreement; and 5) in the United States and Puerto Rico, and People's Republic of China, the laws of the State of New York govern this Agreement.

Part 2 - Country-unique Terms

AUSTRALIA: No Warranty (Section 4): The following paragraph is added to this Section: Although IBM specifies that there are no warranties, you may have certain rights under the Trade Practices Act 1974 or other legislation and are only limited to the extent permitted by the applicable legislation.

Limitation of Liability (Section 5): The following paragraph is added to this Section: Where IBM is in breach of a condition or warranty implied by the Trade Practices Act 1974, IBM's liability is limited to the repair or replacement of the goods, or the supply of equivalent goods. Where that condition or warranty relates to right to sell, quiet possession or clear title, or the goods are of a kind ordinarily acquired for personal, domestic or household use or consumption, then none of the limitations in this paragraph apply.

GERMANY: No Warranty (Section 4): The following paragraphs are added to this Section: The minimum warranty period for Programs is six months. In case a Program is delivered without Specifications, we will only warrant that the Program information correctly describes the Program and that the Program can be used according to the Program information. You have to check the usability according to the Program information within the ″money-back guarantee″ period.

Limitation of Liability (Section 5): The following paragraph is added to this Section: The limitations and exclusions specified in the Agreement will not apply to damages caused by IBM with fraud or gross negligence, and for express warranty.

INDIA: General (Section 6): The following replaces the fourth paragraph of this Section: If no suit or other legal action is brought, within two years after the cause of action arose, in respect of any claim that either party may have against the other, the rights of the concerned party in respect of such claim will be forfeited and the other party will stand released from its obligations in respect of such claim.

IRELAND: No Warranty (Section 4): The following paragraph is added to this Section: Except as expressly provided in these terms and conditions, all statutory conditions, including all warranties implied, but without prejudice to the generality of the foregoing, all warranties implied by the Sale of Goods Act 1893 or the Sale of Goods and Supply of Services Act 1980 are hereby excluded.

ITALY: Limitation of Liability (Section 5): This Section is replaced by the following: Unless otherwise provided by mandatory law, IBM is not liable for any damages which might arise.

NEW ZEALAND: No Warranty (Section 4): The following paragraph is added to this Section: Although IBM specifies that there are no warranties, you may have certain rights under the Consumer Guarantees Act 1993 or other legislation which cannot be excluded or limited. The Consumer Guarantees Act 1993 will not apply in respect of any goods or services which IBM provides, if you require the goods or services for the purposes of a business as defined in that Act.

Limitation of Liability (Section 5): The following paragraph is added to this Section: Where Programs are not acquired for the purposes of a business as defined in the Consumer Guarantees Act 1993, the limitations in this Section are subject to the limitations in that Act.

PEOPLE'S REPUBLIC OF CHINA: Charges (Section 3): The following paragraph is added to the Section: All banking charges incurred in the People's Republic of China will be borne by you and those incurred outside the People's Republic of China will be borne by IBM.

UNITED KINGDOM: Limitation of Liability (Section 5): The following paragraph is added to this Section at the end of the first paragraph: The limitation of liability will not apply to any breach of IBM's obligations implied by Section 12 of the Sale of Goods Act 1979 or Section 2 of the Supply of Goods and Services Act 1982.

License Information

Program: Embedded Software from Cisco Systems, Inc.

Program-unique Terms

The following terms and conditions are in addition to those of the IBM International License Agreement for Non-Warranted Programs (ILAN). Solely with respect to your use of the Cisco software (the ″Cisco Software″) contained within the IBM product you have purchased.

1. Your license to the Cisco Software is a license to (a) use the software in the operation of a Cisco networking product only; (b) make not more than one (1) copy of the Cisco Software, which you may use only for purposes of backup and disaster recovery. You may not otherwise copy the Cisco Software, and you may not transfer the Cisco Software, even if you sell or lease the Cisco networking product with which the Cisco Software is provided. The purchaser or other transferee of the Cisco Software must obtain from Cisco or a Cisco reseller (including IBM) a new license to use the Cisco Software.
2. In addition to the warranty disclaimers provided in Point 4 of the ILA, Cisco disclaims any warranty that the Cisco Software or any equipment, system or network on which the Cisco Software is used will be free of vulnerability to intrusion or attack.
3. In the event you breach any provision of the ILA provided to you, or any provision of these additional terms, your right to use the Cisco Software will terminate immediately.
4. If you received the Cisco Software in the European Union, the Middle East, or Africa, the law applicable to your use of the Cisco Software is English law. If you received the Cisco Software in Canada, the law applicable to your use of the Cisco Software is Ontario law. If you received the Cisco Software in Australia or New Zealand, the law applicable to your use of the Cisco Software is Australian law. If you received the Cisco Software elsewhere in the world, the law applicable to your use of the Cisco Software is the law of the State of California, the United States of America.
5. For United States government users, the Cisco Software is Commercial Computer Software provided with Restricted Rights per the terms of the Federal Acquisition Regulation.
6. In the event you receive upgrades to the Cisco Software, you may only use such upgrades if, at the time you receive them, you have a valid license to use the Cisco Software which was upgraded or updated.

Appendix F. 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

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	TotalStorage
FlashCopy	Update Connector
IBM	Wake on LAN
IBM (logo)	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. 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 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

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。

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。

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

X

Printed in U.S.A.