Cisco HX220c M4 Hyperflex Node Installation Guide

March 22, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

Cisco HX220c M4 Hyperflex Node Installation Guide

CONTENTS

CHAPTER 1

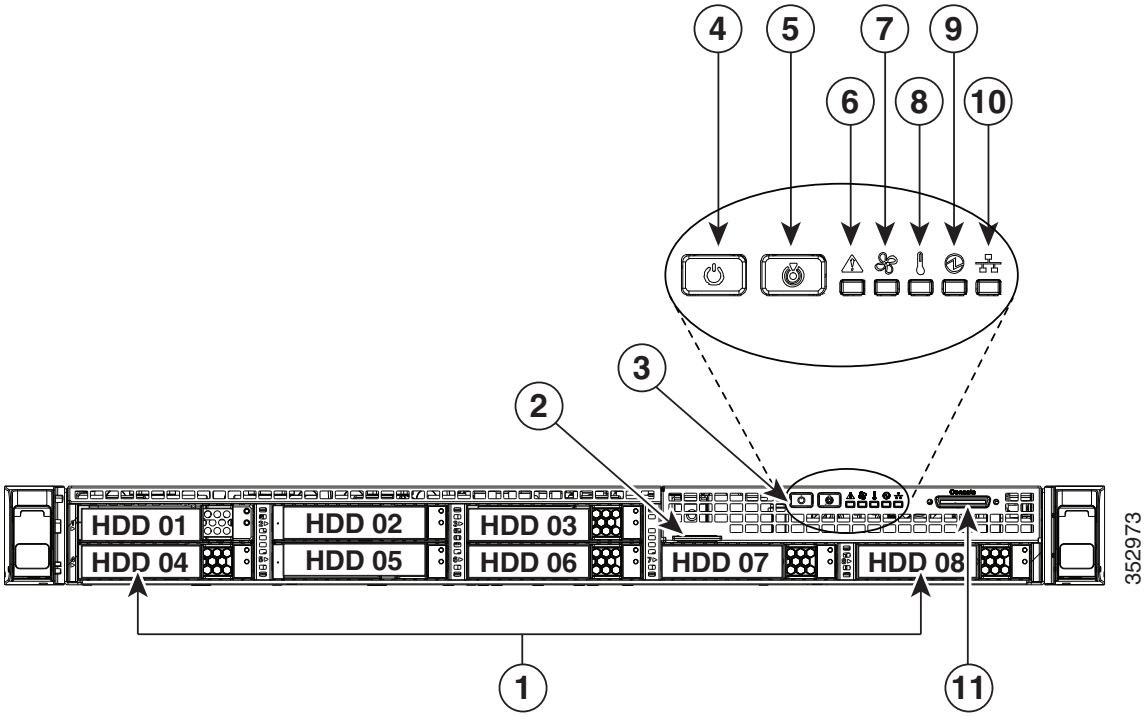
Overview

This chapter provides an overview of the Cisco HX220c M4 Hyperflex Node features:

External Features Overview

Figure 1-1 shows the front panel features.

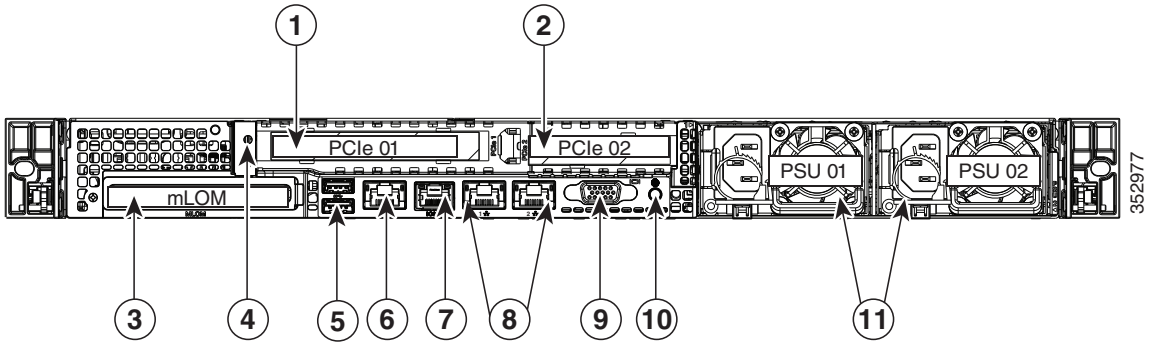
Figure 1-1 Front Panel Features



1	Drive bays 1–8 support SAS/SATA drives	**7**	Node status LED
2	Drive bays 1 and 2 support SAS/SATA and NVMe PCIe solid state drives (SSDs).	**8**	Fan status LED
3	Pull-out asset tag	**9**	Temperature status LED
4	Operations panel buttons and LEDs	**10**	Power supply status LED
5	Power button/power status LED	**11**	Network link activity LED
6	Unit identification button/LED	**12**	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)

Figure 1-2 shows the rear panel features of the node.

Figure 1-2 Rear Panel Features

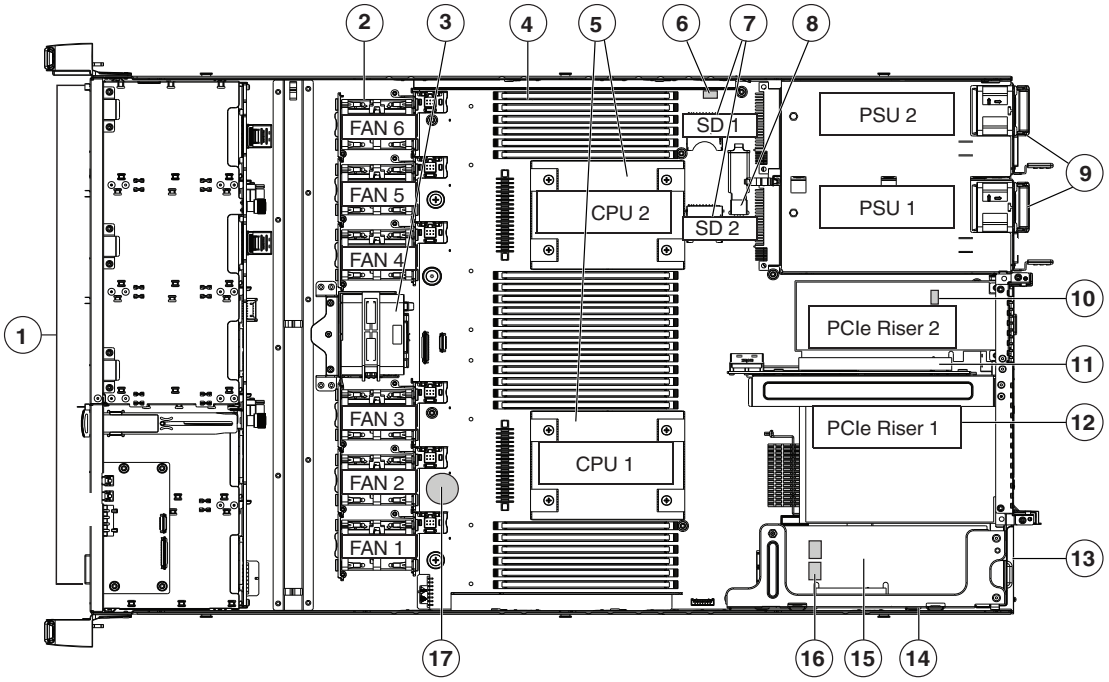


1	PCIe riser 1/slot 1	**7**	Serial port (RJ-45 connector)
2	PCIe riser 2/slot 2	**8**	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
3	Modular LAN-on-motherboard (mLOM) card slot	**9**	VGA video port (DB-15)
4	Grounding-lug hole (for DC power supplies)	**10**	Rear unit identification button/LED
5	USB 3.0 ports (two)	**11**	Power supplies (up to two, redundant as 1+1)
6	1-Gb Ethernet dedicated management port		

Replaceable Component Locations

This section shows the locations of the field-replaceable components. The view in Figure 1-3 is from the top down with the top cover and air baffle removed.

Figure 1-3 Replaceable Component Locations



1	Drive bays 1–8 support SAS/SATA drives. Drive bays 1 and 2 support SAS/SATA drives and NVMe PCIe SSDs. NVMe drives require PCIe riser version 2B in the node to provide the PCIe bus connection.	**10**	Trusted platform module (TPM) socket on motherboard (not visible in this view)
2	Cooling fan modules (six)	**11**	PCIe riser 2 (half-height PCIe slot 2)
3	Supercap Power Module (RAID backup) mounting bracket	**12**	PCIe riser 1 (full-height PCIe slot 1)
4	DIMM sockets on motherboard (24)	**13**	Modular LOM (mLOM) connector on chassis floor
5	CPUs and heatsinks (two)	**14**	Cisco modular RAID controller PCIe riser (dedicated riser with horizontal socket)
6	Embedded SATA RAID header for RAID 5 key	**15**	Cisco modular RAID controller card
7	SD card bays on motherboard (two)	**16**	Embedded SATA RAID mini-SAS connectors on motherboard (not visible in this view)
8	Internal USB 3.0 port on motherboard	**17**	RTC battery on motherboard
9	Power supplies (up to two, hot-swappable when redundant as 1+1)		

Summary of Node Features

Table 1-1 lists the features of the node.

Table 1-1 Cisco HX220c M4 Hyperflex Node Features

Feature	Description
Chassis	One rack-unit (1RU) chassis.
Processors	Two Intel Xeon E5-2600 v3 Series processors.
Memory	24 DDR4 DIMM[1] sockets on the motherboard (12 each CPU).
Multi-bit error protection	Multi-bit error protection is supported.
Baseboard management	BMC, running Cisco Integrated Management Controller (Cisco IMC) firmware. Depending on your Cisco IMC settings, Cisco IMC can be accessed through the 1-Gb dedicated management port, the 1-Gb Ethernet LOM ports, or a Cisco virtual interface card.
Network and management I/O	Supported connectors: • One 1-Gb Ethernet dedicated management port • Two 1-Gb BASE-T Ethernet LAN ports • One RS-232 serial port (RJ-45 connector) • One 15-pin VGA[2] connector • Two USB[3] 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector.
Modular LOM	Dedicated socket that can be used to add an mLOM card for additional rear-panel connectivity.
WoL	1-Gb BASE-T Ethernet LAN ports support the wake-on-LAN (WoL) standard.
Power	Two power supplies: • AC power supplies 770 W AC each. Do not mix power supply types or wattages in the node. Redundant as 1+1. See Power Specifications, page A-3.
ACPI	The advanced configuration and power interface (ACPI) 4.0 standard is supported.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
PCIe I/O	Two horizontal PCIe[4] expansion slots (single riser assembly).
InfiniBand	The bus slots in this node support the InfiniBand architecture.
Storage	Drives are installed into front-panel drive bays hold up to eight 2.5-inch SAS/SATA drives. SAS/SATA drives are hot-swappable.[5]
Internal USB	One internal USB 3.0 port on the motherboard that you can use with a USB thumb drive for additional storage.
SD cards	Two internal bays on the motherboard for up to two SD cards. The two flash drives can be configured in a RAID 1 configuration.

Table 1-1 Cisco HX220c M4 Hyperflex Node Features (continued)

Feature	Description (continued)
Disk Management	The node has a dedicated internal riser for a PCIe-style Cisco modular controller card. For a list of controller options and required cabling, see Supported RAID Controllers and Required Cables, page C-2.
RAID Backup	The node has a mounting bracket for the supercap power module that is used with Cisco modular RAID controller card.
Video	VGA video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory.

1. DIMM = dual inline memory module
2. VGA = video graphics array
3. USB = universal serial bus
4. PCIe = peripheral component interconnect express
5. Hot swappable = no shutdown of the components is required before removal with the node power on.

CHAPTER 2

Installing the Node

This chapter describes how to install the node, and it includes the following sections:

Note Before you install, operate, or service a node, review the *Regulatory Compliance and Safety Information for Cisco UCS C-Series Servers* for important safety information.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

Unpacking and Inspecting the Node

Caution When handling internal node components, wear an ESD strap and handle modules by the carrier edges only.

Tip Keep the shipping container in case the node requires shipping in the future.

Note The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

Step 1 Remove the node from its cardboard container and save all packaging material.

Step 2 Compare the shipment to the equipment list provided by your customer service representative. Verify that you have all items.

Step 3 Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

- Invoice number of shipper (see the packing slip)
- Model and serial number of the damaged unit
- Description of damage
- Effect of damage on the installation

Preparing for Node Installation

This section provides information about preparing for node installation, and it includes the following topics:

Installation Guidelines

Warning **To prevent the node from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° F).**
Statement 1047

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.**
Statement 1019

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A.**
Statement 1005

Warning **Installation of the equipment must comply with local and national electrical codes.**
Statement 1074

Caution To ensure proper airflow it is necessary to rack the nodes using rail kits. Physically placing the units on top of one another or "stacking" without the use of the rail kits blocks the air vents on top of the nodes, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your nodes on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the nodes. No additional spacing between the nodes is required when you mount the units using rail kits.

When you are installing a node, use the following guidelines:

- Ensure that there is adequate space around the node to allow for servicing the node and for adequate airflow. The airflow in this node is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the Environmental Specifications, page A-2.

- Ensure that the cabinet or rack meets the requirements listed in the "Rack Requirements" section on page 2-4.
- Ensure that the site power meets the power requirements listed in the Power Specifications, page A-3. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Rack Requirements

This section provides the requirements for the standard open racks.

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per node must be one RU, equal to 1.75 in. (44.45 mm).

Equipment Requirements

The slide rails sold by Cisco for this node do not require tools for installation.

Supported Slide Rail Kits

This node supports two rail kit options:

- Cisco part UCSC-RAILB-M4= (ball-bearing rail kit).
- Cisco part UCSC-RAILF-M4= (friction rail kit).

Slide Rail Adjustment Range and Cable Management Arm Dimensions

The slide rails for this node have an adjustment range of 24 to 36 inches (610 to 914 mm).

The optional cable management arm (CMA) adds additional length requirements:

- The additional distance from the rear of the node to the rear of the CMA is 5.4 inches (137.4 mm).
- The total length of the node including the CMA is 35.2 inches (894 mm).

Installing the Node In a Rack

This section contains the following sections:

Installing the Slide Rails

This section describes how to install the node in a rack using the rack kits that are sold by Cisco.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the node remains stable. The following guidelines are provided to ensure your safety:**
This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
Statement 1006

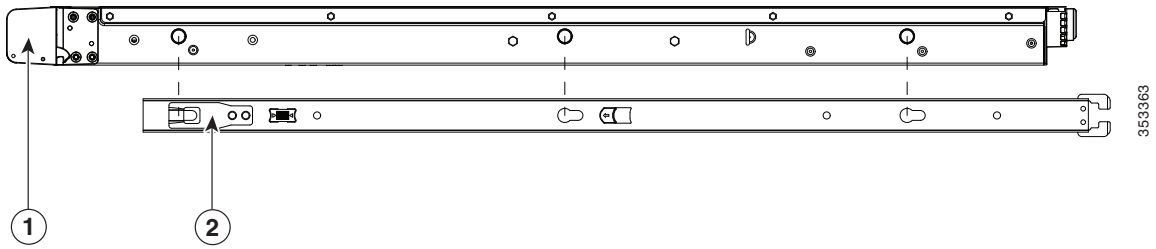
Step 1 Attach the inner rails to the sides of the node:

a. Align an inner rail with one side of the node so that the three keyed slots in the rail align with the three pegs on the side of the node (see Figure 2-1).

b. Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

c. Install the second inner rail to the opposite side of the node.

Figure 2-1 Attaching Inner Rail to Side of Node

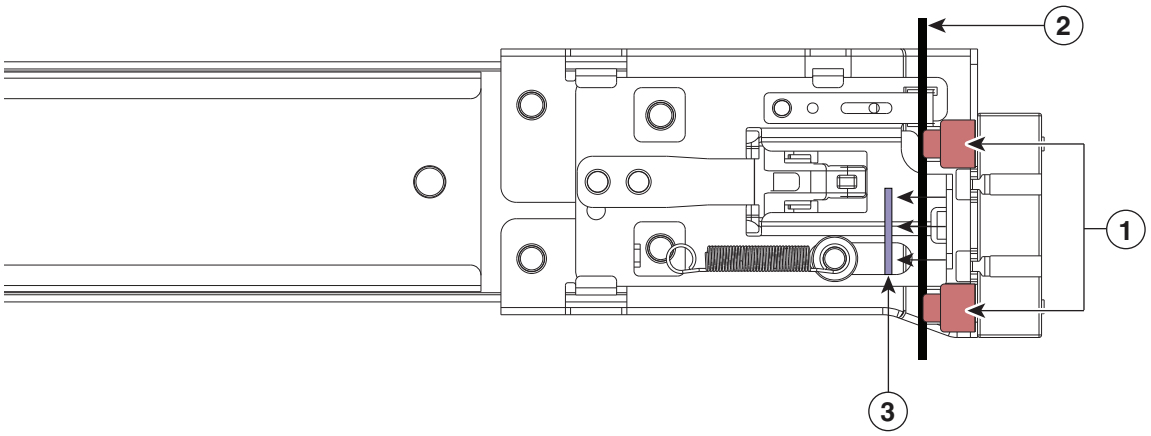


1	Front of node	2	Locking clip on inner rail

Step 2 Open the front securing plate on both slide-rail assemblies. The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes (see Figure 2-2).

On the *outside* of the assembly, push the green arrow button toward the rear to open the securing plate.

Figure 2-2 Front Securing Mechanism, Inside of Front End



1	Front mounting pegs	**3**	Securing plate shown pulled back to open position
2	Rack post		

Step 3 Install the outer slide rails into the rack:

a. Align one slide-rail assembly front end with the front rack-post holes that you want to use.

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front (see Figure 2-2).

Note The rack post must be between the mounting pegs and the *open* securing plate.

b. Push the mounting pegs into the rack-post holes from the outside-front.

c. Press the securing plate release button, marked PUSH. The spring-loaded securing plate closes to lock the pegs in place.

d. Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear rack-post holes. The slide rail must be level front-to-rear.

The rear mounting pegs enter the rear rack-post holes from the inside of the rack post.

e. Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height with each other and are level front-to-back.

f. Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Step 4 Insert the node into the slide rails:

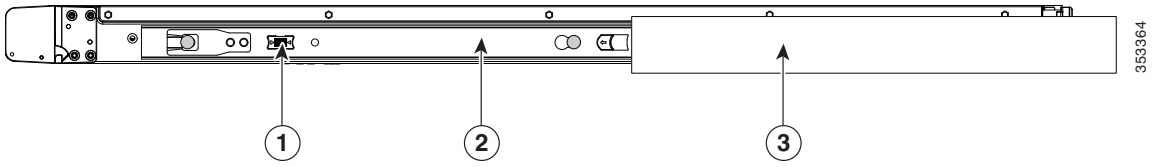
Caution This node can weigh up to 67 pounds (59 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the node. Attempting this procedure alone could result in personal injury or equipment damage.

a. Align the rear of the inner rails that are attached to the node sides with the front ends of the empty slide rails on the rack.

b. Push the inner rails into the slide rails on the rack until they stop at the internal stops.

c. Slide the release clip toward the rear on both inner rails, and then continue pushing the node into the rack until its front slam latches engage with the rack posts.

Figure 2-3 Inner Rail Release Clip



1	Inner rail release clip	**3**	Outer rail attached to rack post
2	Inner rail attached to node and inserted into outer rail		

Step 5 (Optional) Secure the node in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with nodes installed.

With the node fully pushed into the slide rails, open a hinged slam latch lever on the front of the node and insert the screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the node from being pulled out. Repeat for the opposite slam latch.

Installing the Cable Management Arm (Optional)

Note The CMA is reversible left to right. To reverse the CMA, see Reversing the Cable Management Arm (Optional), page 2-9 before installation.

Step 1 With the node pushed fully into the rack, slide the CMA tab of the CMA arm that is farthest from the node onto the end of the stationary slide rail that is attached to the rack post (see Figure 2-4). Slide the tab over the end of the rail until it clicks and locks.

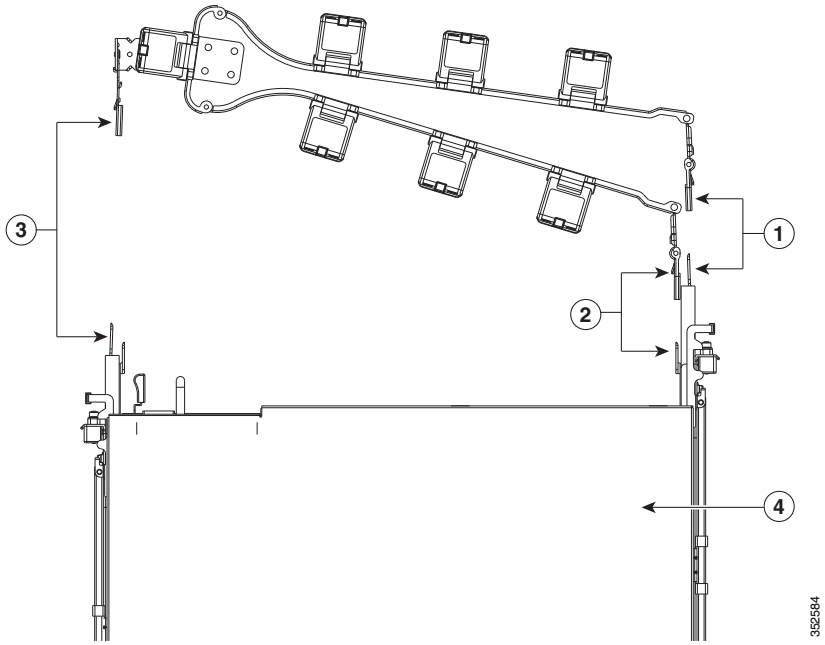
Step 2 Slide the CMA tab that is closest to the node over the end of the inner rail that is attached to the node (see Figure 2-4). Slide the tab over the end of the rail until it clicks and locks.

Step 3 Pull out the width-adjustment slider that is at the opposite end of the CMA assembly until it matches the width of your rack (see Figure 2-4).

Step 4 Slide the CMA tab that is at the end of the width-adjustment slider onto the end of the stationary slide rail that is attached to the rack post (see Figure 2-4). Slide the tab over the end of the rail until it clicks and locks.

Step 5 Open the hinged flap at the top of each plastic cable guide and route your cables through the cable guides as desired.

Figure 2-4 Attaching the Cable Management Arm to the Rear of the Slide Rails



1	CMA tab on arm farthest from node and end of stationary outer slide rail	**3**	CMA tab on width-adjustment slider and end of stationary outer slide rail
2	CMA tab on arm closest to the node and end of inner slide rail attached to node	**4**	Rear of node

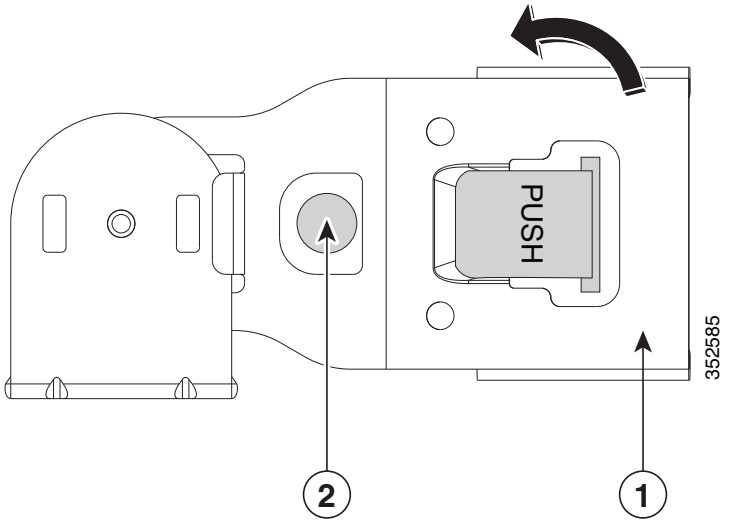
Reversing the Cable Management Arm (Optional)

Step 1 Rotate the entire CMA assembly 180 degrees. The plastic cable guides must remain pointing upward.

Step 2 Flip the tabs at the end of each CMA arm so that they point toward the rear of the node.

Step 3 Pivot the tab that is at the end of the width-adjustment slider. Depress and hold the metal button on the outside of the tab and pivot the tab 180 degrees so that it points toward the rear of the node.

Figure 2-5 Reversing the CMA



1	CMA tab on end of width-adjustment slider	**2**	Metal button for rotating

Initial Node Setup

Connecting and Powering On the Node (Standalone Mode)

Note This section describes how to power on the node, assign an IP address, and connect to node management when using the node *in standalone mode*. To use the node in Cisco UCS Manager integration, specific cabling and settings are required. See Installation for Cisco UCS Manager Integration, page D-1.

The node is shipped with these default settings:

- The NIC mode is Shared LOM EXT.

  Shared LOM EXT mode enables the 1-Gb Ethernet ports and the ports on any installed Cisco virtual interface card (VIC) to access Cisco Integrated Management Interface (Cisco IMC). If you want to use the 10/100/1000 dedicated management ports to access Cisco IMC, you can connect to the node and change the NIC mode as described in Step 1 of the following procedure.
- The NIC redundancy is active-active. All Ethernet ports are utilized simultaneously.
- DHCP is enabled.
- IPv4 is enabled.

There are two methods for connecting to the node for initial setup:

- Local setup—Use this procedure if you want to connect a keyboard and monitor to the node for setup. This procedure can use a KVM cable (Cisco PID N20-BKVM) or the ports on the rear of the node. See Local Connection Procedure, page 2-10.
- Remote setup—Use this procedure if you want to perform setup through your dedicated management LAN. See Remote Connection Procedure, page 2-11.

Note To configure the node remotely, you must have a DHCP server on the same network as the node. Your DHCP server must be preconfigured with the range of MAC addresses for this node. The MAC address is printed on a label that is on the pull-out asset tag on the front panel (see Figure 1-1). This node has a range of six MAC addresses assigned to the Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

Local Connection Procedure

Step 1 Attach a power cord to each power supply in your node, and then attach each power cord to a grounded AC power outlet. See Power Specifications, page A-3 for power specifications.

Wait for approximately two minutes to let the node boot in standby power during the first bootup.

You can verify node power status by looking at the node Power Status LED on the front panel (see External Features Overview, page 1-2). The node is in standby power mode when the LED is amber.

Step 2 Connect a USB keyboard and VGA monitor to the node using one of the following methods:

- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel (see External Features Overview, page 1-2).

- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel (see External Features Overview, page 1-2 for the connector location). Connect your USB keyboard and VGA monitor to the KVM cable.

Step 3 Open the Cisco IMC Configuration Utility:

a. Press and hold the front panel power button for four seconds to boot the node.

b. During bootup, press **F8** when prompted to open the Cisco IMC Configuration Utility.

This utility has two windows that you can switch between by pressing F1 or F2.

Step 4 Continue with Cisco IMC Configuration Utility Setup, page 2-12.

Remote Connection Procedure

Step 1 Attach a power cord to each power supply in your node, and then attach each power cord to a grounded AC power outlet. See Power Specifications, page A-3 for power specifications.

Wait for approximately two minutes to let the node boot in standby power during the first bootup.

You can verify node power status by looking at the node Power Status LED on the front panel (see External Features Overview, page 1-2). The node is in standby power mode when the LED is amber.

Step 2 Plug your management Ethernet cable into the dedicated management port on the rear panel (see External Features Overview, page 1-2).

Step 3 Allow your preconfigured DHCP server to assign an IP address to the node.

Step 4 Use the assigned IP address to access and log in to the Cisco IMC for the node. Consult with your DHCP server administrator to determine the IP address.

Note The default user name for the node is *admin*. The default password is *password*.

Step 5 From the Cisco IMC node Summary page, click **Launch KVM Console**. A separate KVM console window opens.

Step 6 From the Cisco IMC Summary page, click **Power Cycle**. The node reboots.

Step 7 Select the KVM console window.

Note The KVM console window must be the active window for the following keyboard actions to work.

Step 8 When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.

This utility has two windows that you can switch between by pressing F1 or F2.

Step 9 Continue with Cisco IMC Configuration Utility Setup, page 2-12.

Cisco IMC Configuration Utility Setup

The following procedure is performed after you connect to the node and open the Cisco IMC Configuration Utility.

Step 1 Set NIC mode and NIC redundancy:

a. Set the NIC mode to choose which ports to use to access Cisco IMC for node management (see Figure 1-2 for identification of the ports):

- Shared LOM EXT (default)—This is the shared LOM extended mode, the factory-default setting. With this mode, the Shared LOM and Cisco Card interfaces are both enabled.

  In this mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the node determines that the Cisco card connection is not getting its IP address from a Cisco UCS Manager node because the node is in standalone mode, further DHCP requests from the Cisco card are disabled. Use the Cisco Card NIC mode if you want to connect to Cisco IMC through a Cisco card in standalone mode.
- Shared LOM—The 1-Gb Ethernet ports are used to access Cisco IMC. You must select a NIC redundancy and IP setting.
- Dedicated—The dedicated management port is used to access Cisco IMC. You must select a NIC redundancy and IP setting.
- Cisco Card—The ports on an installed Cisco UCS virtual interface card (VIC) are used to access the Cisco IMC. You must select a NIC redundancy and IP setting.

  See also the required VIC Slot setting below.
- VIC Slot—If you use the Cisco Card NIC mode, you must select this setting to match where your VIC is installed. The choices are Riser1, Riser2, or Flex-LOM (the mLOM slot).
  - If you select Riser1, slot 1 is used.
  - If you select Riser2, slot 2 is used.
  - If you select Flex-LOM, you must use an mLOM-style VIC in the mLOM slot.

b. Use this utility to change the NIC redundancy to your preference. This node has three possible NIC redundancy settings:

- None—The Ethernet ports operate independently and do not fail over if there is a problem. This setting can be used only with the Dedicated NIC mode.
- Active-standby—If an active Ethernet port fails, traffic fails over to a standby port.
- Active-active—All Ethernet ports are utilized simultaneously. The Shared LOM EXT mode can have only this NIC redundancy setting. Shared LOM and Cisco Card modes can have both Active-standby and Active-active settings.

Step 2 Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.

Note Before you enable DHCP, you must preconfigure your DHCP node with the range of MAC addresses for this node. The MAC address is printed on a label on the rear of the node. This node has a range of six MAC addresses assigned to Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

The static IPv4 and IPv6 settings include the following:

- The Cisco IMC IP address.
- The prefix/subnet.

  For IPv6, valid values are 1–127.
- The gateway.

  For IPv6, if you do not know the gateway, you can set it as none by entering **::** (two colons).
- The preferred DNS node address.

  For IPv6, you can set this as none by entering **::** (two colons).

Step 3 (Optional) Use this utility to make VLAN settings.

Step 4 Press **F1** to go to the second settings window, then continue with the next step.

From the second window, you can press **F2** to switch back to the first window.

Step 5 (Optional) Set a hostname for the node.

Step 6 (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 7 (Optional) If you check the Factory Default check box, the node reverts to the factory defaults.

Step 8 (Optional) Set a default user password.

Step 9 (Optional) Enable auto-negotiation of port settings or set the port speed and duplex mode manually.

Note Auto-negotiation is applicable only when you use the Dedicated NIC mode. Auto-negotiation sets the port speed and duplex mode automatically based on the switch port to which the node is connected. If you disable auto-negotiation, you must set the port speed and duplex mode manually.

Step 10 (Optional) Reset port profiles and the port name.

Step 11 Press **F5** to refresh the settings that you made. You might have to wait about 45 seconds until the new settings appear and the message, “Network settings configured” is displayed before you reboot the node in the next step.

Step 12 Press **F10** to save your settings and reboot the node.

Note If you chose to enable DHCP, the dynamically assigned IP and MAC addresses are displayed on the console screen during bootup.

Use a browser and the IP address of the Cisco IMC to connect to the Cisco IMC management interface. The IP address is based upon the settings that you made (either a static address or the address assigned by your DHCP node).

Note The default username for the node is *admin*. The default password is *password*.

To manage the node, see the *Cisco UCS C-Series Rack-Mount Server Configuration Guide* or the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide* for instructions on using those interfaces. The links to these documents are in the C-Series documentation roadmap:

http://www.cisco.com/go/unifiedcomputing/c-series-doc

NIC Modes and NIC Redundancy Settings

NIC Modes

This node has the following NIC mode settings that you can choose from:

- Shared LOM EXT (default)—This is the Shared LOM extended mode, the factory-default setting. With this mode, the shared LOM and Cisco Card interfaces are both enabled.

  In this mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the node determines that the Cisco card connection is not getting its IP address from a Cisco UCS Manager node because the node is in standalone mode, further DHCP requests from the Cisco card are disabled. If the node determines that the Cisco card connection is getting its IP address from a Cisco UCS Manager node, the reply has parameters that automatically move the node to UCSM mode.
- Dedicated—The dedicated management port is used to access Cisco IMC. You must select a NIC redundancy and IP setting.
- Shared LOM—The 1-Gb Ethernet ports are used to access Cisco IMC. You must select a NIC redundancy and IP setting.
- Cisco Card—The ports on an installed Cisco UCS virtual interface card (VIC) are used to access Cisco IMC. You must select a NIC redundancy and IP setting.

  See also the required VIC Slot setting below.
- VIC Slot—If you use the Cisco Card NIC mode, you select this setting to match where your VIC is installed. The choices are Riser1, Riser2, or Flex-LOM (the mLOM slot).
  - If you select Riser1, slot 1 is used.
  - If you select Riser2, slot 2 is used.
  - If you select Flex-LOM, you must use an mLOM-style VIC in the mLOM slot.

NIC Redundancy

This node has the following NIC redundancy settings that you can choose from:

- None—The Ethernet ports operate independently and do not fail over if there is a problem. This setting can be used only with the Dedicated NIC mode.
- Active-standby—If an active Ethernet port fails, traffic fails over to a standby port.
- Active-active—All Ethernet ports are utilized simultaneously. Shared LOM EXT mode can have only this NIC redundancy setting. Shared LOM and Cisco Card modes can have both Active-standby and Active-active settings.

  The active/active setting uses Mode 5 or Balance-TLB (adaptive transmit load balancing). This is channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

Node BIOS and Cisco IMC Firmware

This section includes information about the node BIOS and it includes the following sections:

Updating the BIOS and Cisco IMC Firmware

Caution When you upgrade the BIOS firmware, you must also upgrade the Cisco IMC firmware to the same version or the node does not boot. Do not power off the node until the BIOS and Cisco IMC firmware are matching or the node does not boot.

Cisco provides the Cisco Host Upgrade Utility to assist with simultaneously upgrading the BIOS, Cisco IMC, and other firmware to compatible levels.

The node uses firmware obtained from and certified by Cisco. Cisco provides release notes with each firmware image. There are several methods for updating the firmware:

- **Recommended method for node components firmware update**: Use the Cisco Host Upgrade Utility to simultaneously upgrade the Cisco IMC, BIOS, LOM, LSI storage controller, and Cisco UCS VIC firmware to compatible levels.

  See the *Cisco Host Upgrade Utility Quick Reference Guide* for your firmware level at the documentation roadmap link below.
- You can upgrade the BIOS using the EFI interface, or upgrade from a Windows or Linux platform.

  See the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*.
- You can upgrade the Cisco IMC and BIOS firmware by using the Cisco IMC GUI interface.

  See the *Cisco UCS C-Series Rack-Mount Server Configuration Guide.*
- You can upgrade the Cisco IMC and BIOS firmware by using the Cisco IMC CLI interface.

  See the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide.*

For links to the documents listed above, see the documentation roadmap at the following URL:
http://www.cisco.com/go/unifiedcomputing/c-series-doc

Accessing the Node BIOS

Step 1 Enter the BIOS setup utility by pressing the **F2** key when prompted during bootup.

Note The version and build of the current BIOS are displayed on the Main page of the utility.

Step 2 Use the arrow keys to select the BIOS menu page.

Step 3 Highlight the field to be modified by using the arrow keys.

Step 4 Press **Enter** to select the field that you want to change, and then modify the value in the field.

Step 5 Press the right arrow key until the Exit menu screen is displayed.

Step 6 Follow the instructions on the Exit menu screen to save your changes and exit the setup utility (or Press **F10**). You can exit without saving changes by pressing **Esc**.

CHAPTER 3

Maintaining the Node

This chapter describes how to diagnose node problems using LEDs. It also provides information about how to install or replace hardware components, and it includes the following sections:

Node Monitoring and Management Tools

Cisco Integrated Management Interface

You can monitor the node inventory, health, and system event logs by using the built-in Cisco Integrated Management Controller (Cisco IMC) GUI or CLI interfaces. See the user documentation for your firmware release at the following URL:

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

Server Configuration Utility

Cisco has also developed the Cisco Server Configuration Utility, which can aid and simplify the following tasks:

- Monitoring system inventory and health
- Diagnosing common system problems with diagnostic tools and logs
- Setting the BIOS booting order
- Configuring some RAID configurations
- Installing operating systems

You can download the ISO image from Cisco.com. See the user documentation for your version of the utility at the following URL:

http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

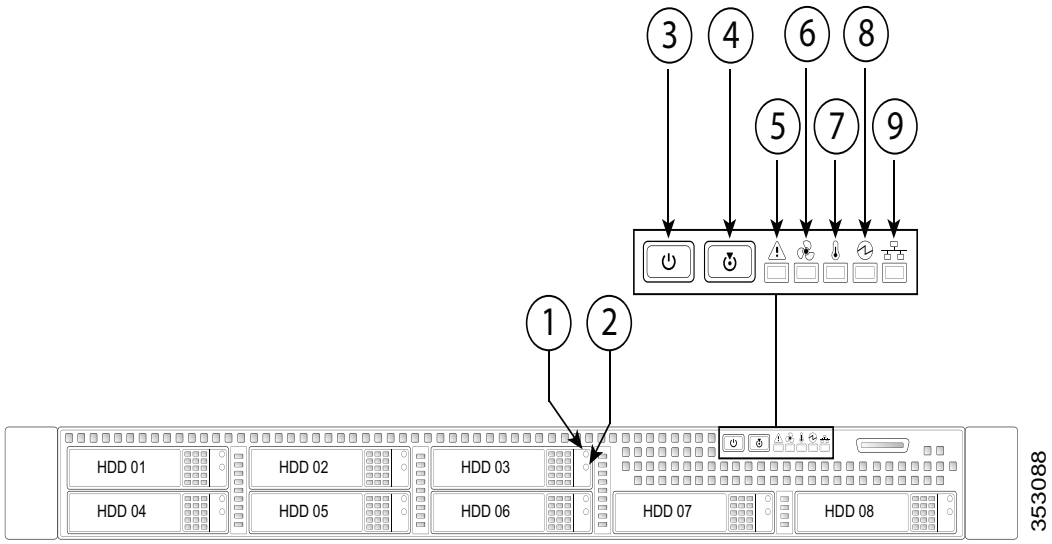
Status LEDs and Buttons

This section describes the location and meaning of LEDs and buttons and includes the following topics

Front Panel LEDs

Figure 3-1 shows the front panel LEDs. Table 3-1 defines the LED states.

Figure 3-1 Front Panel LEDs



1	Hard drive fault LED **Note:** NVMe PCIe SSDs drive tray LEDs have slightly different behavior. See Table 3-1 for the LED states.	**6**	Fan status LED
2	Hard drive activity LED	**7**	Temperature status LED
3	Power button/power status LED	**8**	Power supply status LED
4	Identification button/LED	**9**	Network link activity LED
5	Node status LED		

Table 3-1 Front Panel LEDs, Definitions of States

	LED Name	State
1 **SAS**	SAS/SATA drive fault	• Off—The hard drive is operating properly. • Amber—Drive fault detected. • Amber, blinking—The device is rebuilding. • Amber, blinking with one-second interval—Drive locate function activated.
2 **SAS**	SAS/SATA drive activity	• Off—There is no hard drive in the hard drive tray (no access, no fault). • Green—The hard drive is ready. • Green, blinking—The hard drive is reading or writing data.
1 **PCIe**	NVMe PCIe SSD status (SFF, 8-drives version only)	• Off—The drive is not in use and can be safely removed. • Green—The drive is in use and functioning properly. • Green, blinking—the driver is initializing following insertion or the driver is unloading following an eject command. • Amber—The drive has failed. • Amber, blinking—A drive Locate command has been issued in the software.
2 **PCIe**	NVMe PCIe SSD activity (SFF, 8-drives version only)	• Off—No drive activity. • Green, blinking—There is drive activity.
3	Power button/LED	• Off—There is no AC power to the node. • Amber—The node is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions. • Green—The node is in main power mode. Power is supplied to all node components.
4	Unit identification	• Off—The unit identification function is not in use. • Blue—The unit identification function is activated.
5	Node status	• Green—The node is running in normal operating condition. • Green, blinking—The node is performing node initialization and memory check. • Amber, steady—The node is in a degraded operational state. For example: – Power supply redundancy is lost. – CPUs are mismatched. – At least one CPU is faulty. – At least one DIMM is faulty. – At least one drive in a RAID configuration failed. • Amber, blinking—The node is in a critical fault state. For example: – Boot failed. – Fatal CPU and/or bus error is detected. – node is in an over-temperature condition.

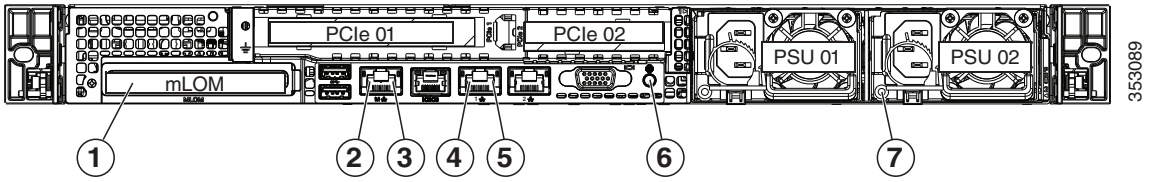
Table 3-1 Front Panel LEDs, Definitions of States (continued)

	LED Name	State
6	Fan status	• Green—All fan modules are operating properly. • Amber, steady—One or more fan modules breached the critical threshold. • Amber, blinking—One or more fan modules breached the non-recoverable threshold.
7	Temperature status	• Green—The node is operating at normal temperature. • Amber, steady—One or more temperature sensors breached the critical threshold. • Amber, blinking—One or more temperature sensors breached the non-recoverable threshold.
8	Power supply status	• Green—All power supplies are operating normally. • Amber, steady—One or more power supplies are in a degraded operational state. • Amber, blinking—One or more power supplies are in a critical fault state.
9	Network link activity	• Off—The Ethernet link is idle. • Green—One or more Ethernet LOM ports are link-active, but there is no activity. • Green, blinking—One or more Ethernet LOM ports are link-active, with activity.

Rear Panel LEDs and Buttons

Figure 3-2 shows the rear panel LEDs and buttons. Table 3-2 defines the LED states.

Figure 3-2 Rear Panel LEDs and Buttons



1	Optional mLOM card LEDs (not shown, see Table 3-2)	**5**	1-Gb Ethernet link status LED
2	1-Gb Ethernet dedicated management link status LED	**6**	Rear unit identification button/LED
3	1-Gb Ethernet dedicated management link speed LED	**7**	Power supply status LED
4	1-Gb Ethernet link speed LED		

Table 3-2 Rear Panel LEDs, Definitions of States

	LED Name	State
1	Optional mLOM 10-Gb SFP+ (there is a single status LED)	• Off—No link is present. • Green, steady—Link is active. • Green, blinking—Traffic is present on the active link.
1	Optional mLOM 10-Gb BASE-T link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps/1 Gbps. • Green—Link speed is 10 Gbps.
1	Optional mLOM 10-Gb BASE-T link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
2	1-Gb Ethernet dedicated management link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
3	1-Gb Ethernet dedicated management link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
4	1-Gb Ethernet link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.

Table 3-2 Rear Panel LEDs, Definitions of States (continued)

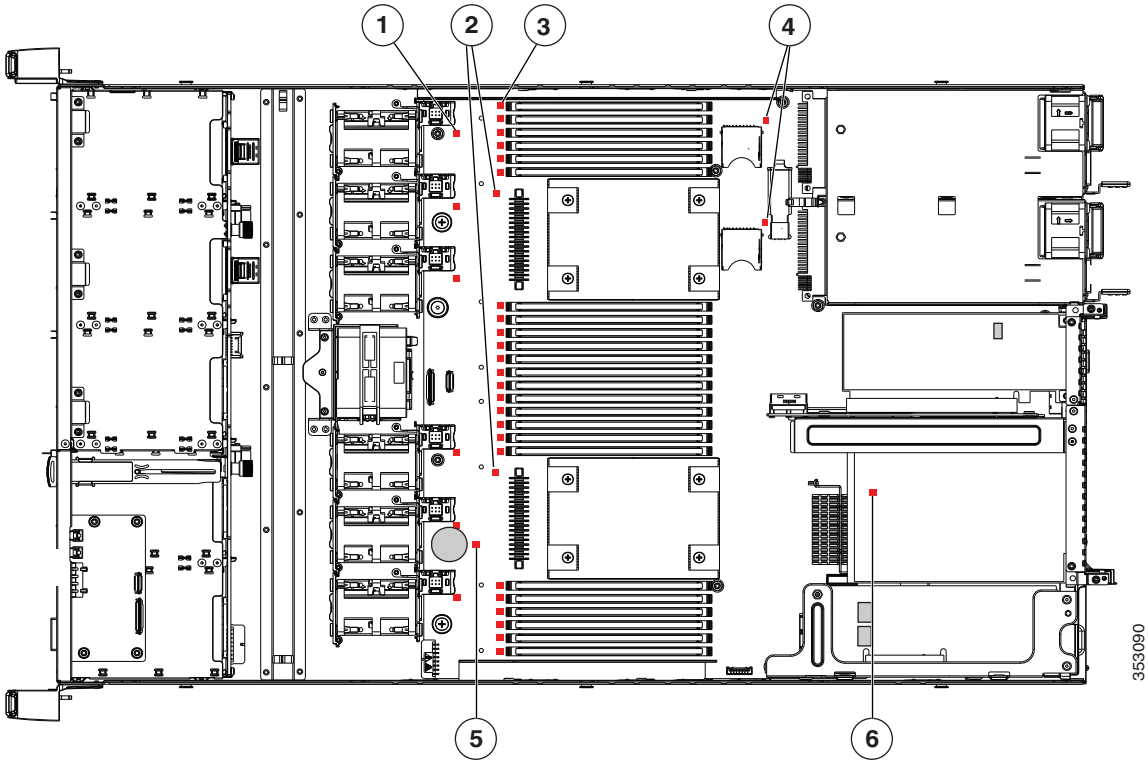
	LED Name	State
5	1-Gb Ethernet link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
6	Rear unit identification	• Off—The unit identification LED is not in use. • Blue—The unit identification LED is activated.
7	Power supply status	**AC power supplies:** • Off—No AC input (12 V main power off, 12 V standby power off). • Green, blinking—12 V main power off; 12 V standby power on. • Green, solid—12 V main power on; 12 V standby power on. • Amber, blinking—Warning threshold detected but 12 V main power on. • Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure). **DC power supply (UCSC-PSUV2-1050DC):** • Off—No DC input (12 V main power off, 12 V standby power off). • Green, blinking—12 V main power off; 12 V standby power on. • Green, solid—12 V main power on; 12 V standby power on. • Amber, blinking—Warning threshold detected but 12 V main power on. • Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure).

Internal Diagnostic LEDs

The node has internal fault LEDs for CPUs, DIMMs, fan modules, SD cards, the RTC battery, and the mLOM card. These LEDs are available only when the node is in standby power mode. An LED lights amber to indicate a faulty component.

See Figure 3-3 for the locations of these internal LEDs.

Figure 3-3 Internal Diagnostic LED Locations



1	Fan module fault LEDs (one next to each fan connector on the motherboard)	**4**	SD card fault LEDs (one next to each bay)
2	CPU fault LEDs (one in front of each CPU)	**5**	RTC battery fault LED
3	DIMM fault LEDs (one in front of each DIMM socket on the motherboard)	**6**	mLOM card fault LED (on motherboard next to mLOM socket)

Table 3-3 Internal Diagnostic LEDs, Definition of States

LED Name	State
Internal diagnostic LEDs (all)	• Off—Component is functioning normally. • Amber—Component has failed.

Preparing for Node Component Installation

This section describes how to prepare for component installation, and it includes the following topics:

Required Equipment

The following equipment is used to perform the procedures in this chapter:

- Number 2 Phillips-head screwdriver
- Electrostatic discharge (ESD) strap or other grounding equipment such as a grounded mat

Shutting Down and Powering Off the Node

The node can run in two power modes:

- Main power mode—Power is supplied to all node components and any operating system on your drives can run.
- Standby power mode—Power is supplied only to the service processor and the cooling fans and it is safe to power off the node from this mode.

You can invoke a graceful shutdown or a hard shutdown by using either of the following methods:

- Use the Cisco IMC management interface.
- Use the **Power** button on the node front panel. To use the **Power** button, follow these steps:

Step 1 Check the color of the Power Status LED (see the "Front Panel LEDs" section on page 3-2).

- Green—The node is in main power mode and must be shut down before it can be safely powered off. Go to Step 2.
- Amber—The node is already in standby mode and can be safely powered off. Go to Step 3.

Step 2 Invoke either a graceful shutdown or a hard shutdown:

Caution To avoid data loss or damage to your operating node, you should always invoke a graceful shutdown of the operating system.

- Graceful shutdown—Press and release the **Power** button. The operating system performs a graceful shutdown and the node goes to standby mode, which is indicated by an amber Power Status LED.
- Emergency shutdown—Press and hold the **Power** button for 4 seconds to force the main power off and immediately enter standby mode.

Step 3 Disconnect the power cords from the power supplies in your node to completely power off the node.

Removing and Replacing the Node Top Cover

Step 1 Remove the top cover (see Figure 3-4).

a. If the cover latch is locked, use a screwdriver to turn the lock 90-degrees counterclockwise to unlock it. See Figure 3-4.

b. Lift on the end of the latch that has the green finger grip. The cover is pushed back to the open position as you lift the latch.

c. Lift the top cover straight up from the node and set it aside.

Step 2 Replace the top cover:

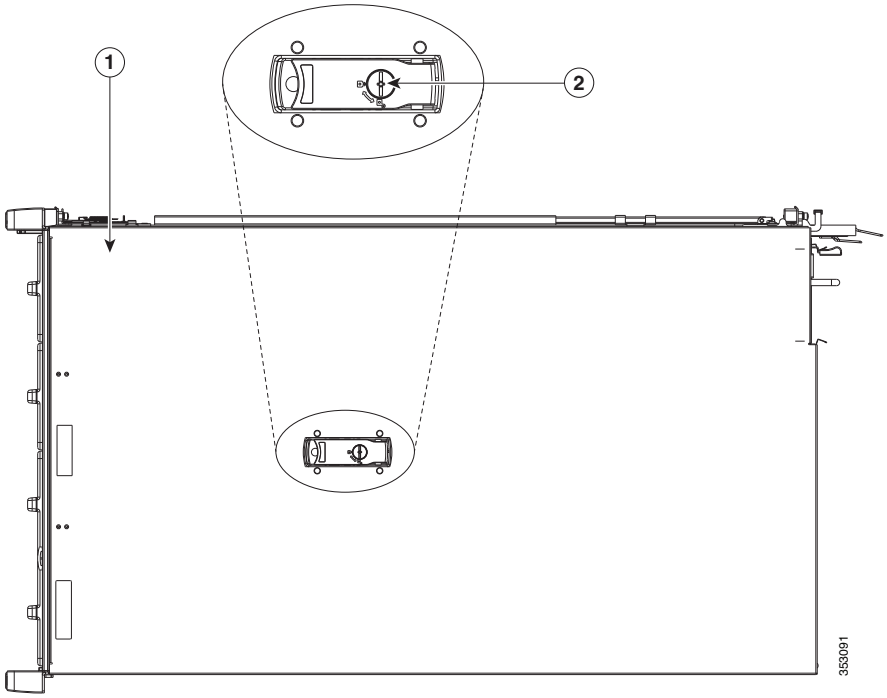
Note The latch must be in the fully open position when you set the cover back in place, which allows the opening in the latch to sit over a peg that is on the fan tray.

a. With the latch in the fully open position, place the cover on top of the node about one-half inch (1.27 cm) behind the lip of the front cover panel. The opening in the latch should fit over the peg that sticks up from the fan tray.

b. Press the cover latch down to the closed position. The cover is pushed forward to the closed position as you push down the latch.

c. If desired, lock the latch by using a screwdriver to turn the lock 90-degrees clockwise.

Figure 3-4 Removing the Top Cover



1	Top cover	**2**	Locking cover latch

Serial Number Location

The serial number for the node is printed on a label on the top of the node, near the front.

Hot-Swap or Hot-Plug Replacement

Some components can be removed and replaced without powering off and removing AC power from the node. This type of replacement has two varieties: hot-swap and hot-plug.

- Hot-swap replacement—You do not have to precondition or shut down the component in the software before you remove it for the following components:
  - SAS/SATA drives
  - Cooling fan modules
  - Power supplies (when 1+1 redundant)
- Hot-plug replacement—You must take the component offline before removing it for the following component:
  - NVMe PCIE SSD drives

Installing or Replacing Node Components

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the node unless all cards, faceplates, front covers, and rear covers are in place.**
Statement 1029

Caution When handling node components, wear an ESD strap to avoid damage.

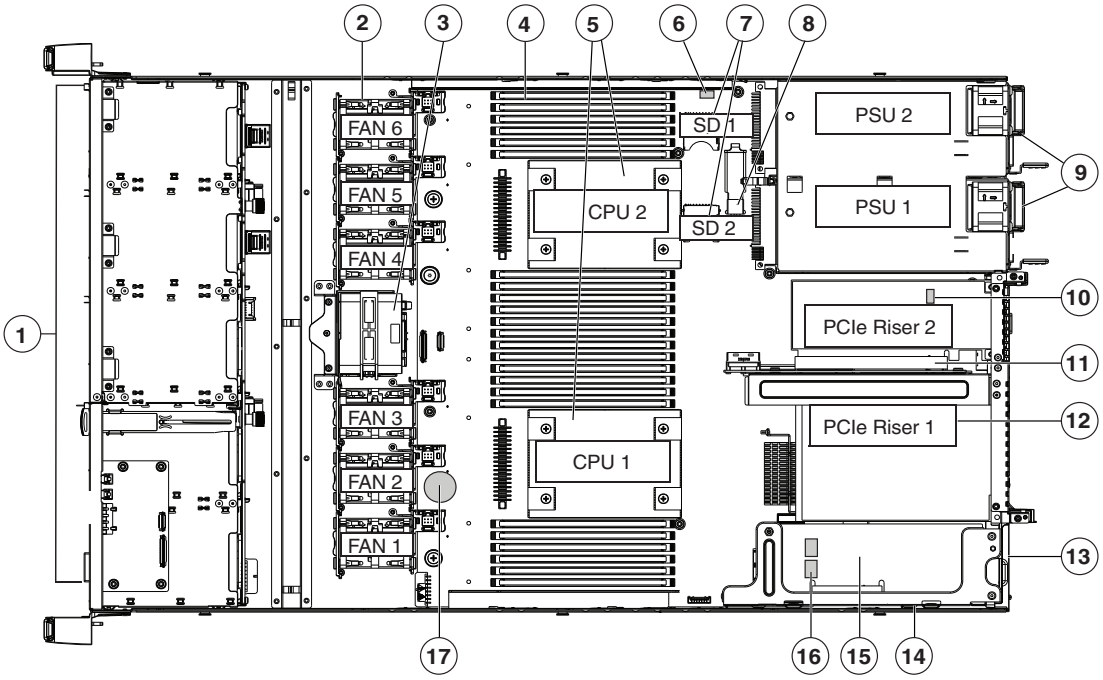
Tip You can press the unit identification button on the front panel or rear panel to turn on a flashing unit identification LED on the front and rear panels of the node. This button allows you to locate the specific node that you are servicing when you go to the opposite side of the rack. You can also activate these LEDs remotely by using the Cisco IMC interface. See the "Status LEDs and Buttons" section on page 3-2 for locations of these LEDs.

This section describes how to install and replace node components, and it includes the following topics:

Replaceable Component Locations

This section shows the locations of the field-replaceable components. The view in Figure 3-5 is from the top down with the top cover and air baffle removed.

Figure 3-5 Replaceable Component Locations



1	Drive bays 1–8 support SAS/SATA drives. SFF, 8-drive version only: Drive bays 1 and 2 support SAS/SATA and NVMe PCIe SSDs. NVMe SSDs require PCIe riser version 2B in the node to provide the PCIe bus connection.	**10**	Trusted platform module (TPM) socket on motherboard (not visible in this view)
2	Cooling fan modules (six)	**11**	PCIe riser 2 (half-height PCIe slot 2)
3	Supercap Power Module (RAID backup) mounting bracket	**12**	PCIe riser 1 (full-height PCIe slot 1)
4	DIMM sockets on motherboard (24)	**13**	Modular LOM (mLOM) connector on chassis floor
5	CPUs and heatsinks (up to two)	**14**	Cisco modular RAID controller PCIe riser (dedicated riser with horizontal socket)
6	Embedded SATA RAID header for RAID 5 key	**15**	Cisco modular RAID controller card
7	SD card bays on motherboard (two)	**16**	Embedded SATA RAID mini-SAS connectors on motherboard (not visible in this view)
8	Internal USB 3.0 port on motherboard	**17**	RTC battery on motherboard
9	Power supplies (up to two, hot-swappable when redundant as 1+1)		

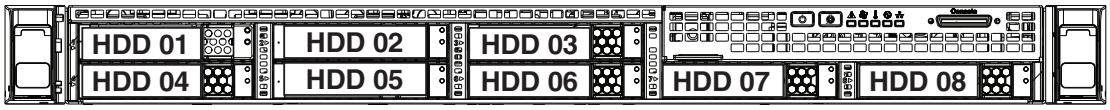
Replacing Hard Drives or Solid State Drives

This section includes the following information:

Drive Population Guidelines

The drive-bay numbering is shown in Figure 3-6.

Figure 3-6 Drive Numbering, SFF Drives, Eight-Drive Version



Observe these drive population guidelines for optimum performance:

- When populating drives, add drives to the lowest-numbered bays first.
- SFF, 8-drive version only: Populate NVMe PCIe SSDs only in bays 1 and 2.
- Keep an empty drive blanking tray in any unused bays to ensure proper airflow.
- You can mix SAS/SATA hard drives and SAS/SATA SSDs in the same node (the LFF version of the node does not support SSDs). However, you cannot configure a logical volume (virtual drive) that contains a mix of hard drives and SSDs. That is, when you create a logical volume, it must contain all SAS/SATA hard drives or all SAS/SATA SSDs.

Replacing a SAS/SATA Drive

Note You do not have to shut down the node or drive to replace SAS/SATA hard drives or SSDs because they are hot-swappable. To replace an NVMe PCIe SSD drive, which must be shut down before removal, see Replacing an NVMe PCIe SSD, page 3-15.

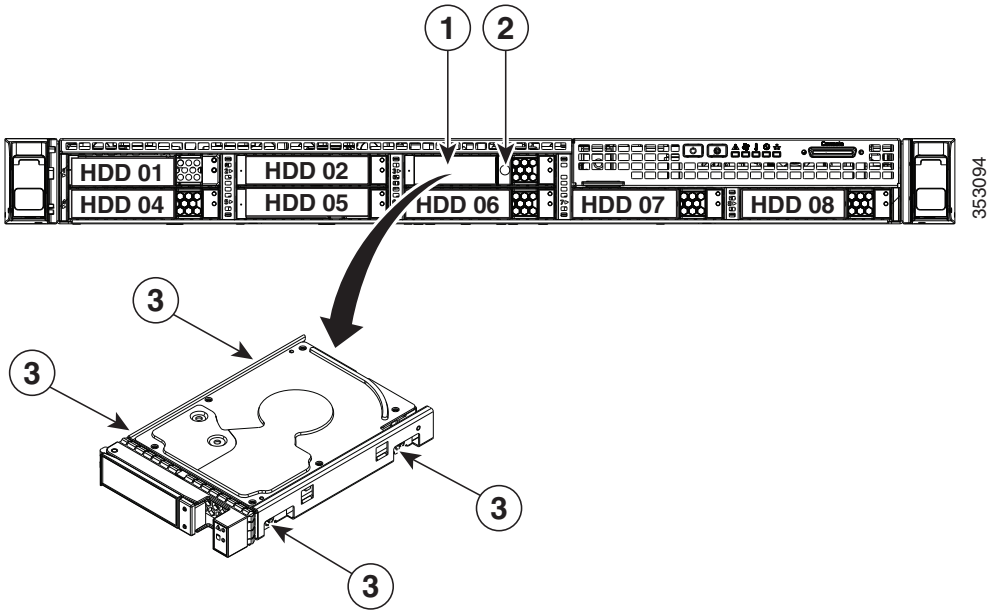
Step 1 Remove the drive that you are replacing or remove a blank drive tray from the bay:

- **a.** Press the release button on the face of the drive tray. See Figure 3-7.
- **b.** Grasp and open the ejector lever and then pull the drive tray out of the slot.
- **c.** If you are replacing an existing drive, remove the four drive-tray screws that secure the drive to the tray and then lift the drive out of the tray.

Step 2 Install a new drive:

- **a.** Place a new drive in the empty drive tray and install the four drive-tray screws.
- **b.** With the ejector lever on the drive tray open, insert the drive tray into the empty drive bay.
- **c.** Push the tray into the slot until it touches the backplane, and then close the ejector lever to lock the drive in place.

Figure 3-7 Replacing Hard Drives



1	Ejector lever	**3**	Drive tray securing screws (4)
2	Release button		–

Replacing an NVMe PCIe SSD

Observe these requirements for NVMe PCIe SSDs:

- The SFF, 8-drives version of the node.
- PCIe riser version 2B (UCSC-PCI-2B-220M4), with bundled cables. This version of the riser has cable connectors for the PCIe cables that connect to the drive backplane.

Observe these restrictions for NVMe PCIe SSDs:

- You cannot boot from an NVMe PCIe SSD.
- You cannot control an NVMe PCIe SSD with a SAS RAID controller because they communicate with the node via the PCIe bus.

Caution NVMe PCIe SSDs are hot-pluggable, which means that you must shut down the drive before removal, but you do not have to fully power off the node. To replace a SAS/SATA drive, see Replacing a SAS/SATA Drive, page 3-14.

For information about drive tray LEDs, see Front Panel LEDs, page 3-2.

Step 1 Remove an existing NVMe PCIe SSD:

a. Shut down the NVMe PCIe SSD. Use your operating system interface to shut down the drive, and then observe the drive-tray LED:
   - Green—The drive is in use and functioning properly. Do not remove.
   - Green, blinking—the driver is unloading following a shutdown command. Do not remove.
   - Off—The drive is not in use and can be safely removed.

b. Press the release button on the face of the drive tray. See Figure 3-7.

c. Grasp and open the ejector lever and then pull the drive tray out of the slot.

d. If you are replacing an existing SSD, remove the four drive tray screws that secure the SSD to the tray and then lift the SSD out of the tray.

Note If this is the first time that NVMe PCIe SSDs are being installed in the node, you must install PCIe riser version 2B and connect its cables before installing the drive. See Installing PCIe Riser Version 2B, page 3-16.

Step 2 Install a new NVMe PCIe SSD:

a. Place a new SSD in the empty drive tray and replace the four drive tray screws.

b. With the ejector lever on the drive tray open, insert the drive tray into the empty drive bay.

c. Push the tray into the slot until it touches the backplane, and then close the ejector lever to lock the drive in place.

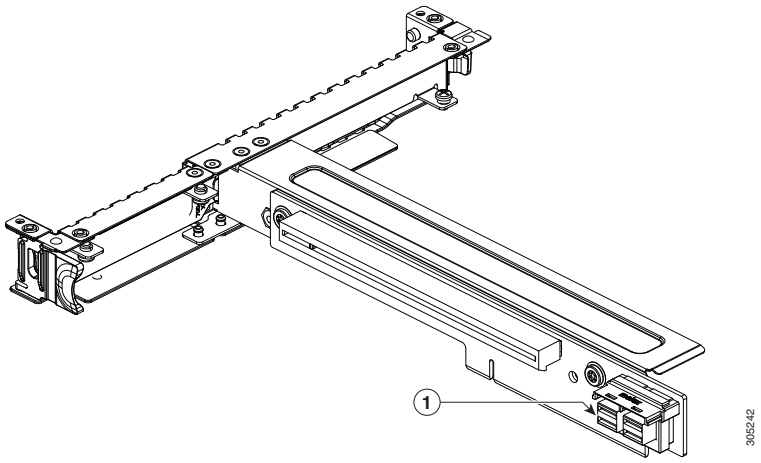
Step 3 Observe the drive-tray LED and wait until it returns to solid green before accessing the drive:

- Off—The drive is not in use.
- Green, blinking—the driver is initializing following hot-plug insertion.
- Green—The drive is in use and functioning properly.

Installing PCIe Riser Version 2B

PCIe Riser Version 2B (UCSC-PCI-2B-220M4) has two cable connectors that are used to provide communication with the PCIe bus from the NVMe PCIe SSDs in the front panel bays.

Figure 3-8 PCIe Riser Assembly UCSC-PCI-2B-C220M4



1	Connectors for PCIe cables		

Step 1 Remove an existing PCIe riser assembly that you are replacing:

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

d. Use two hands to grasp the metal bracket of the riser assembly and lift straight up to disengage its connectors from the two sockets on the motherboard.

e. If the riser has any cards installed, remove them from the riser.

Step 2 Install a new PCIe riser assembly Version 2B:

a. If you removed any cards from the old riser assembly, install the cards to the new riser assembly (see Replacing a PCIe Card, page 3-42).

b. Position the riser assembly over its two sockets on the motherboard and over the chassis alignment channels (see Figure 3-23):

c. Carefully push down on both ends of the riser assembly to fully engage its connectors with the two sockets on the motherboard.

Step 3 Connect the two cables that come with UCSC-PCI-2B-220M4:

a. Connect both cable connectors to the two connectors on the riser 2B (see Figure 3-9).

b. Route the cables to the front of the node using the recommended path through the chassis cable guides as shown in Figure 3-9.

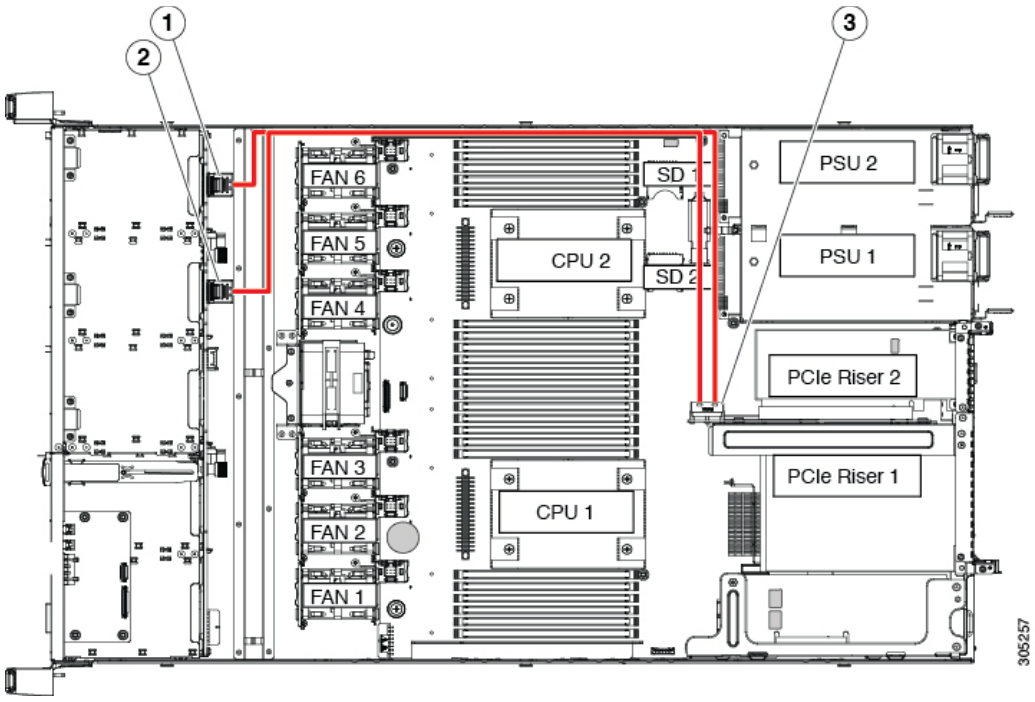
c. Connect the two ends of the cable to the PCIe connectors on the drive backplane.

   Connect the cable labeled Port A to the Port A connector; connect the cable labeled Port B to the Port B connector (see Figure 3-9).

Step 4 Replace the top cover.

Step 5 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-9 PCIe Riser Version 2B Cabling to Drive Backplane



1	PCIe connector, Port A	**3**	Cable connector on PCIe riser 2B (UCSC-PCI-2B-220M4)
2	PCIe connector, Port B		

Replacing Fan Modules

The six fan modules in the node are numbered as follows when you are facing the front of the node (also see Figure 3-11).

Figure 3-10 Fan Module Numbering

FAN 6	FAN 5	FAN 4	FAN 3	FAN 2	FAN 1

Tip Each fan module has a fault LED next to the fan connector on the motherboard that lights amber if the fan module fails. Standby power is required to operate these LEDs.

Caution You do not have to shut down or power off the node to replace fan modules because they are hot-swappable. However, to maintain proper cooling, do not operate the node for more than one minute with any fan module removed.

Step 1 Remove a fan module that you are replacing (see Figure 3-11):

a. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

b. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

c. Grasp the fan module at its front and on the green connector. Lift straight up to disengage its connector from the motherboard and free it from the two alignment pegs.

Step 2 Install a new fan module:

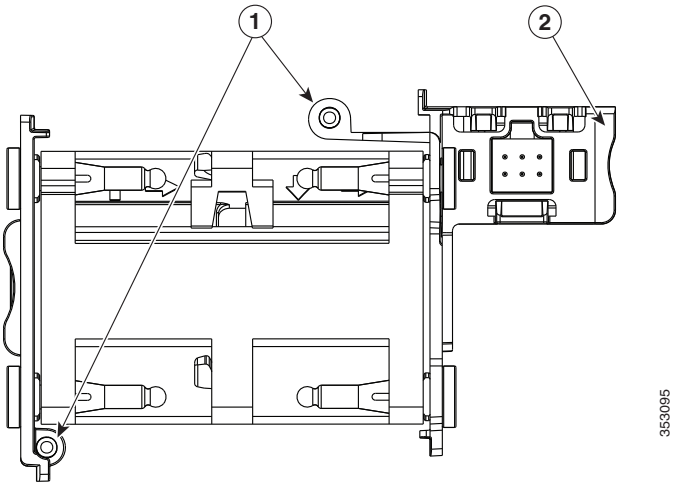
a. Set the new fan module in place, aligning its two openings with the two alignment pegs on the motherboard. See Figure 3-11.

b. Press down gently on the fan module connector to fully engage it with the connector on the motherboard.

c. Replace the top cover.

d. Replace the node in the rack.

Figure 3-11 Top View of Fan Module



1	Openings in fan module for motherboard alignment pegs	**2**	Fan connector to motherboard

Replacing the Motherboard RTC Battery

Warning **There is danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** [Statement 1015]

The real-time clock (RTC) battery retains node settings when the node is disconnected from power. The battery type is CR2032. Cisco supports the industry-standard CR2032 battery, which can be purchased from most electronic stores.

Step 1 Remove the RTC battery (see Figure 3-12):

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

d. Locate the RTC battery. See Figure 3-12.

e. Gently remove the battery from the holder on the motherboard.

Step 2 Install an RTC battery:

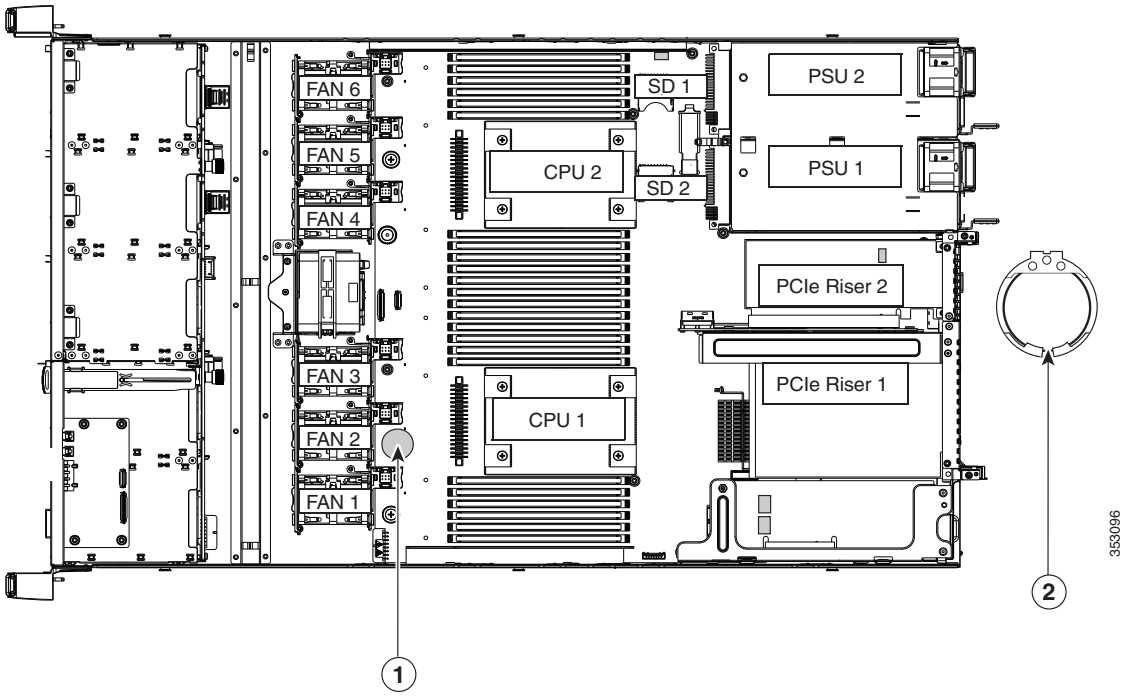
a. Insert the battery into its holder and press down until it clicks in place.

Note The positive side of the battery marked "3V+" should face upward.

b. Replace the top cover.

c. Replace the node in the rack, replace cables, and power on the node by pressing the **Power** button.

Figure 3-12 Motherboard RTC Battery Location



1	RTC battery holder on motherboard	**2**	Prying point on battery in holder

Replacing DIMMs

This section includes the following topics:

Caution DIMMs and their sockets are fragile and must be handled with care to avoid damage during installation.

Caution Cisco does not support third-party DIMMs. Using non-Cisco DIMMs in the node might result in node problems or damage to the motherboard.

Note To ensure the best node performance, it is important that you are familiar with memory performance guidelines and population rules before you install or replace DIMMs.

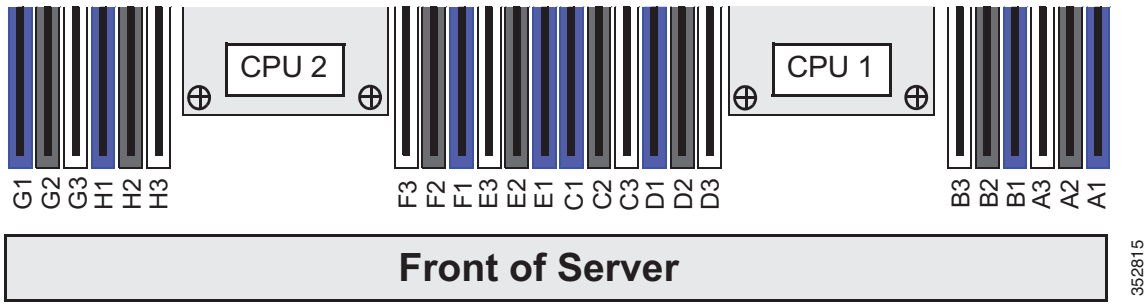
Memory Performance Guidelines and Population Rules

This section describes the type of memory that the node requires and its effect on performance. The section includes the following topics:

DIMM Slot Numbering

Figure 3-13 shows the numbering of the DIMM slots.

Figure 3-13 DIMM Slots and CPUs



DIMM Population Rules

Observe the following guidelines when installing or replacing DIMMs:

- Each CPU supports four memory channels.
  - CPU1 supports channels A, B, C, and D.
  - CPU2 supports channels E, F, G, and H.
- Each channel has three DIMM sockets (for example, channel A = slots A1, A2, and A3).
  - A channel can operate with one, two, or three DIMMs installed.
  - If a channel has only one DIMM, populate slot 1 first (the blue slot).
- When both CPUs are installed, populate the DIMM sockets of each CPU identically.
  - Fill blue #1 slots in the channels first: A1, E1, B1, F1, C1, G1, D1, H1
  - Fill black #2 slots in the channels second: A2, E2, B2, F2, C2, G2, D2, H2
  - Fill white #3 slots in the channels third: A3, E3, B3, F3, C3, G3, D3, H3
- Any DIMM installed in a DIMM socket for which the CPU is absent is not recognized. In a single-CPU configuration, populate the channels for CPU1 only (A, B, C, D).
- Memory mirroring reduces the amount of memory available by 50 percent because only one of the two populated channels provides data. When memory mirroring is enabled, DIMMs must be installed in sets of 4, 6, or 8 as described in Memory Mirroring and RAS, page 3-24.
- Observe the DIMM mixing rules shown in Table 3-4.

Table 3-4 DIMM Mixing Rules for HX220c M4 Nodes

DIMM Parameter	DIMMs in the Same Channel	DIMMs in the Same Bank
DIMM Capacity: RDIMM = 8 or 16 GB LRDIMM = 32 or 64 GB	You can mix different capacity DIMMs in the same channel (for example, A1, A2, A3).	You can mix different capacity DIMMs in the same bank. However, for optimal performance DIMMs in the same bank (for example, A1, B1, C1, D1) should have the same capacity.
DIMM Speed: 2133 or 2400 MHz	You can mix speeds, but DIMMs will run at the speed of the slowest DIMMs/CPUs installed in the channel.	You can mix speeds, but DIMMs will run at the speed of the slowest DIMMs/CPUs installed in the bank.
DIMM Type: RDIMMs or LRDIMMs	You cannot mix DIMM types in a channel.	You cannot mix DIMM types in a bank.

Memory Mirroring and RAS

The Intel E5-2600 CPUs within the node support memory mirroring only when an even number of channels are populated with DIMMs. If one or three channels are populated with DIMMs, memory mirroring is automatically disabled. Furthermore, if memory mirroring is used, DRAM size is reduced by 50 percent for reasons of reliability.

Lockstep Channel Mode

When you enable lockstep channel mode, each memory access is a 128-bit data access that spans four channels.

Lockstep channel mode requires that all four memory channels on a CPU must be populated identically with regard to size and organization. DIMM socket populations within a channel (for example, A1, A2, A3) do not have to be identical but the same DIMM slot location across all four channels must be populated the same.

For example, DIMMs in sockets A1, B1, C1, and D1 must be identical. DIMMs in sockets A2, B2, C2, and D2 must be identical. However, the A1-B1-C1-D1 DIMMs do not have to be identical with the A2-B2-C2-D2 DIMMs.

DIMM Replacement Procedure

This section includes the following topics:

Identifying a Faulty DIMM

Each DIMM socket has a corresponding DIMM fault LED, directly in front of the DIMM socket. See Figure 3-3 for the locations of these LEDs. The LEDs light amber to indicate a faulty DIMM. To operate these LEDs from the supercap power source, remove AC power cords and then press the **unit identification** button. See also Internal Diagnostic LEDs, page 3-7.

Replacing DIMMs

Step 1 Remove the DIMM that you are replacing:

a. Power off the node as described in the Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

d. Identify the faulty DIMM by observing the DIMM slot fault LEDs on the motherboard.

e. Open the ejector levers at both ends of the DIMM slot, and then lift the DIMM out of the slot.

Step 2 Install a new DIMM:

Note Before installing DIMMs, see the population guidelines: Memory Performance Guidelines and Population Rules, page 3-22.

f. Align the new DIMM with the empty slot on the motherboard. Use the alignment key in the DIMM slot to correctly orient the DIMM.

g. Push down evenly on the top corners of the DIMM until it is fully seated and the ejector levers on both ends lock into place.

h. Replace the top cover.

i. Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Replacing CPUs and Heatsinks

This section contains the following topics:

CPU Configuration Rules

This node has two CPU sockets. Each CPU supports four DIMM channels (12 DIMM slots). See Figure 3-13.

CPU Replacement Procedure

Caution CPUs and their motherboard sockets are fragile and must be handled with care to avoid damaging pins during installation. The CPUs must be installed with heatsinks and their thermal pads to ensure proper cooling. Failure to install a CPU correctly might result in damage to the node.

Note This node uses the new independent loading mechanism (ILM) CPU sockets, so no Pick-and-Place tools are required for CPU handling or installation. Always grasp the plastic frame on the CPU when handling.

Step 1 Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

Step 2 Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

Step 3 Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 4 Remove the plastic air baffle that sits over the CPUs.

Step 5 Remove the heatsink that you are replacing. Use a Number 2 Phillips-head screwdriver to loosen the four captive screws that secure the heatsink and then lift it off of the CPU.

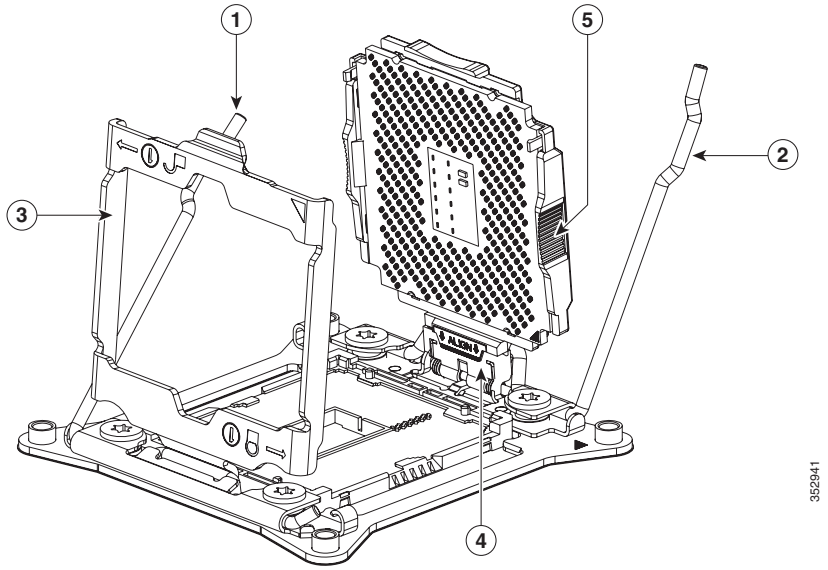
Note Alternate loosening each screw evenly to avoid damaging the heatsink or CPU.

Step 6 Open the CPU retaining mechanism:

a. Unclip the first retaining latch labeled with the icon, and then unclip the second retaining latch labeled with the icon. See Figure 3-14.

b. Open the hinged CPU cover plate.

Figure 3-14 CPU Socket



1	CPU retaining latch (unlocked)	**4**	Hinged CPU seat
2	CPU retaining latch (locked)	**5**	Finger grips on plastic CPU frame
3	Hinged CPU cover plate		

Step 7 Remove any existing CPU:

a. With the latches and hinged CPU cover plate open, swing up the CPU in its hinged seat to the open position, as shown in Figure 3-14.

b. Grasp the CPU by the finger grips on its plastic frame and lift it up and out of the hinged CPU seat.

c. Set the CPU aside on an anti-static surface.

Step 8 Install a new CPU:

a. Grasp the new CPU by the finger grips on its plastic frame and align the tab on the frame that is labeled “ALIGN” with the SLS mechanism, as shown in Figure 3-15.

b. Insert the tab on the CPU frame into the seat until it stops and is held firmly.

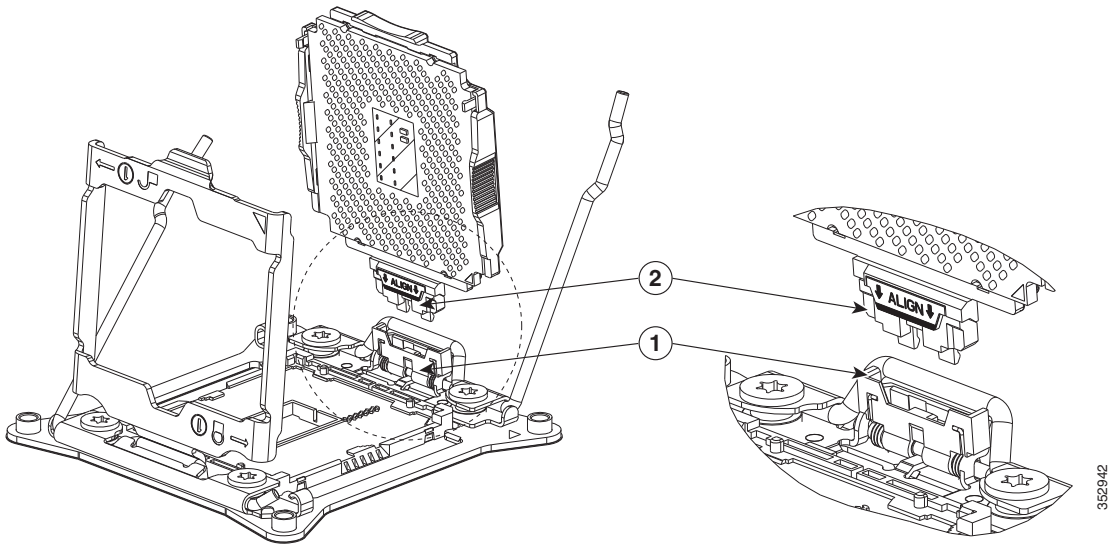
The line below the word “ALIGN” should be level with the edge of the seat, as shown in Figure 3-15.

c. Swing the hinged seat with the CPU down until the CPU frame clicks in place and holds flat in the socket.

d. Close the hinged CPU cover plate.

e. Clip down the CPU retaining latch with the (locked) icon, and then clip down the CPU retaining latch with the (unlocked) icon. See Figure 3-14.

Figure 3-15 CPU and Socket Alignment Features



1	SLS mechanism on socket	**2**	Tab on CPU frame (labeled ALIGN)

Step 9 Install a heat sink:

Caution The heat sink must have new thermal grease on the heat sink-to-CPU surface to ensure proper cooling. If you are reusing a heat sink, you must remove the old thermal grease from the heatsink and the CPU surface. If you are installing a new heat sink, skip to Step d.

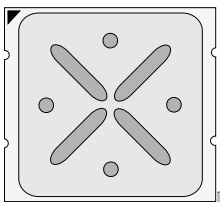
a. Apply the cleaning solution, which is included with the heatsink cleaning kit (UCSX-HSCK=, shipped with spare CPUs), to the old thermal grease on the heatsink and CPU and let it soak for a least 15 seconds.

b. Wipe all of the old thermal grease off the old heat sink and CPU using the soft cloth that is included with the heatsink cleaning kit. Be careful to not scratch the heat sink surface.

Note New heatsinks come with a pre-applied pad of thermal grease. If you are reusing a heatsink, you must apply thermal grease from a syringe (UCS-CPU-GREASE3=).

c. Using the syringe of thermal grease provided with the CPU (UCS-CPU-GREASE3=), apply 2 cubic centimeters of thermal grease to the top of the CPU. Use the pattern shown in Figure 3-16 to ensure even coverage.

Figure 3-16 Thermal Grease Application Pattern



d. Align the four heatsink captive screws with the motherboard standoffs, and then use a Number 2 Phillips-head screwdriver to tighten the captive screws evenly.

Note Alternate tightening each screw evenly to avoid damaging the heatsink or CPU.

Step 10 Replace the air baffle.

Step 11 Replace the top cover.

Step 12 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Additional CPU-Related Parts to Order with RMA Replacement Motherboards

When a return material authorization (RMA) of the motherboard or CPU is done on a node, additional parts might not be included with the CPU or motherboard spare bill of materials (BOM). The TAC engineer might need to add the additional parts to the RMA to help ensure a successful replacement.

- Scenario 1—You are reusing the existing heatsinks:
  - Heat sink cleaning kit (UCSX-HSCK=)
  - Thermal grease kit for C240 M4 (UCS-CPU-GREASE3=)
- Scenario 2—You are replacing the existing heatsinks:
  - Heat sink (UCSC-HS-C220M4=)
  - Heat sink cleaning kit (UCSX-HSCK=)

A CPU heatsink cleaning kit is good for up to four CPU and heatsink cleanings. The cleaning kit contains two bottles of solution, one to clean the CPU and heatsink of old thermal interface material and the other to prepare the surface of the heatsink.

New heatsink spares come with a pre-applied pad of thermal grease. It is important to clean the old thermal grease off of the CPU prior to installing the heatsinks. Therefore, when you are ordering new heatsinks, you must order the heatsink cleaning kit.

Replacing an Internal SD Card

The node has two internal SD card bays on the motherboard.

Dual SD cards are supported. RAID 1 support can be configured through the Cisco IMC interface.

Step 1 Remove the SD card that you are replacing:

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

d. Locate the SD card that you are replacing on the motherboard (see Figure 3-17).

e. Push on the top of the SD card, and then release it to allow it to spring up in the slot.

f. Remove the SD card from the slot.

Step 2 Install an SD card:

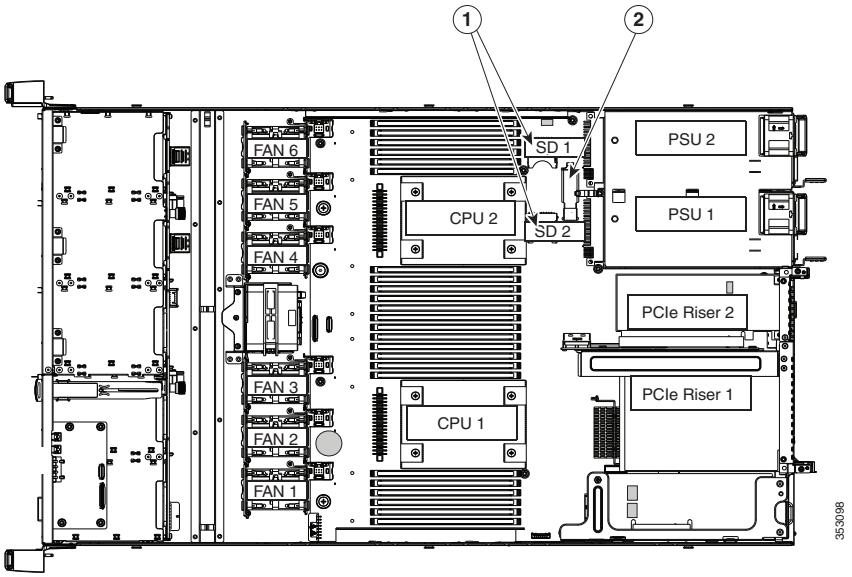
a. Insert the SD card into the slot with the label side facing up.

b. Press on the top of the card until it clicks in the slot and stays in place.

c. Replace the top cover.

Step 3 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-17 SD Card Bays and USB Port Locations on the Motherboard



1	SD card bays SD1 and SD2	**2**	USB 3.0 port

Enabling or Disabling the Internal USB Port

Caution We do not recommend that you hot-swap the internal USB drive while the node is powered on.

The factory default is for all USB ports on the node to be enabled. However, the internal USB port can be enabled or disabled in the node BIOS. See Figure 3-17 for the location of the USB port on the motherboard.

Step 1 Enter the BIOS Setup Utility by pressing the **F2** key when prompted during bootup.

Step 2 Navigate to the **Advanced** tab.

Step 3 On the Advanced tab, select **USB Configuration**.

Step 4 On the USB Configuration page, select **USB Ports Configuration**.

Step 5 Scroll to **USB Port: Internal**, press **Enter**, and then choose either **Enabled** or **Disabled** from the dialog box.

Step 6 Press **F10** to save and exit the utility.

Replacing a Cisco Modular RAID Controller Riser (Internal Riser 3)

The node has a dedicated internal riser (riser 3) that is only used for the Cisco modular RAID controller card. This riser plugs into a dedicated motherboard socket and provides a horizontal socket for the Cisco modular RAID controller card.

Step 1 Prepare the node for component installation:

- **a.** Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.
- **b.** Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

- **c.** Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 2 Remove the existing RAID controller riser (see Figure 3-18):

- **a.** If the existing riser has a card in it, disconnect the SAS cable from the card.
- **b.** Lift the riser straight up to disengage the riser from the motherboard socket. The riser bracket must also lift off of two pegs that hold it to the inner chassis wall.
- **c.** Set the riser upside down.
- **d.** Remove the card from the riser. Loosen the single thumbscrew that secures the card to the riser bracket and then pull the card straight out from its socket on the riser (see Figure 3-19).

Step 3 Install a new RAID controller riser:

- **a.** Install your RAID controller card into the new riser. See Replacing a Cisco Modular RAID Controller Card, page 3-33.

b. Align the connector on the riser with the socket on the motherboard. At the same time, align the two slots on the back side of the bracket with the two pegs on the inner chassis wall.

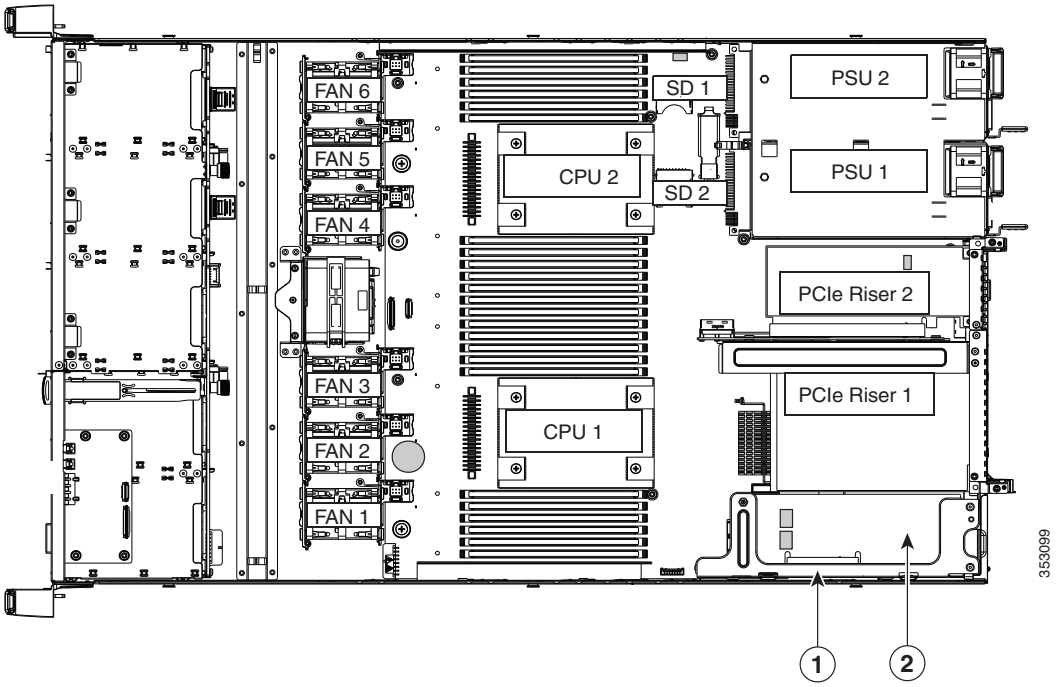
c. Push down gently to engage the riser connector with the motherboard socket. The metal riser bracket must also engage the two pegs that secure it to the chassis wall.

d. Reconnect the SAS cable to its connector on the RAID controller card.

Step 4 Replace the top cover.

Step 5 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-18 Cisco Modular RAID Controller Riser (Internal Riser 3) Location



1	Cisco modular RAID controller riser assembly (top of bracket)	**2**	Cisco modular RAID controller card in riser

Replacing a Cisco Modular RAID Controller Card

The node can use a Cisco modular RAID controller card that plugs into a horizontal socket on a dedicated internal riser (riser 3).

See also:

- Replacing a Modular RAID Controller Transportable Memory Module (TMM), page 3-35
- Replacing the Supercap Power Module (RAID Backup), page 3-38

Note You cannot use a hardware RAID controller card and the embedded RAID controller at the same time. See RAID Controller Considerations, page C-1 for details about RAID support.

RAID Card Firmware Compatibility

Firmware on the RAID controller must be verified for compatibility with the current Cisco IMC and BIOS versions that are installed on the node. If not compatible, upgrade or downgrade the RAID controller firmware accordingly using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring node components to compatible levels: HUU Guides

Replacement Procedure

Step 1 Prepare the node for component installation:

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 2 Remove the RAID controller riser from the node (see Figure 3-18):

a. Disconnect the SAS cable from the existing RAID controller card.

b. Lift the riser straight up to disengage the riser from the motherboard socket. The riser bracket must also lift off of two pegs that hold it to the inner chassis wall.

c. Set the riser upside down.

Step 3 Remove the card from the riser:

a. Loosen the single thumbscrew that secures the card to the metal riser bracket (see Figure 3-19).

b. Pull the card straight out from its socket on the riser and the guide channel on the riser bracket.

Step 4 Install the RAID controller card into the riser:

Caution Be careful when inserting the card to the riser so that you do not scrape electronic components on the underside of the card on features of the riser. The threaded standoff on the riser that is for the thumbscrew on the card might snag and damage the card components (see item 4 in Figure 3-19).

a. With the riser upside down, set the card on the riser. Align the right end of the card with the alignment channel on the riser; align the connector on the card edge with the socket on the riser (see Figure 3-19).

b. Being careful to avoid scraping the underside of the card on the threaded standoff on the riser, push on both corners of the card to seat its connector in the riser socket.

c. Tighten the single thumbscrew that secures the card to the riser bracket.

Step 5 Return the riser to the node:

a. Align the connector on the riser with the socket on the motherboard. At the same time, align the two slots on the back side of the bracket with the two pegs on the inner chassis wall.

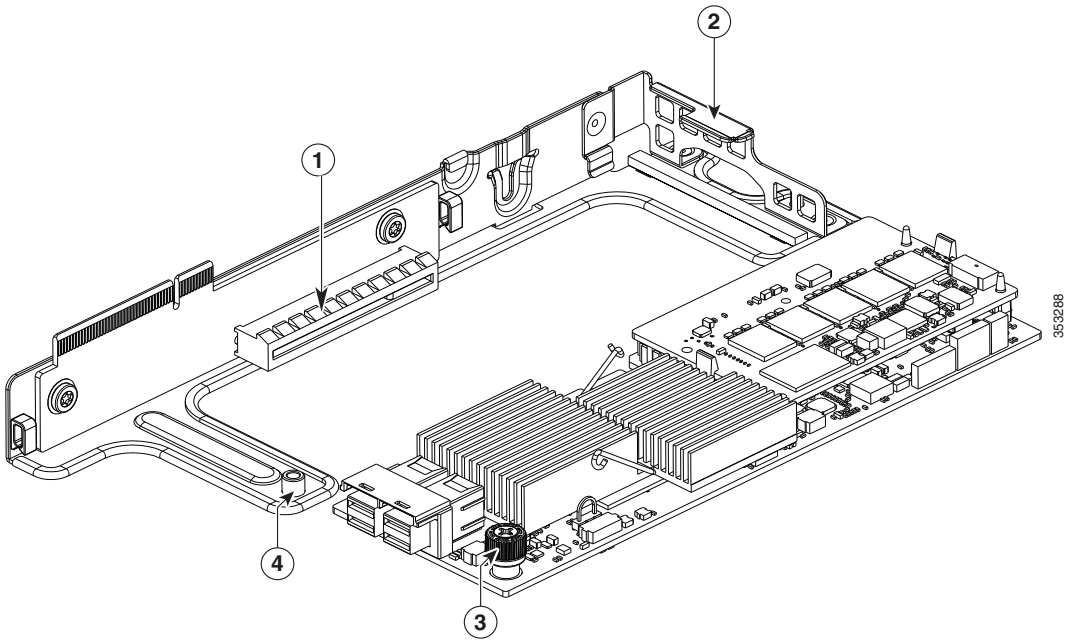
b. Push down gently to engage the riser connector with the motherboard socket. The metal riser bracket must also engage the two pegs that secure it to the chassis wall.

Step 6 Reconnect the SAS cable to its connector on the RAID controller card.

Step 7 Replace the top cover.

Step 8 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-19 Cisco Modular RAID Controller Card in Riser



1	Card socket on upside down riser	**3**	Thumbscrew on card
2	Guide channel on riser	**4**	Threaded standoff on riser **CAUTION:** Do not scrape the underside of the card on this threaded standoff.

Replacing a Modular RAID Controller Transportable Memory Module (TMM)

The transportable memory module (TMM) that attaches to the modular RAID controller card can be installed or replaced after-factory.

See also:

- Replacing a Cisco Modular RAID Controller Card, page 3-33
- Replacing the Supercap Power Module (RAID Backup), page 3-38

Step 1 Prepare the node for component installation:

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 2 Remove the RAID controller riser from the node (see Figure 3-18):

a. Disconnect the SAS cable from the existing RAID controller card.

b. Lift the riser straight up to disengage the riser from the motherboard socket. The riser bracket must also lift off of two pegs that hold it to the inner chassis wall.

c. Set the riser upside down.

Step 3 Remove the card from the riser:

a. Loosen the single thumbscrew that secures the card to the metal riser bracket (see Figure 3-19).

b. Pull the card straight out from its socket on the riser and the guide channel on the riser bracket.

c. Set the card on an antistatic surface.

Step 4 Remove a TMM from the modular RAID controller card (see Figure 3-20):

a. The plastic bracket on the card has a securing plastic clip at each end of the TMM. Gently spread each clip away from the TMM.

b. Pull straight up on the TMM to lift it off the two plastic guide pegs and the socket on the card.

Step 5 Install a TMM to the modular RAID controller card (see Figure 3-20):

a. Align the TMM over the bracket on the card. Align the connector on the underside of the TMM with the socket on the card. Align the two guide holes on the TMM over the two guide pegs on the card.

Caution In the next step, keep the TMM level and parallel with the surface of the card to avoid damaging the connector or socket.

b. Gently lower the TMM so that the guide holes on the TMM go over the guide pegs on the card.

c. Press down on the TMM until the plastic clips on the bracket close over each end of the TMM.

d. Press down on the TMM to fully seat its connector with the socket on the card.

Step 6 Install the modular RAID controller card back into the riser:

Note If this is a first-time installation of your TMM, you must also install a supercap power module (SCPM). The SCPM cable attaches to a connector on the TMM. See Replacing the Supercap Power Module (RAID Backup), page 3-38.

a. Connect the cable from the supercap power module (RAID battery) to the connector on the TMM (see Figure 3-20).

b. With the riser upside down, align the connector on the card with the socket on the riser. The end of the card should also go into the guide channel on the riser bracket (see Figure 3-19).

c. Carefully push on both corners of the card until it is seated in the socket.

d. Tighten the single thumbscrew that secures the card to the riser bracket.

Step 7 Return the riser to the node:

a. Align the connector on the riser with the socket on the motherboard. At the same time, align the two slots on the back side of the bracket with the two pegs on the inner chassis wall.

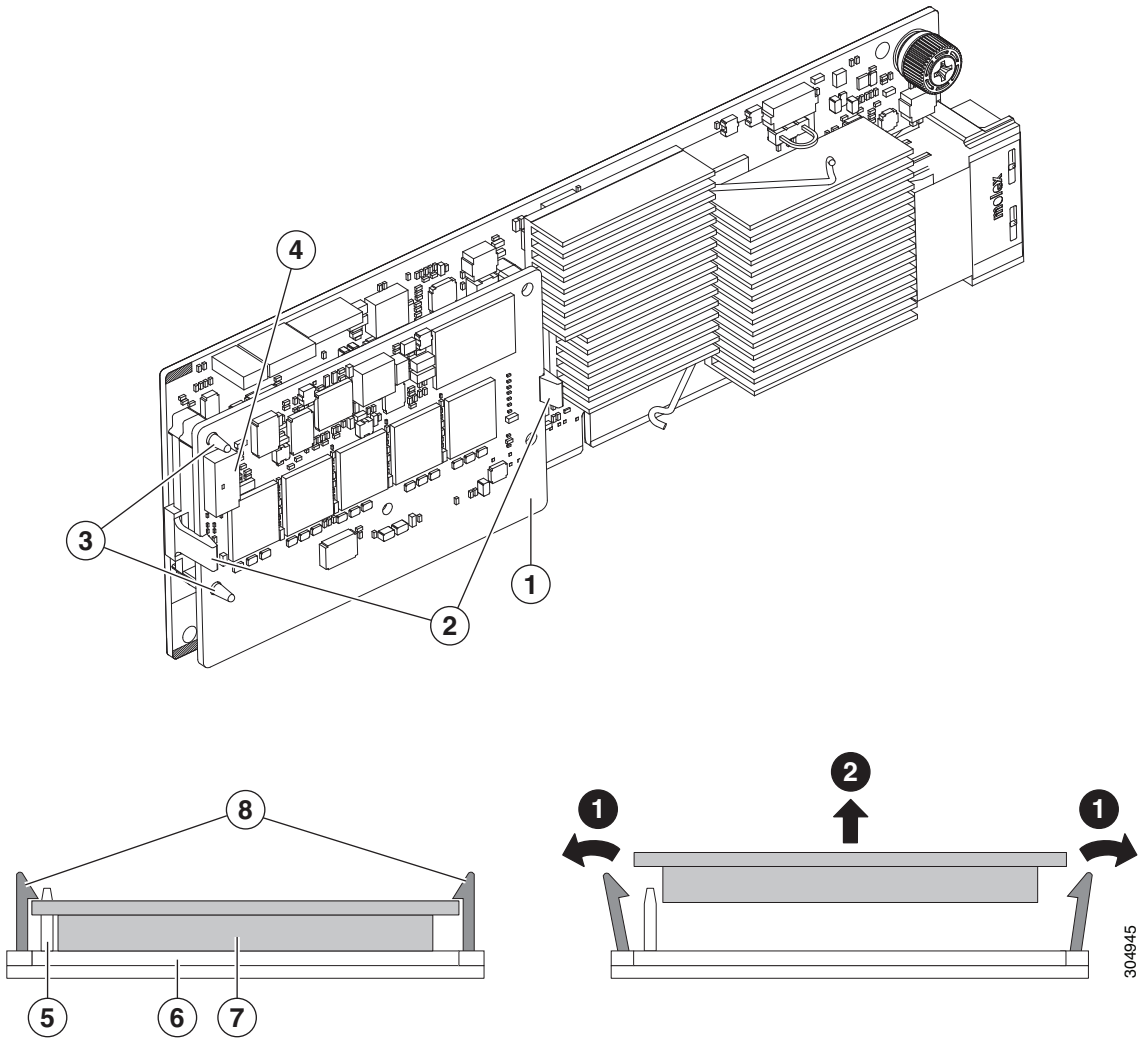
b. Push down gently to engage the riser connector with the motherboard socket. The metal riser bracket must also engage the two pegs that secure it to the chassis wall.

Step 8 Reconnect the SAS cable to its connector on the RAID controller card.

Step 9 Replace the top cover.

Step 10 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-20 TMM on Modular RAID Controller Card



1	TMM on modular RAID card	**5**	Side view, guide peg
2	Securing bracket clips	**6**	Side view, socket on modular RAID card
3	Guide pegs on bracket protruding through guide holes on TMM	**7**	Side view, connector on underside of TMM
4	SCPM cable connector on TMM	**8**	Side view, securing clips

Replacing the Supercap Power Module (RAID Backup)

This node supports installation of one supercap Power module (SCPM). The unit mounts to a bracket that is in the middle of the row of fan modules (see Figure 3-21).

The SCPM provides approximately three years of backup for the disk write-back cache DRAM in the case of a sudden power loss by offloading the cache to the NAND flash.

See also:

- Replacing a Cisco Modular RAID Controller Card, page 3-33
- Replacing a Modular RAID Controller Transportable Memory Module (TMM), page 3-35

Warning **There is danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.**
Statement 1015

Step 1 Remove an existing SCPM (see Figure 3-21).

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

d. Disconnect the SCPM cable from the existing SCPM.

e. Release the securing clip on the bracket retainer bar and then open the retainer bar (see Figure 3-21).

f. Lift the SCPM free of the bracket and set it aside.

Step 2 Install a new SCPM:

a. Set the new SCPM into the mounting bracket.

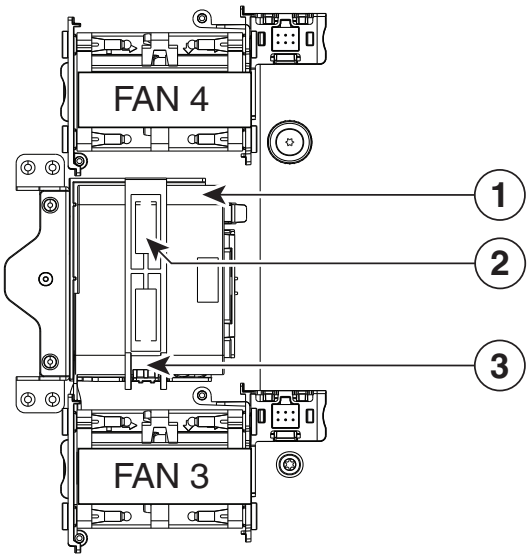
b. Connect the cable from the Cisco modular RAID controller to the new SCPM.

c. Close the retainer bar over the SCPM. Push down until the securing clip clicks and holds down the retainer bar.

d. Replace the top cover.

e. Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-21 SCPM Bracket Location

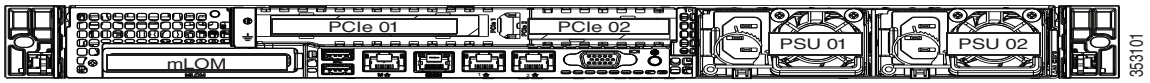


1	SCPM mounting bracket between fans 3 and 4	**3**	Retainer bar securing clip
2	Retainer bar		

Replacing a PCIe Riser Assembly

The node contains two PCIe risers that are attached to a single riser assembly. Riser 1 provides PCIe slot 1 and riser 2 provides PCIe slot 2, as shown in Figure 3-22. See Table 3-5 for a description of the PCIe slots on each riser.

Figure 3-22 Rear Panel, Showing PCIe Slots



To install or replace a PCIe riser, follow these steps:

Step 1 Remove the PCIe riser assembly that you are replacing:

- **a.** Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.
- **b.** Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

- **c.** Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.
- **d.** Use two hands to grasp the metal bracket of the riser assembly and lift straight up to disengage its connectors from the two sockets on the motherboard.
- **e.** If the riser has any cards installed, remove them from the riser.

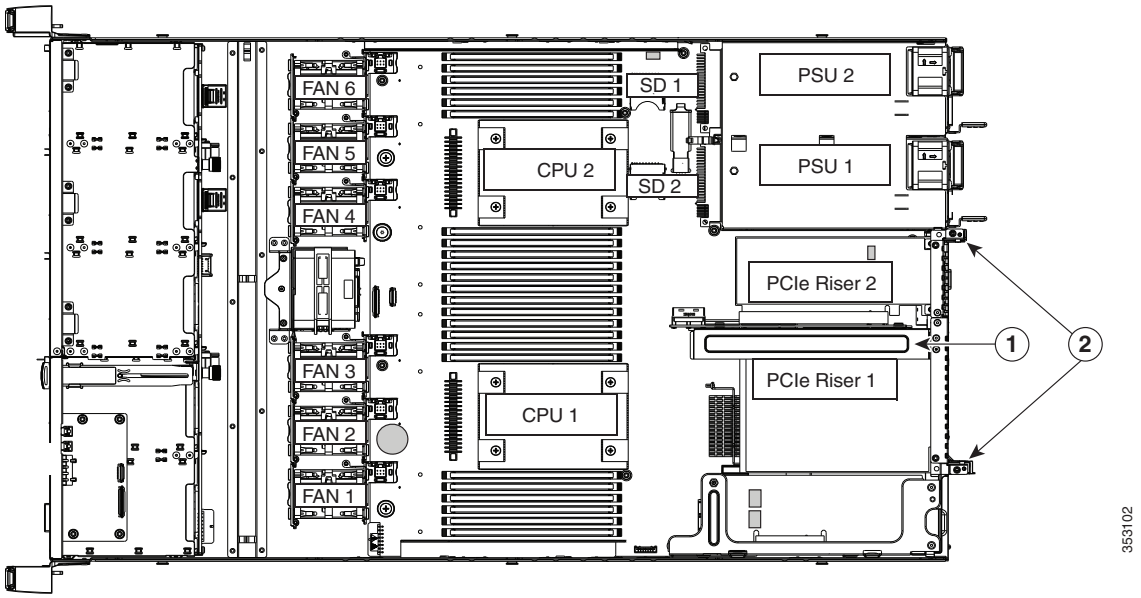
Step 2 Install a new PCIe riser assembly:

- **a.** If you removed any cards from the old riser assembly, install the cards to the new riser assembly (see Replacing a PCIe Card, page 3-42).
- **b.** Position the riser assembly over its two sockets on the motherboard and over the chassis alignment channels (see Figure 3-23):
- **c.** Carefully push down on both ends of the riser assembly to fully engage its connectors with the two sockets on the motherboard.

Step 3 Replace the top cover.

Step 4 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-23 PCIe Riser Assembly Location and Alignment Channels



1	PCIe riser assembly bracket	**3**	Chassis alignment channels

Replacing a PCIe Card

Caution Cisco supports all PCIe cards qualified and sold by Cisco. PCIe cards not qualified or sold by Cisco are the responsibility of the customer. Although Cisco will always stand behind and support the HX-Series nodes, customers using standard, off-the-shelf, third-party cards must go to the third-party card vendor for support if any issue with that particular third-party card occurs.

This section includes the following topics:

PCIe Slots

The node contains two toolless PCIe risers for horizontal installation of PCIe cards. See Figure 3-24 and Table 3-5 for a description of the PCIe slots on these risers.

Both slots support the network communications services interface (NCSI) protocol and standby power.

Figure 3-24 Rear Panel, Showing PCIe Slots

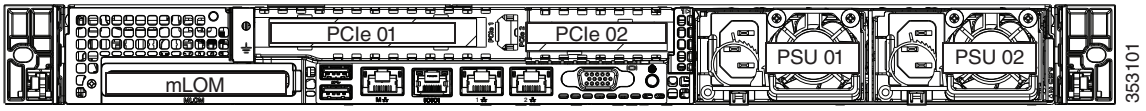


Table 3-5 PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Card Length[1]	Card Height [2]	NCSI Support
1 (on riser 1)	Gen-3 x16	x24 connector	3/4 length	Full-height	Yes
2 (on riser version 2A)[3]	Gen-3 x16	x24 connector	1/2 length	1/2 height	Yes
2 (on riser version 2B)[4]	Gen-3 x8	x24 connector	1/2 length	1/2 height	Yes

1. This is the supported length because of internal clearance.
2. This is the size of the rear panel opening.
3. Slot 2 is not available in single-CPU configurations.
4. Riser version 2B(UCSC-PCI-2B-220M4) includes two cable connectors that support NVMe PCIe SSDs.

Replacing a PCIe Card

Note If you are installing a Cisco UCS Virtual Interface Card, there are prerequisite considerations. See Special Considerations for Cisco UCS Virtual Interface Cards, page 3-45.

Note If you are installing a RAID controller card, see RAID Controller Considerations, page C-1 for more information about supported cards and cabling.

To install or replace a PCIe card, follow these steps:

Step 1 Remove an existing PCIe card (or a blank filler panel) from the PCIe riser:

a. Shut down and power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

d. Remove any cables from the ports of the PCIe card that you are replacing.

e. Use two hands to grasp the metal bracket of the riser assembly and lift straight up to disengage its connectors from the two sockets on the motherboard.

f. Open the hinged plastic retainer that secures the rear-panel tab of the card (see Figure 3-25).

g. Pull evenly on both ends of the PCIe card to remove it from the socket on the PCIe riser.

If the riser has no card, remove the blanking panel from the rear opening of the riser.

Step 2 Install a new PCIe card:

a. Open the hinged plastic retainer

b. With the hinged tab retainer open, align the new PCIe card with the empty socket on the PCIe riser.

c. Push down evenly on both ends of the card until it is fully seated in the socket.

d. Ensure that the card's rear panel tab sits flat against the riser rear-panel opening and then close the hinged tab retainer over the card's rear-panel tab (see Figure 3-25).

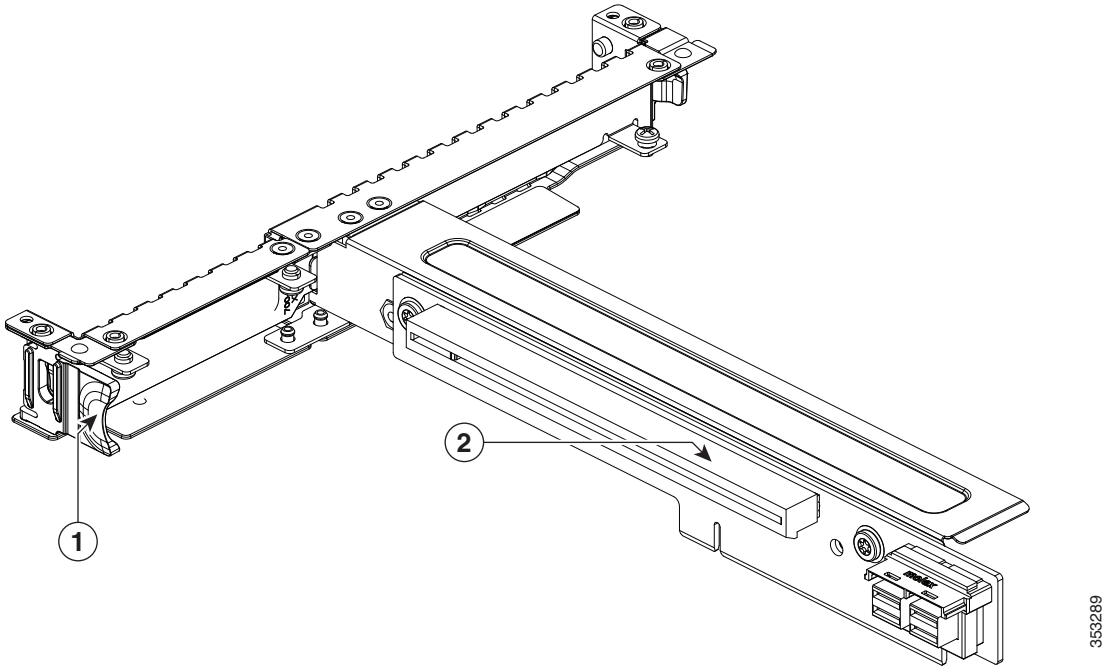
e. Position the PCIe riser over its two sockets on the motherboard and over the chassis alignment channels (see Figure 3-23).

f. Carefully push down on both ends of the PCIe riser to fully engage its connector with the sockets on the motherboard.

g. Replace the top cover.

h. Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-25 PCIe Riser Assembly



1	Hinged rear-panel tab retainer	**2**	Card socket on riser (riser 2 socket shown)

Special Considerations for Cisco UCS Virtual Interface Cards

Table 3-6 describes the requirements for the supported Cisco UCS virtual interface cards (VICs).

The node can support up to two PCIe-style VICs plus one mLOM-style VIC.

Note If you use the Cisco Card NIC mode, you must also make a VIC Slot setting that matches where your VIC is installed. The options are Riser1, Riser2, and Flex-LOM. See NIC Modes and NIC Redundancy Settings, page 2-14.

If you want to use the Cisco UCS VIC card for Cisco UCS Manager integration, also see the Cisco UCS C-Series Server Integration with UCS Manager Guides for details about supported configurations, cabling, and other requirements.

Table 3-6 Cisco UCS HX220c M4 Requirements for Virtual Interface Cards

Virtual Interface Card (VIC)	Number of This VIC Supported in node	Slots That Support VICs	Primary Slot For Cisco UCS Manager Integration	Primary Slot For Cisco Card NIC Mode	Minimum Cisco IMC Firmware	Minimum VIC Firmware
Cisco UCS VIC 1227 UCSC-MLOM-CSC-02	1 mLOM	mLOM	mLOM	mLOM	2.0(3)	4.0(0)

Note The Cisco UCS VIC 1227 (UCSC-MLOM-CSC-02) is not compatible to use in *Cisco Card* NIC mode with a certain Cisco SFP+ module. Do not use a Cisco SFP+ module part number 37-0961-01 that has a serial number in the range MOC1238*xxxx* to MOC1309*xxxx*. If you use the Cisco UCS VIC 1227 in Cisco Card NIC mode, use a different part number Cisco SFP+ module, or you can use this part number 37-0961-01 if the serial number is *not* included in the range above. See the data sheet for this adapter for other supported SFP+ modules: Cisco UCS VIC 1227 Data Sheet

Installing Multiple PCIe Cards and Resolving Limited Resources

When a large number of PCIe add-on cards are installed in the node, the node might run out of the following resources required for PCIe devices:

- Option ROM memory space
- 16-bit I/O space

The topics in this section provide guidelines for resolving the issues related to these limited resources:

- Resolving Insufficient Memory Space to Execute Option ROMs, page 3-46
- Resolving Insufficient 16-Bit I/O Space, page 3-46

Resolving Insufficient Memory Space to Execute Option ROMs

The node has very limited memory to execute PCIe legacy option ROMs, so when a large number of PCIe add-on cards are installed in the node, the node BIOS might not able to execute all of the option ROMs. The node BIOS loads and executes the option ROMs in the order that the PCIe cards are enumerated (slot 1, slot 2, slot 3, and so on).

If the node BIOS does not have sufficient memory space to load any PCIe option ROM, it skips loading that option ROM, reports a node event log (SEL) event to the Cisco IMC controller and reports the following error in the Error Manager page of the BIOS Setup utility:

```
ERROR CODE  SEVERITY    INSTANCE    DESCRIPTION
146         Major       N/A         PCI out of resources error.
                                    Major severity requires user
                                    intervention but does not
                                    prevent system boot.
```

To resolve this issue, disable the Option ROMs that are not needed for system booting. The BIOS Setup Utility provides the setup options to enable or disable the Option ROMs at the PCIe slot level for the PCIe expansion slots and at the port level for the onboard NICs. These options can be found in the BIOS Setup Utility **Advanced** > **PCI Configuration** page.

- **Guidelines for RAID controller booting**

  If the node is configured to boot primarily from RAID storage, make sure that the option ROMs for the slots where your RAID controllers installed are enabled in the BIOS, depending on your RAID controller configuration.

  If the RAID controller does not appear in the node boot order even with the option ROMs for those slots enabled, the RAID controller option ROM might not have sufficient memory space to execute. In that case, disable other option ROMs that are not needed for the node configuration to free up some memory space for the RAID controller option ROM.

- **Guidelines for onboard NIC PXE booting**

  If the node is configured to primarily perform PXE boot from onboard NICs, make sure that the option ROMs for the onboard NICs to be booted from are enabled in the BIOS Setup Utility. Disable other option ROMs that are not needed to create sufficient memory space for the onboard NICs.

Resolving Insufficient 16-Bit I/O Space

The node has only 64 KB of legacy 16-bit I/O resources available. This 64 KB of I/O space is divided between the CPUs in the node because the PCIe controller is integrated into the CPUs. This node BIOS has the capability to dynamically detect the 16-bit I/O resource requirement for each CPU and then balance the 16-bit I/O resource allocation between the CPUs during the PCI bus enumeration phase of the BIOS POST.

When a large number of PCIe cards are installed in the node, the node BIOS might not have sufficient I/O space for some PCIe devices. If the node BIOS is not able to allocate the required I/O resources for any PCIe devices, the following symptoms have been observed:

- The node might get stuck in an infinite reset loop.
- The BIOS might appear to hang while initializing PCIe devices.
- The PCIe option ROMs might take excessive time to complete, which appears to lock up the node.
- PCIe boot devices might not be accessible from the BIOS.
- PCIe option ROMs might report initialization errors. These errors are seen before the BIOS passes control to the operating system.

- The keyboard might not work.

To work around this problem, rebalance the 16-bit I/O load using the following methods:

1. Physically remove any unused PCIe cards.
2. If the node has one or more Cisco virtual interface cards (VICs) installed, disable the PXE boot on the VICs that are not required for the node boot configuration by using the Network Adapters page in the Cisco IMC Web UI to free up some 16-bit I/O resources. Each VIC uses a minimum 16 KB of 16-bit I/O resource, so disabling PXE boot on Cisco VICs would free up some 16-bit I/O resources that can be used for other PCIe cards that are installed in the node.

Installing and Enabling a Trusted Platform Module

The trusted platform module (TPM) is a small circuit board that attaches to a motherboard socket. The socket location is on the motherboard between the power supplies and PCIe riser 2 (see Figure 3-26).

This section contains the following procedures, which must be followed in this order when installing and enabling a TPM:

1. Installing the TPM Hardware, page 3-48
2. Enabling TPM Support in the BIOS, page 3-49
3. Enabling the Intel TXT Feature in the BIOS, page 3-50

Note For security purposes, the TPM is installed with a one-way screw. It cannot be removed with a standard screwdriver.

Installing the TPM Hardware

Step 1 Prepare the node for component installation.

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

d. Check if there is a card installed in PCIe riser 2. See Figure 3-26.

- If no card is installed in PCIe riser 2, you can access the TPM socket. Go to Step 2.
- If a card is installed in PCIe riser 2, remove the PCIe riser assembly from the chassis. See Replacing a PCIe Riser Assembly, page 3-40 for details.

Step 2 Install a TPM (see Figure 3-26):

a. Locate the TPM socket on the motherboard, as shown in Figure 3-26.

b. Align the connector that is on the bottom of the TPM circuit board with the motherboard TPM socket. Align the screw hole on the TPM board with the screw hole adjacent to the TPM socket.

c. Push down evenly on the TPM to seat it in the motherboard socket.

d. Install the single one-way screw that secures the TPM to the motherboard.

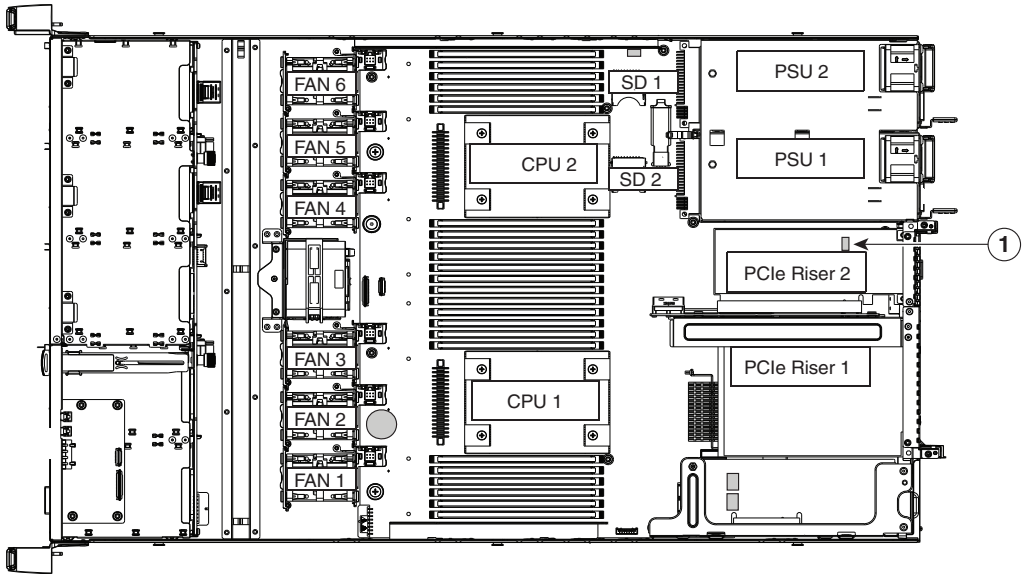
e. If you removed the PCIe riser assembly, return it to the node now. See Replacing a PCIe Riser Assembly, page 3-40 for details.

f. Replace the top cover.

g. Replace the node in the rack and then power on the node by pressing the **Power** button.

Step 3 Continue with Enabling TPM Support in the BIOS, page 3-49.

Figure 3-26 TPM Socket Location on Motherboard



1	TPM socket and screw hole on motherboard		

Enabling TPM Support in the BIOS

Note After hardware installation, you must enable TPM support in the BIOS:

Step 1 Enable TPM support:

a. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.
b. Log in to the BIOS Setup Utility with your BIOS Administrator password.
c. On the BIOS Setup Utility window, choose the **Advanced** tab.
d. Choose **Trusted Computing** to open the TPM Security Device Configuration window.
e. Change TPM SUPPORT to **Enabled**.
f. Press **F10** to save your settings and reboot the node.

Step 2 Verify that TPM support is now enabled:

a. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.
b. Log into the BIOS Setup utility with your BIOS Administrator password.
c. Choose the **Advanced** tab.
d. Choose **Trusted Computing** to open the TPM Security Device Configuration window.
e. Verify that TPM SUPPORT and TPM State are Enabled.

Step 3 Continue with Enabling the Intel TXT Feature in the BIOS, page 3-50.

Enabling the Intel TXT Feature in the BIOS

Intel Trusted Execution Technology (TXT) provides greater protection for information that is used and stored on the node. A key aspect of that protection is the provision of an isolated execution environment and associated sections of memory where operations can be conducted on sensitive data, invisibly to the rest of the node. Intel TXT provides for a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code.

Step 1 Reboot the node and watch for the prompt to press F2.

Step 2 When prompted, press **F2** to enter the BIOS Setup utility.

Step 3 Verify that the prerequisite BIOS values are enabled:

a. Choose the **Advanced** tab.

b. Choose **Intel TXT(LT-SX) Configuration** to open the Intel TXT(LT-SX) Hardware Support window.

c. Verify that the following items are listed as Enabled:

- VT-d Support (default is Enabled)
- VT Support (default is Enabled)
- TPM Support
- TPM State

- If VT-d Support and VT Support are already enabled, skip to Step 4.
- If VT-d Support and VT Support are not enabled, continue with the next steps to enable them.

d. Press **Escape** to return to the BIOS Setup utility **Advanced** tab.

e. On the Advanced tab, choose **Processor Configuration** to open the Processor Configuration window.

f. Set Intel (R) VT and Intel (R) VT-d to **Enabled**.

Step 4 Enable the Intel Trusted Execution Technology (TXT) feature:

a. Return to the Intel TXT(LT-SX) Hardware Support window if you are not already there.

b. Set TXT Support to **Enabled**.

Step 5 Press **F10** to save your changes and exit the BIOS Setup utility.

Replacing an mLOM Card

The node can use a modular LOM (mLOM) card to provide additional rear-panel connectivity. The mLOM card socket remains powered when the node is in 12 V standby power mode and it supports the network communications services interface (NCSI) protocol.

Step 1 Remove any existing mLOM card (or a blanking panel):

a. Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

b. Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

c. Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 2 See the location of the mLOM socket in Figure 3-27. You might have to remove PCIe riser 1 and the Cisco modular RAID controller riser to provide clearance.

- If there is no card in PCIe riser 1 or the RAID card riser, you can access the mLOM socket. Continue with Step 3.
- If there is a card in PCIe riser 1 or the RAID card riser, remove those risers to provide clearance. See Replacing a PCIe Riser Assembly, page 3-40 and Replacing a Cisco Modular RAID Controller Card, page 3-33 for instructions.

Step 3 Loosen the single thumbscrew that secures the mLOM card to the chassis floor and then slide the mLOM card horizontally to disengage its connector from the motherboard socket.

Step 4 Install a new mLOM card:

a. Set the mLOM card on the chassis floor so that its connector is aligned with the motherboard socket and its thumbscrew is aligned with the standoff on the chassis floor.

b. Push the card's connector into the motherboard socket horizontally.

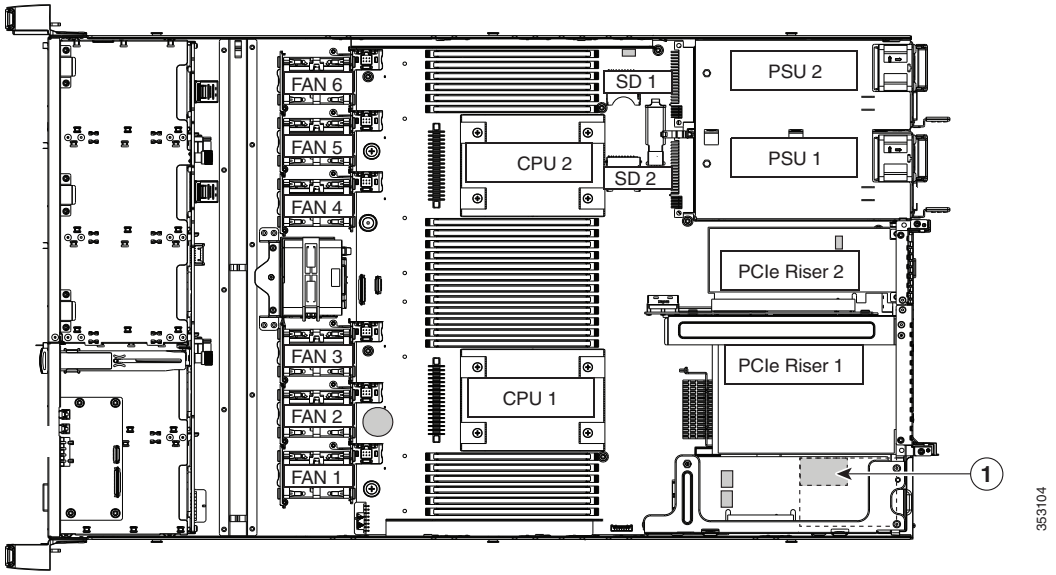
c. Tighten the thumbscrew to secure the card to the chassis floor.

Step 5 If you removed PCIe riser 1 or the RAID card riser, return them to the node. See Replacing a PCIe Riser Assembly, page 3-40 or Replacing a Cisco Modular RAID Controller Card, page 3-33 for instructions.

Step 6 Replace the top cover.

Step 7 Replace the node in the rack, replace cables, and then power on the node by pressing the **Power** button.

Figure 3-27 mLOM Card Socket Location



1	mLOM card socket location on motherboard (under a PCIe riser 1 card and the RAID controller card)		

Replacing Power Supplies

When two power supplies are installed they are redundant as 1+1.

- Replacing an AC Power Supply, page 3-53
- See Power Specifications, page A-3 for more information about the power supplies.
- See Rear Panel LEDs and Buttons, page 3-5 for information about the power supply LEDs.

Note You do not have to power off the node to replace power supplies because they are redundant as 1+1.

Note Do not mix power supply types or wattages in the node.

Replacing an AC Power Supply

Step 1 Remove the power supply that you are replacing or a blank panel from an empty bay (see Figure 3-28):

a. Perform one of the following actions:
   - If your node has only one power supply, shut down and power off the node as described in the "Shutting Down and Powering Off the Node" section on page 3-8.
   - If your node has two power supplies, you do not have to shut down the node.

b. Remove the power cord from the power supply that you are replacing.

c. Grasp the power supply handle while pinching the release lever toward the handle.

d. Pull the power supply out of the bay.

Step 2 Install a new power supply:

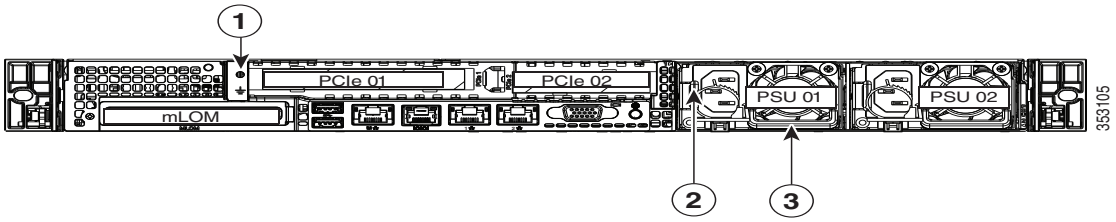
a. Grasp the power supply handle and insert the new power supply into the empty bay.

b. Push the power supply into the bay until the release lever locks.

c. Connect the power cord to the new power supply.

d. If you shut down the node, press the **Power** button to return the node to main power mode.

Figure 3-28 Removing and Replacing Power Supplies



1	Power supply release lever	2	Power supply handle

Service DIP Switches

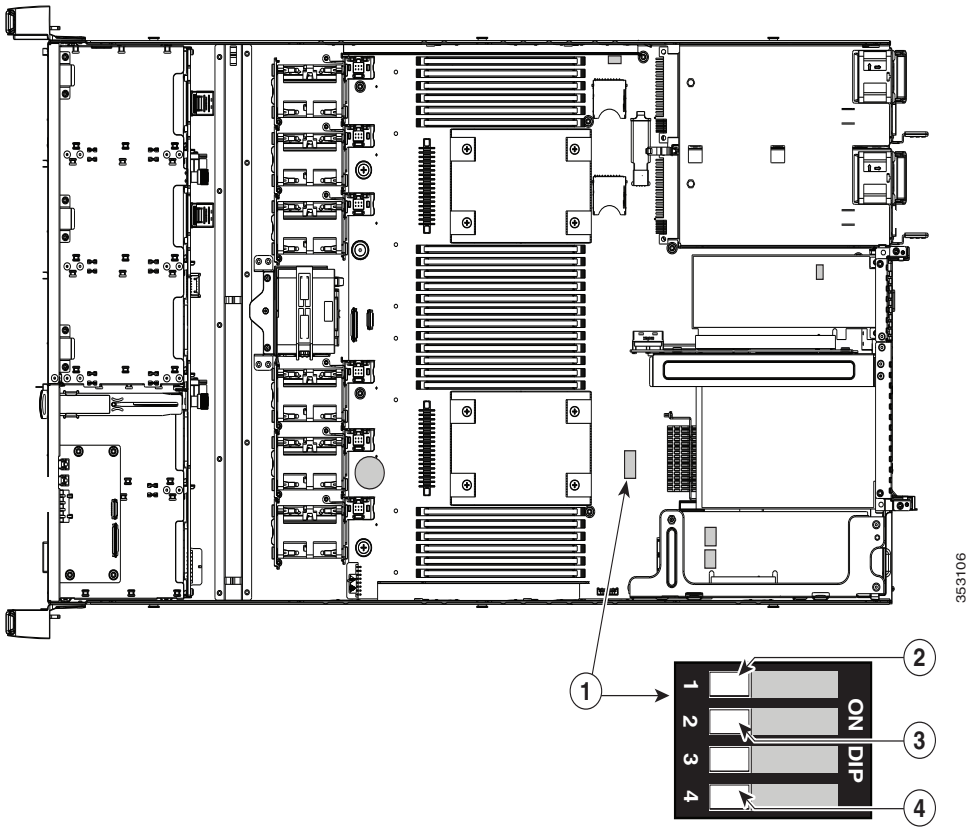
This section includes the following topics:

DIP Switch Location on the Motherboard

See Figure 3-29. The position of the block of DIP switches (SW6) is shown in red. In the magnified view, all switches are shown in the default position.

- BIOS recovery—Switch 1
- Clear password—Switch 2
- Not used—Switch 3
- Clear CMOS—Switch 4

Figure 3-29 Service DIP Switches (SW6)



1	DIP switch block SW6	**3**	Clear password switch 2
2	BIOS recovery switch 1	**4**	Clear CMOS switch 4

Using the BIOS Recovery DIP Switch

Depending on which stage the BIOS becomes corrupted, you might see different behavior.

- If the BIOS BootBlock is corrupted, you might see the node get stuck on the following message:

```
Initializing and configuring memory/hardware
```

- If it is a non-BootBlock corruption, the following message is displayed:

```
****BIOS FLASH IMAGE CORRUPTED****
Flash a valid BIOS capsule file using Cisco IMC WebGUI or CLI interface.
IF Cisco IMC INTERFACE IS NOT AVAILABLE, FOLLOW THE STEPS MENTIONED BELOW.
1. Connect the USB stick with recovery.cap file in root folder.
2. Reset the host.
IF THESE STEPS DO NOT RECOVER THE BIOS
1. Power off the system.
2. Mount recovery jumper.
3. Connect the USB stick with recovery.cap file in root folder.
4. Power on the system.
Wait for a few seconds if already plugged in the USB stick.
REFER TO SYSTEM MANUAL FOR ANY ISSUES.
```

Note As indicated by the message shown above, there are two procedures for recovering the BIOS. Try procedure 1 first. If that procedure does not recover the BIOS, use procedure 2.

Procedure 1: Reboot with recovery.cap File

Step 1 Download the BIOS update package and extract it to a temporary location.

Step 2 Copy the contents of the extracted recovery folder to the root directory of a USB thumb drive. The recovery folder contains the recovery.cap file that is required in this procedure.

Note The recovery.cap file must be in the root directory of the USB thumb drive. Do not rename this file. The USB thumb drive must be formatted with either FAT16 or FAT32 file systems.

Step 3 Insert the USB thumb drive into a USB port on the node.

Step 4 Reboot the node.

Step 5 Return the node to main power mode by pressing the **Power** button on the front panel.

The node boots with the updated BIOS boot block. When the BIOS detects a valid recovery.cap file on the USB thumb drive, it displays this message:

```
Found a valid recovery file...Transferring to Cisco IMC
System would flash the BIOS image now...
System would restart with recovered image after a few seconds...
```

Step 6 Wait for node to complete the BIOS update, and then remove the USB thumb drive from the node.

Note During the BIOS update, Cisco IMC shuts down the node and the screen goes blank for about 10 minutes. Do not unplug the power cords during this update. Cisco IMC powers on the node after the update is complete.

Procedure 2: Use BIOS Recovery DIP switch and recovery.cap File

See Figure 3-29 for the location of the SW8 block of DIP switches.

Step 1 Download the BIOS update package and extract it to a temporary location.

Step 2 Copy the contents of the extracted recovery folder to the root directory of a USB thumb drive. The recovery folder contains the recovery.cap file that is required in this procedure.

Note The recovery.cap file must be in the root directory of the USB thumb drive. Do not rename this file. The USB thumb drive must be formatted with either FAT16 or FAT32 file systems.

Step 3 Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

Step 4 Disconnect all power cords from the power supplies.

Step 5 Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

Step 6 Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 7 Slide the BIOS recovery DIP switch from position 1 to the closed position (see Figure 3-29).

Step 8 Reconnect AC power cords to the node. The node powers up to standby power mode.

Step 9 Insert the USB thumb drive that you prepared in Step 2 into a USB port on the node.

Step 10 Return the node to main power mode by pressing the **Power** button on the front panel.

The node boots with the updated BIOS boot block. When the BIOS detects a valid recovery.cap file on the USB thumb drive, it displays this message:

```
Found a valid recovery file...Transferring to Cisco IMC
System would flash the BIOS image now...
System would restart with recovered image after a few seconds...
```

Step 11 Wait for node to complete the BIOS update, and then remove the USB thumb drive from the system.

Note During the BIOS update, Cisco IMC shuts down the node and the screen goes blank for about 10 minutes. Do not unplug the power cords during this update. Cisco IMC powers on the node after the update is complete.

Step 12 After the node has fully booted, power off the node again and disconnect all power cords.

Step 13 Slide the BIOS recovery DIP switch from the closed position back to the default position 1 (see Figure 3-29).

Note If you do not move the jumper, after recovery completion you see the prompt, “Please remove the recovery jumper.”

Step 14 Replace the top cover, replace the node in the rack, replace power cords and any other cables, and then power on the node by pressing the **Power** button.

Using the Clear Password DIP Switch

See Figure 3-29 for the location of this DIP switch. You can use this switch to clear the administrator password.

Step 1 Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

Step 2 Disconnect all power cords from the power supplies.

Step 3 Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

Step 4 Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 5 Slide the clear password DIP switch from position 2 to the closed position (see Figure 3-29).

Step 6 Reinstall the top cover and reconnect AC power cords to the node. The node powers up to standby power mode, indicated when the Power LED on the front panel is amber.

Step 7 Return the node to main power mode by pressing the **Power** button on the front panel. The node is in main power mode when the Power LED is green.

Note You must allow the entire node, not just the service processor, to reboot to main power mode to complete the reset. The state of the jumper cannot be determined without the host CPU running.

Step 8 Press the **Power** button to shut down the node to standby power mode, and then remove AC power cords from the node to remove all power.

Step 9 Remove the top cover from the node.

Step 10 Slide the clear CMOS DIP switch from the closed position back to default position 2 (see Figure 3-29).

Note If you do not move the jumper, the CMOS settings are reset to the default every time that you power-cycle the node.

Step 11 Replace the top cover, replace the node in the rack, replace power cords and any other cables, and then power on the node by pressing the **Power** button.

Using the Clear CMOS DIP Switch

See Figure 3-29 for the location of this DIP switch. You can use this switch to clear the node's CMOS settings in the case of a node hang. For example, if the node hangs because of incorrect settings and does not boot, use this jumper to invalidate the settings and reboot with defaults.

Caution Clearing the CMOS removes any customized settings and might result in data loss. Make a note of any necessary customized settings in the BIOS before you use this clear CMOS procedure.

Step 1 Power off the node as described in Shutting Down and Powering Off the Node, page 3-8.

Step 2 Disconnect all power cords from the power supplies.

Step 3 Slide the node out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the node from the rack.

Step 4 Remove the top cover as described in Removing and Replacing the Node Top Cover, page 3-9.

Step 5 Slide the clear CMOS DIP switch from position 4 to the closed position (see Figure 3-29).

Step 6 Reinstall the top cover and reconnect AC power cords to the node. The node powers up to standby power mode, indicated when the Power LED on the front panel is amber.

Step 7 Return the node to main power mode by pressing the **Power** button on the front panel. The node is in main power mode when the Power LED is green.

Note You must allow the entire node, not just the service processor, to reboot to main power mode to complete the reset. The state of the jumper cannot be determined without the host CPU running.

Step 8 Press the **Power** button to shut down the node to standby power mode, and then remove AC power cords from the node to remove all power.

Step 9 Remove the top cover from the node.

Step 10 Slide the clear CMOS DIP switch from the closed position back to default position 4 (see Figure 3-29).

Note If you do not move the jumper, the CMOS settings are reset to the default every time that you power-cycle the node.

Step 11 Replace the top cover, replace the node in the rack, replace power cords and any other cables, and then power on the node by pressing the **Power** button.

APPENDIX A

Node Specifications

This appendix lists the technical specifications for the node and includes the following sections:

Physical Specifications

Table A-1 lists the physical specifications for the node.

Table A-1 Physical Specifications

Description	Specification
Height	1.7 in. (4.3 cm)
Width	16.9 in. (42.9 cm)
Depth (length)	29.8 in. (75.8 cm)
Maximum weight (fully loaded chassis)	37.9 lb. (17.2 Kg)

Environmental Specifications

Table A-2 lists the environmental specifications for the node.

Table A-2 Environmental Specifications

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.
Temperature, non-operating (when the node is stored or transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), operating	10 to 90%
Humidity, non-operating	5 to 93%
Altitude, operating	0 to 10,000 feet
Altitude, non-operating (when the node is stored or transported)	0 to 40,000 feet
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	5.4
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	37

Power Specifications

The power specifications for the power supply option is listed in the following sections:

- 770 W AC Power Supply, page A-3

You can get more specific power information for your exact node configuration by using the Cisco UCS Power Calculator:

http://ucspowercalc.cisco.com

Note Do not mix power supply types in the node. Both power supplies must be identical.

770 W AC Power Supply

Table A-3 lists the specifications for each 770 W AC power supply (Cisco part number UCSC-PSU1-770W).

Table A-3 Power Supply Specifications

Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC input frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC input current	9.5 A at 100 VAC 4.5 A at 208 VAC
Maximum input volt-amperes	950 VA at 100 VAC
Maximum output power per PSU	770 W
Maximum inrush current	15 A (sub-cycle duration)
Maximum hold-up time	12 ms at 770 W
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C14

APPENDIX B

Power Cord Specifications

This appendix provides supported power cable specifications.

Supported Power Cords and Plugs

Each power supply has a separate power cord. Standard power cords or jumper power cords are available for connection to the node. The jumper power cords, for use in racks, are available as an optional alternative to the standard power cords.

Note Only the approved power cords or jumper power cords provided with the node are supported.

Table B-1 lists the power cords for the node power supplies.

Table B-1 Supported Power Cords for the Node

Description	Length		Power Cord Reference Illustration
	Feet	Meters	
CAB-250V-10A-AR Power Cord, 250 VAC 10 A IRAM 2073 Plug Argentina	8.2	2.5	Figure B-1
CAB-9K10A-AU 250 VAC 10 A 3112 Plug, Australia	8.2	2.5	Figure B-2
CAB-250V-10A-CN Power Cord, 250 VAC 10 A GB 2009 Plug China	8.2	2.5	Figure B-3
CAB-9K10A-EU Power Cord, 250 VAC 10 A M 2511 Plug Europe	8.2	2.5	Figure B-4
CAB-250V-10A-ID Power Cord, 250 VAC 16A EL-208 Plug South Africa, United Arab Emirates, India	8.2	2.5	Figure B-5
CAB-250V-10A-IS Power Cord, 250 VAC 10 A SI32 Plug Israel	8.2	2.5	Figure B-6

Table B-1 Supported Power Cords for the Node (continued)

Description	Length		Power Cord Reference Illustration
	Feet	Meters	
CAB-9K10A-IT Power Cord, 250 VAC 10 A CEI 23-16 Plug Italy	8.2	2.5	Figure B-7
CAB-9K10A-SW Power Cord, 250 VAC 10 A MP232 Plug Switzerland	8.2	2.5	Figure B-8
CAB-9K10A-UK Power Cord, 250 VAC 10 A BS1363 Plug (13 A fuse) United Kingdom	8.2	2.5	Figure B-9
CAB-AC-250V/13A Power Cord, 250 VAC 13 A IEC60320 Plug North America	6.6	2.0	Figure B-10
CAB-N5K6A-NA Power Cord, 250 VAC 13 A NEMA 6-15 Plug, North America	8.2	2.5	Figure B-11
CAB-9K12A-NA Power cord, 125 VAC, 13 A, NEMA 5-15 Plug North America	8.2	2.5	Figure B-12
CAB-C13-CBN Cabinet Jumper Power Cord, 250 VAC 10 A, C13-C14 Connectors	2.2	0.68	Figure B-13
CAB-C13-C14-2M Cabinet Jumper Power Cord, 250 VAC 10 A, C13-C14 Connectors	6.6	2.0	Figure B-14
CAB-C13-C14-AC Cabinet Jumper Power Cord, 250 VAC 10 A, C13-C14 Connectors	9.8	3.0	Figure B-15

AC Power Cord Illustrations

This section includes the AC power cord illustrations. See Figure B-1 through Figure B-15.

Figure B-1 CAB-250V-10A-AR

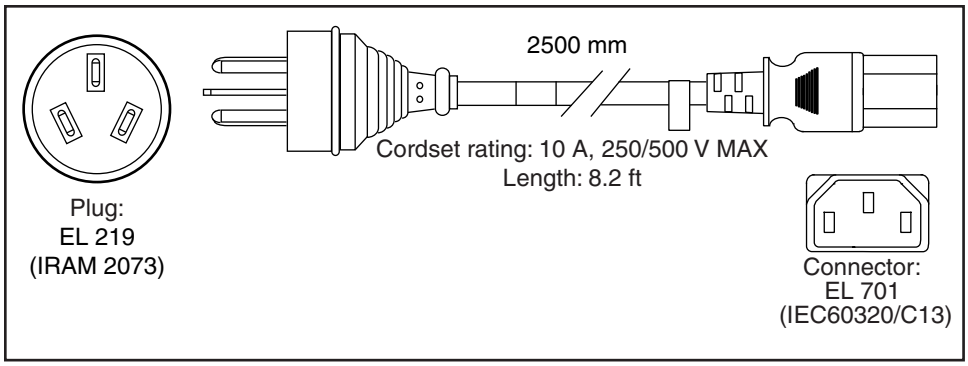


Figure B-2 CAB-9K10A-AU

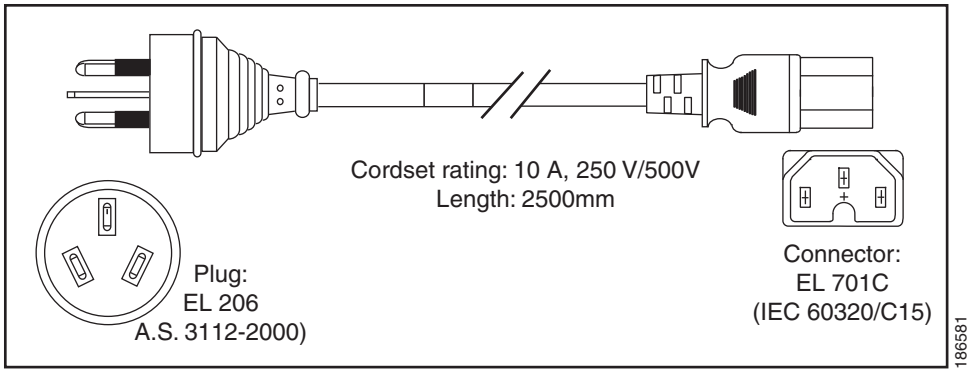


Figure B-3 CAB-250V-10A-CN

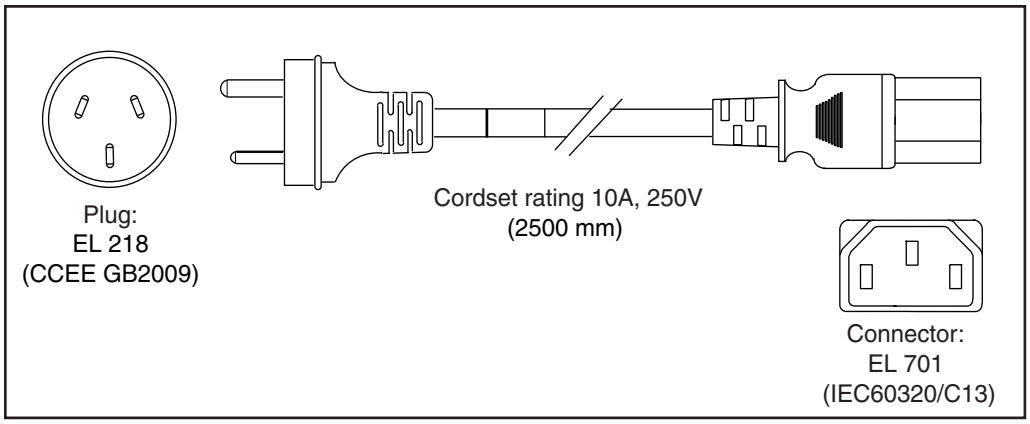


Figure B-4 CAB-9K10A-EU

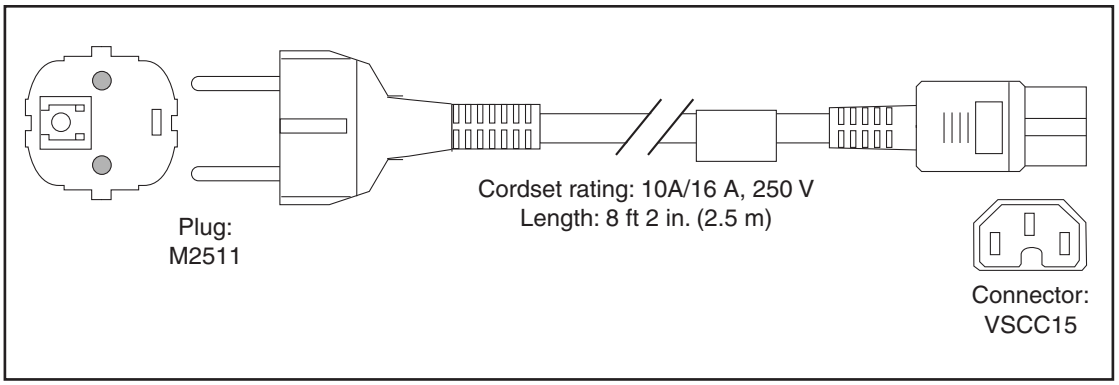


Figure B-5 CAB-250V-10A-ID

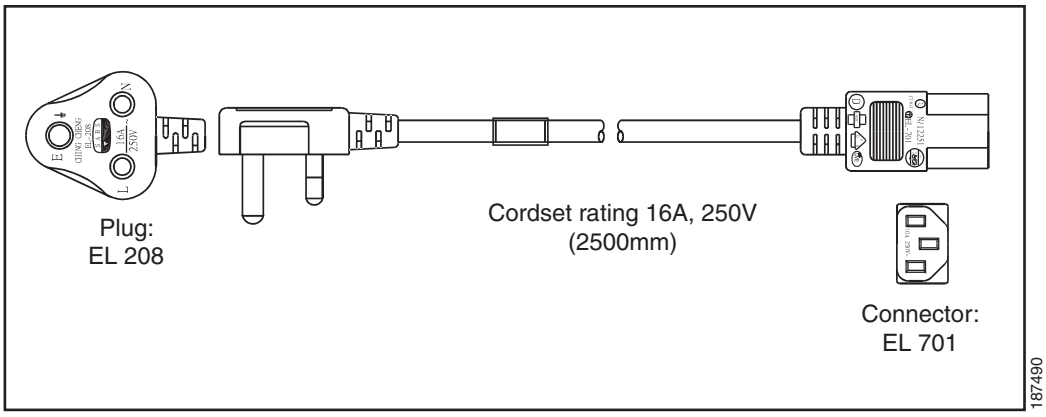


Figure B-6 CAB-250V-10A-IS

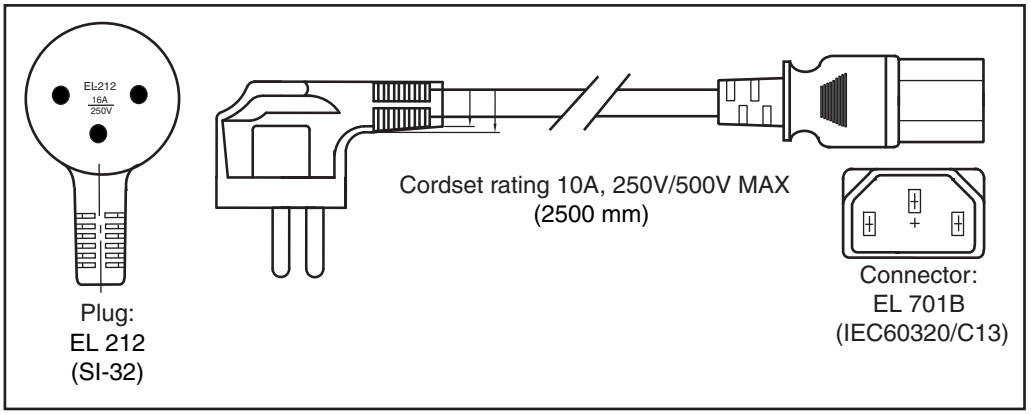


Figure B-7 CAB-9K10A-IT

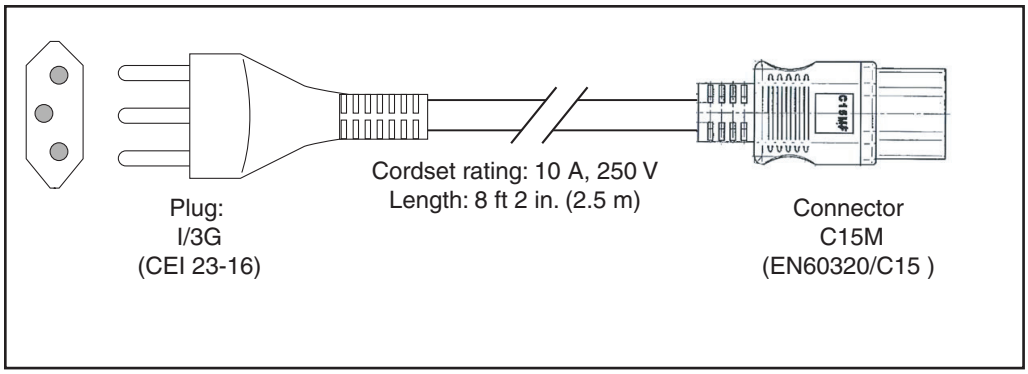


Figure B-8 CAB-9K10A-SW

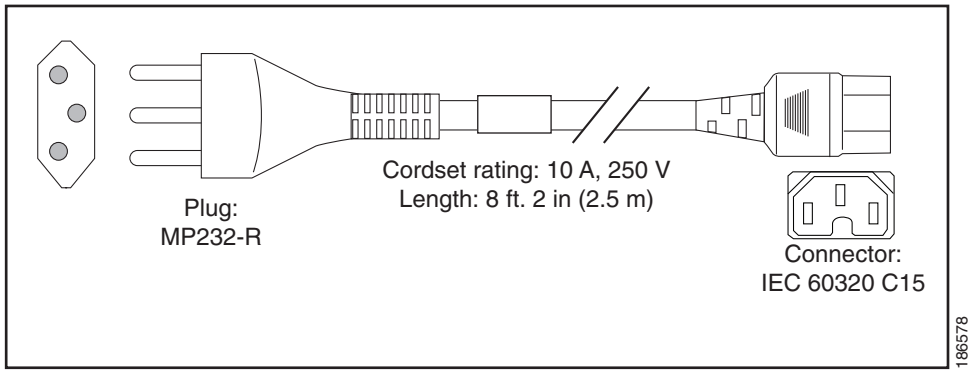


Figure B-9 CAB-9K10A-UK

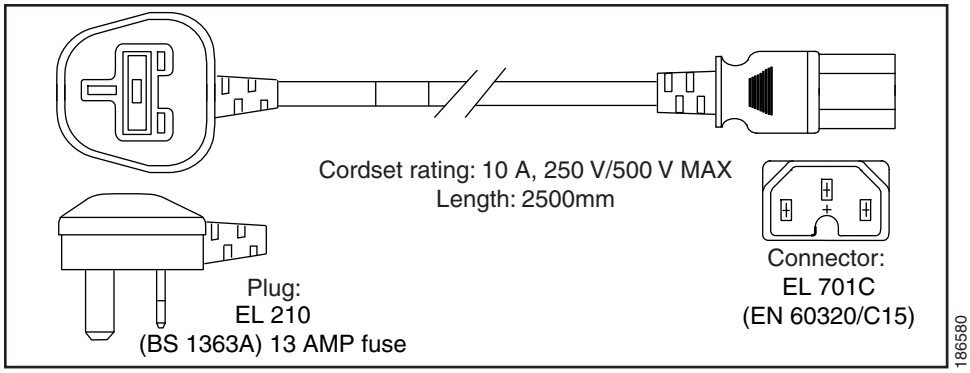


Figure B-10 CAB-AC-250V/13A

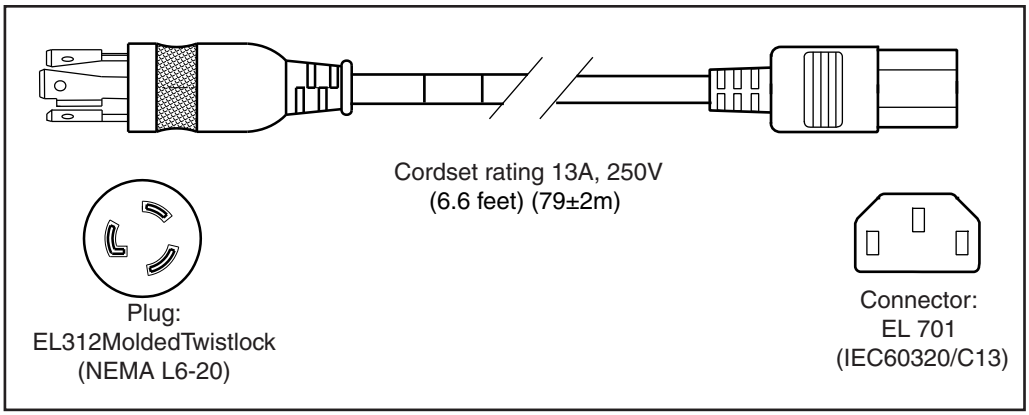


Figure B-11 CAB-N5K6A-NA

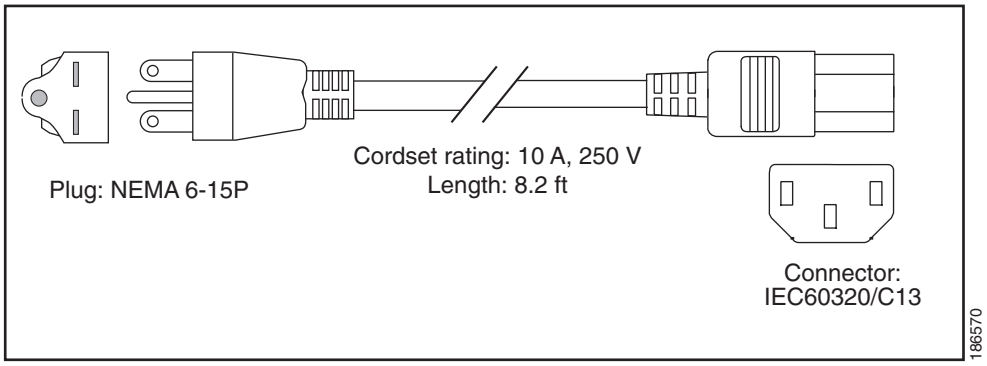


Figure B-12 CAB-9K12A-NA

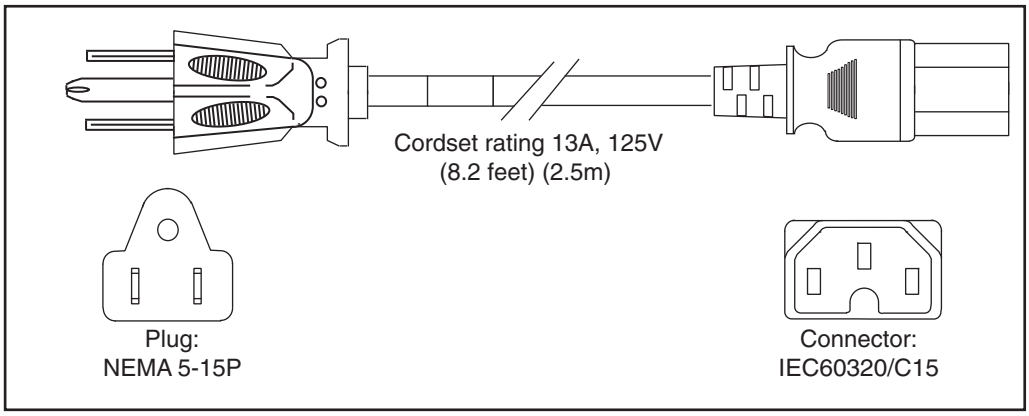


Figure B-13 CAB-C13-CBN, Jumper Power Cord (0.68 m)

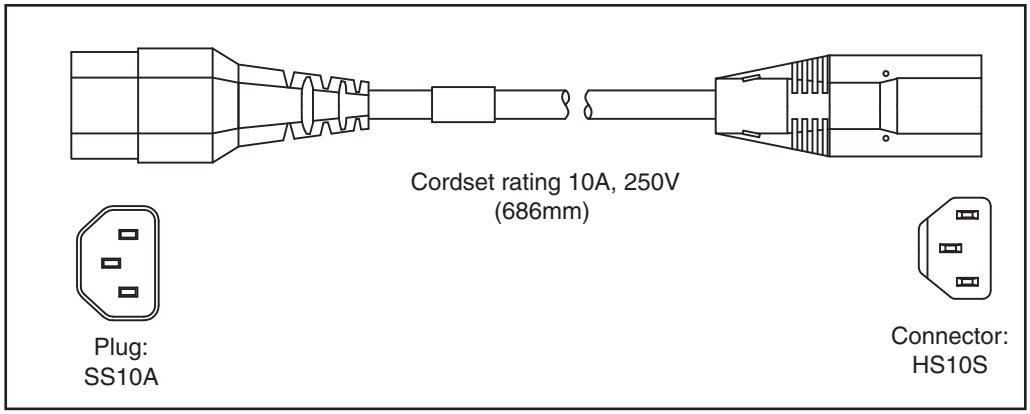


Figure B-14 CAB-C13-C14-2M, Jumper Power Cord (2 m)

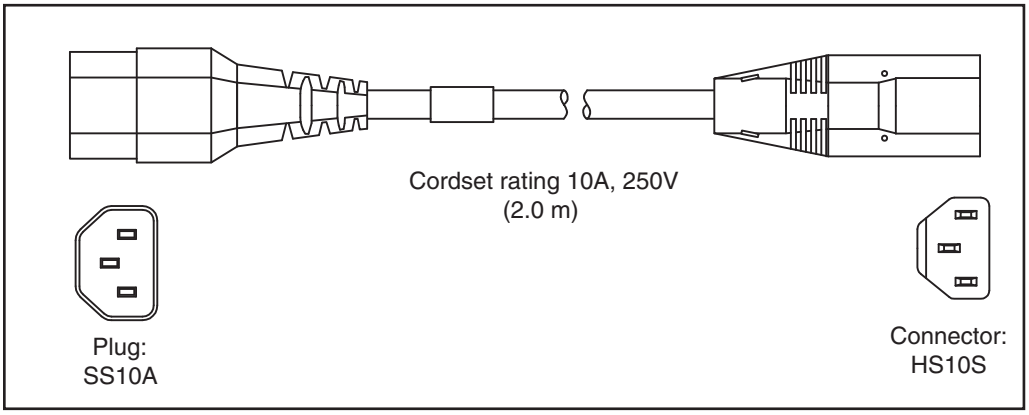
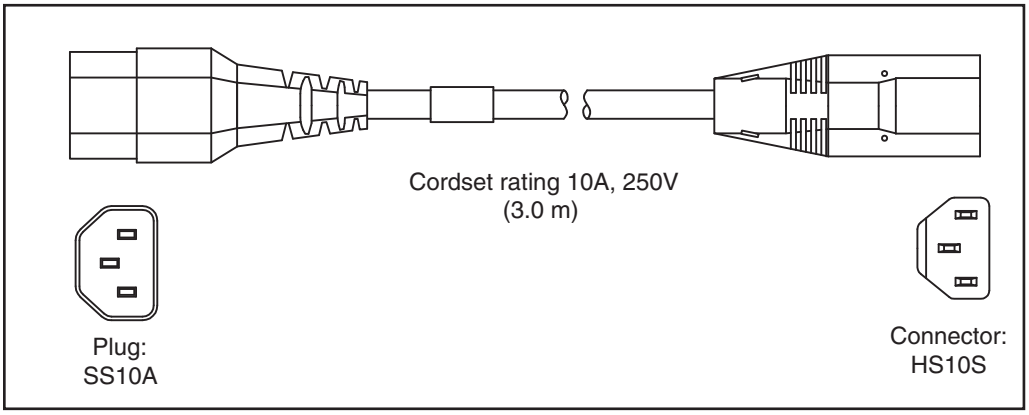


Figure B-15 CAB-C13-C14-AC, Jumper Power Cord (3 m)



RAID Controller Considerations

This appendix contains the following sections:

Supported RAID Controllers and Required Cables

This node supports the RAID controller options and cable requirements shown in Table C-1.

Caution Do not mix controller types in the node. Do not use the embedded MegaRAID controller and a hardware RAID controller card at the same time. This combination is not supported and could result in data loss.

Table C-1 Cisco HX220c M4 RAID Options

Controller	Style	Node Version/ Maximum Drives Controlled	SCPM	RAID Levels	Node Version/Required Cables
Embedded RAID (PCH SATA)	On board	• SFF 8-drives/no expander: 8 internal SATA drives	No	0, 1, 5[1], 10	• SFF 8-drives/no expander: (UCS-220CBLSR8=)
Cisco UCS 12G SAS Modular HBA	PCIe	• SFF 8-drives/no expander: 8 internal drives	No	Non-RAID	• SFF 8 drives/expander: (UCS-220CBLMR8=)

1. Embedded RAID 5 support requires an optional RAID 5 key module.

RAID Card Firmware Compatibility

Firmware on the RAID controller must be verified for compatibility with the current Cisco IMC and BIOS versions that are installed on the node. If not compatible, upgrade or downgrade the RAID controller firmware accordingly using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring node components to compatible levels: HUU Guides

Mixing Drive Types in RAID Groups

Table C-2 lists the technical capabilities for mixing hard disk drive (HDD) and solid state drive (SSD) types in a RAID group. However, see the recommendations that follow for the best performance.

Table C-2 Drive Type Mixing in RAID Groups

Mix of Drive Types in RAID Group	Allowed?
SAS HDD + SATA HDD	Yes
SAS SSD + SATA SSD	Yes
HDD + SSD	No

Mixing Drive Types in RAID Groups

For the best performance, follow these guidelines:

- Use either all SAS or all SATA drives in a RAID group.
- Use the same capacity for each drive in the RAID group.
- Never mix HDDs and SSDs in the same RAID group.

RAID Controller Cabling

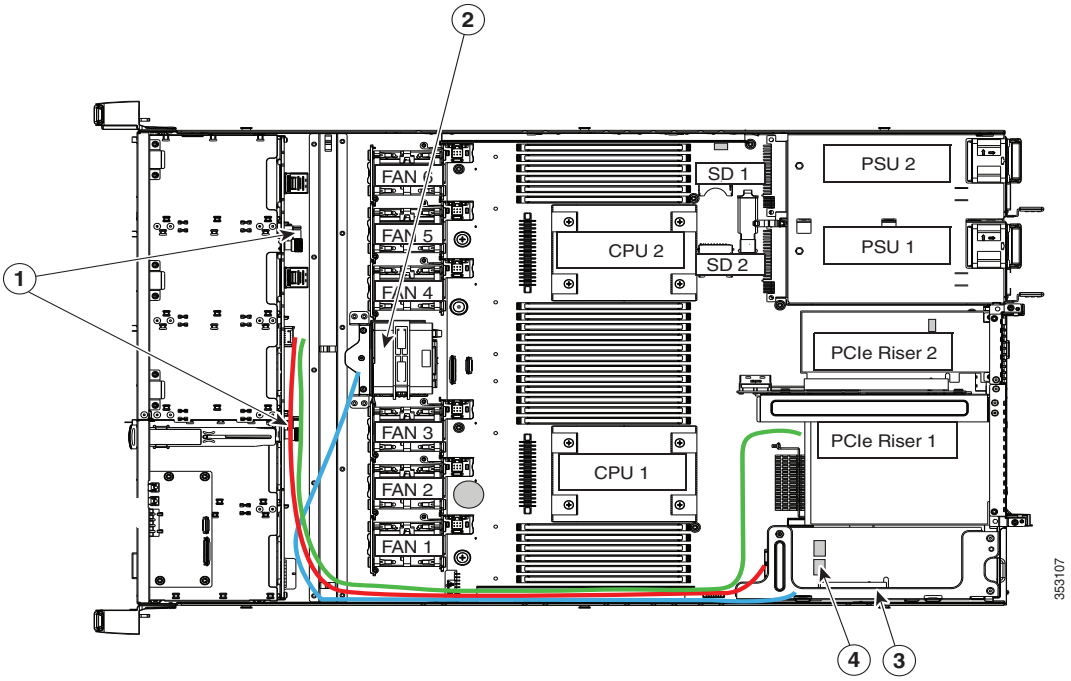
This section includes the following topics:

Cable Routing

The RAID controller connectors in this node are shown in Figure C-1.

- The red line shows the recommended cable routing path from the Cisco modular RAID controller card or the embedded SATA RAID motherboard connectors to the drive backplane. Cable guides on the chassis wall help route the cables.
- The green line shows the recommended cable routing path from an HBA card in slot 1 to the drive backplane.

Figure C-1 RAID Controller Connectors



1	SAS/SATA connectors on the drive backplane	**3**	Cisco modular RAID controller riser (dedicated internal riser)
2	SCPM mounting bracket	**4**	Embedded RAID mini-SAS connectors on motherboard (two)

Cisco HX220c M4 Node Cabling

This section contains the following topics:

SFF 8-Drive Backplane Cabling

The cable connections required for each type of controller are as follows:

Embedded RAID

This option can control up to eight SATA drives.

The required UCS-220CBLSR8= cable kit has two mini-SAS cables (mini-SAS HD to mini-SAS iPass connectors).

Step 1 Connect mini-SAS cable 1 from the PORT A motherboard connector to the PORT A connector on the backplane.

Step 2 Connect mini-SAS cable 2 from the PORT B motherboard connector to the PORT B connector on the backplane.

Cisco UCS 12G Modular HBA

This non-RAID option can control up to eight SAS/SATA drives.

The required UCS-220CBLMR8= cable kit has one Y-cable with a mini-SAS HD double connector on one end and two mini-SAS HD single connectors on the other end.

Step 1 Connect the mini-SAS double connector to the modular HBA card.

Step 2 Connect single connector PORT A to the PORT A connector on the backplane.

Step 3 Connect single connector PORT B to the PORT B connector on the backplane.

Embedded SATA RAID Controllers

Note VMware ESX/ESXi or any other virtualized environments are not supported for use with the embedded MegaRAID controller. Hypervisors such as Hyper-V, Xen, or KVM are also not supported for use with the embedded MegaRAID controller.

This node includes an embedded MegaRAID controller that can control up to eight SATA-only drives.

This section contains the following topics:

Embedded SATA RAID Controller Requirements

The embedded SATA RAID controller hub requires the following items:

- Mini-SAS cables:
  - SFF 8-drive: UCS-220CBLSR8=
- The embedded SATA RAID controller must be enabled in the system BIOS.
- (Optional) A SATA RAID 5 key module.

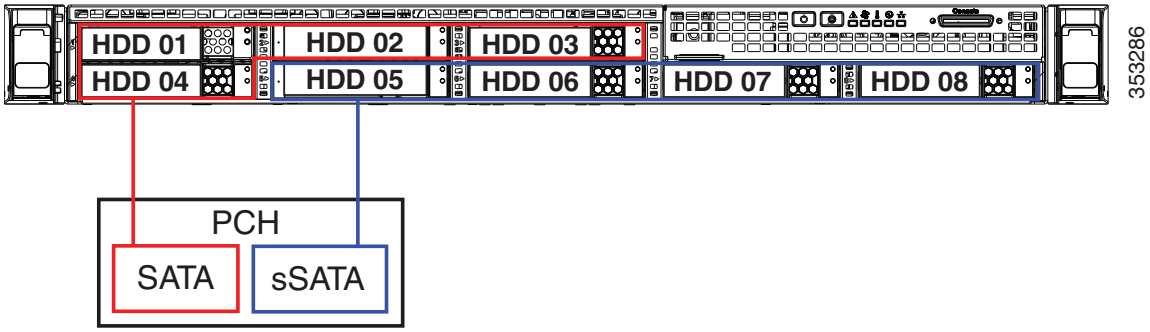
  This optional module can be installed to a motherboard header to add SATA RAID 5 support.
- (Optional) LSI MegaSR drivers for Windows or Linux.

Embedded SATA RAID: Two SATA Controllers

The embedded RAID Patsburgh controller hub (PCH) is split into two controllers: SATA and sSATA (secondary SATA). These two controllers are seen as separate RAID controllers in the Cisco IMC interface and are configurable separately.

- The first SATA controller controls drives 1–4; the secondary sSATA controller controls drives 5–8.
- When configuring RAID groups, you cannot create a group that spans more than four drives.
  - The first SATA controller can control a RAID group of up to four drives, comprised only of drives 1–4.
  - The secondary sSATA controller can control a RAID group of up to four drives, comprised only of drives 5–8. See Figure C-2.

Figure C-2 Embedded RAID Controller Drive Groups



- See Enabling or Disabling the Embedded SATA RAID Controller in the BIOS, page C-8 for instructions on enabling the two SATA controllers.
- Each controller is listed separately in the BIOS. You can select the boot order of the controllers in the BIOS (use the **Boot Options** tab in the BIOS Setup Utility).

Note To set boot order for virtual drives, use the LSI Embedded RAID Configuration Utility. See Launching the LSI Embedded RAID Configuration Utility, page C-10.

Embedded SATA RAID Controller Considerations

Note the following considerations:

- The default setting for this embedded controller hub is SATA RAID 0, 1, and 10 support for up to eight SATA drives (in two groups of four drives).
- You can upgrade to SATA RAID 0, 1, 5, 10 support for up to eight SATA drives (in two groups of four drives) by installing a RAID 5 key module on the motherboard. See Installing a Software RAID 5 Key Module for Embedded RAID 5 Support, page C-8.
- When you order the node with this embedded controller, the controller is enabled in the BIOS. Instructions for enabling the controller are included for the case in which a node is reset to defaults (Disabled). See Enabling or Disabling the Embedded SATA RAID Controller in the BIOS, page C-8.
- You cannot downgrade from using a hardware RAID controller card to using the software RAID embedded controller (see RAID Controller Cabling, page C-4).

Caution Data migration from software RAID (embedded RAID) to hardware RAID (a controller card) is not supported and could result in data loss. Migrations from software RAID to hardware RAID are supported only before there is data on the drives, or when there are no drives in the node (see RAID Controller Cabling, page C-4).

- The required drivers for this controller are already installed and ready to use with the LSI SWRAID Configuration Utility. However, if you will use this controller with Windows or Linux, you must download and install additional drivers for those operating nodes. See Installing LSI MegaSR Drivers For Windows and Linux, page C-11.

Installing a Software RAID 5 Key Module for Embedded RAID 5 Support

The software RAID 5 key module contains a chip on a small circuit board. This module attaches to a two-pin motherboard header. This chip upgrades support to add embedded SATA RAID 5 support.

To install a RAID 5 key module, see Installing a Software RAID 5 Key Module for Embedded RAID 5 Support, page C-8.

Enabling or Disabling the Embedded SATA RAID Controller in the BIOS

Note The default setting in the BIOS for the embedded controller is disabled.

When you enable this controller, both the primary (SATA) and secondary (sSATA) controllers are enabled.

Enabling SATA Mode and Selecting Option ROM Mode

Step 1 Set the SATA mode for managing the two boot drives:

a. Boot the node and press **F2** when prompted to enter the BIOS Setup utility.

b. Choose the **Advanced** tab, and then choose **LOM and PCIe Slots Configuration**.

c. Select **PCH SATA Mode** and then choose one of the options from the dialog:

- AHCI—Not used at this time.
- Disabled—The embedded RAID controller is disabled.
- LSI SW RAID—In supported node versions, you can manage the internal SSD boot drives or the front-facing drives by using the node's embedded SATA RAID controller.

Note Before you change from LSI SW RAID mode to AHCI mode, delete all the RAID volumes configured in the connected physical drives.

d. If you selected LSI SW RAID mode and you want to set the option ROM mode, continue with the next step. If not, skip to Step 3.

Note There is no option ROM mode setting in AHCI SATA mode.

Step 2 Optional: Set the SATA option ROM mode for the two boot drives (only with LSI SW RAID SATA mode):

a. Choose the **Advanced** tab, and then choose **LOM and PCIe Slots Configuration**.

b. Select **PCH SATA OPROM Mode** and then choose one of the options from the dialog:

- Enabled—You can boot from these boot drives. You can use the UEFI management interface or the free-standing legacy management utility.
- Disabled—You cannot boot from these boot drives.
- UEFI Only—Select this to enable booting but manage RAID only by using the UEFI version of the LSI utility that is built into the system BIOS. See Launching the LSI Embedded RAID Configuration Utility, page C-10.
- Legacy Only—Select this enable booting but manage RAID only by using the free-standing version of the LSI utility. See Launching the LSI Embedded RAID Configuration Utility, page C-10.

Step 3 Press **F10** to save your changes and exit the utility.

Disabling the Embedded RAID Controller in the BIOS

Step 1 Boot the node and press **F2** when prompted to enter the BIOS Setup Utility.

Step 2 Select the **Advanced** tab, and then select **LOM and PCIe Slots Configuration**.

Step 3 Set PCH SATA Mode to **Disabled**.

Step 4 Press **F10** to save your changes and exit the utility.

Launching the LSI Embedded RAID Configuration Utility

Launch the LSI utility by pressing **Ctrl-M** when you see the prompt during node boot.

For information about using the Embedded MegaRAID software to configure your disk arrays, see the LSI Embedded MegaRAID Software User Guide.

Installing LSI MegaSR Drivers For Windows and Linux

Note The required drivers for this controller are already installed and ready to use with the LSI software RAID Configuration Utility. However, if you will use this controller with Windows or Linux, you must download and install additional drivers for those operating systems.

This section explains how to install the LSI MegaSR drivers for the following supported operating systems:

- Microsoft Windows Server
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your node release.

This section contains the following topics:

Downloading the LSI MegaSR Drivers

The MegaSR drivers are included in the C-Series driver ISO for your node and OS. Download the drivers from Cisco.com.

Step 1 Find the drivers ISO file download for your node online and download it to a temporary location on your workstation:

a. See the following URL: **http://www.cisco.com/cisco/software/navigator.html**
b. Click **Unified Computing and Servers** in the middle column.
c. Click **Cisco UCS C-Series Rack-Mount Standalone System Software** in the right-hand column.
d. Click your model of node in the right-hand column.
e. Click **Unified Computing System (UCS) Drivers**.
f. Click the release number that you are downloading.
g. Click **Download** to download the drivers' ISO file.
h. Verify the information on the next page, and click **Proceed With Download**.
i. Continue through the subsequent screens to accept the license agreement and then browse to a location where you want to save the drivers' ISO file.

Microsoft Windows Driver Installation

This section describes how to install the LSI MegaSR driver in a Windows installation.

This section contains the following topics:

Windows System 2008R2 Driver Installation

The Windows operating system automatically adds the driver to the registry and copies the driver to the appropriate directory.

Step 1 Create a RAID drive group using the LSI Software RAID Configuration Utility before you install this driver for Windows. Launch this utility by pressing **Ctrl-M** when `LSI SWRAID` is shown during the BIOS POST.

Step 2 Download the Cisco UCS C-Series drivers' ISO, as described in Downloading the LSI MegaSR Drivers, page C-11.

Step 3 Prepare the drivers on a USB thumb drive:

a. Burn the ISO image to a disk.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

/<OS>/Storage/Intel/C600/

c. Expand the Zip file, which contains the folder with the MegaSR driver files.

d. Copy the expanded folder to a USB thumb drive.

Step 4 Start the Windows driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the node and then insert the first Windows installation disk into the drive. Skip to Step 6.
- To install from remote ISO, log in to the node's Cisco IMC interface and continue with the next step.

Step 5 Launch a Virtual KVM console window and click the **Virtual Media** tab.

a. Click **Add Image** and browse to select your remote Windows installation ISO file.

b. Check the check box in the Mapped column for the media that you just added, and then wait for mapping to complete.

Step 6 Power cycle the node.

Step 7 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 8 On the Boot Manager window, choose the physical disk or virtual DVD and press **Enter**. The Windows installation begins when the image is booted.

Step 9 Press **Enter** when you see the prompt, "Press any key to boot from CD."

Step 10 Observe the Windows installation process and respond to prompts in the wizard as required for your preferences and company standards.

Step 11 When Windows prompts you with "Where do you want to install Windows," install the drivers for embedded MegaRAID:

a. Click **Load Driver**. You are prompted by a Load Driver dialog box to select the driver to be installed.

b. Connect the USB thumb drive that you prepared in Step 3 to the target node.

c. On the Windows Load Driver dialog that you opened in Step a, click **Browse**.

d. Use the dialog box to browse to the location of the drivers folder on the USB thumb drive, and then click **OK**.

   Windows loads the drivers from the folder and when finished, the driver is listed under the prompt, "Select the driver to be installed."

e. Click **Next** to install the drivers.

Updating the Windows Driver

Step 1 Click **Start**, point to **Settings**, and then click **Control Panel**.

Step 2 Double-click **Server**, click the **Hardware** tab, and then click **Device Manager**. Device Manager starts.

Step 3 In Device Manager, double-click **SCSI and RAID Controllers**, right-click the device for which you are installing the driver, and then click **Properties**.

Step 4 On the Driver tab, click **Update Driver** to open the Update Device Driver wizard, and then follow the wizard instructions to update the driver.

Linux Driver Installation

This section explains the steps to install the embedded MegaRAID device driver in a Red Hat Enterprise Linux installation or a SUSE Linux Enterprise Server installation.

This section contains the following topics:

Obtaining the Driver Image File

See Downloading the LSI MegaSR Drivers, page C-11 for instructions on obtaining the drivers. The Linux driver is offered in the form of dud-[*driver version*].img, which is the boot image for the embedded MegaRAID stack.

Note The LSI MegaSR drivers that Cisco provides for Red Hat Linux and SUSE Linux are for the original GA versions of those distributions. The drivers do not support updates to those OS kernels.

Preparing Physical Installation Disks For Linux

This section describes how to prepare physical Linux installation disks from the driver image files, using either the Windows operating system or the Linux operating system.

Note The driver image is too large for a floppy disk, so use a USB thumb drive instead.

Note Alternatively, you can mount the dud.img file as a virtual floppy disk, as described in the installation procedures.

Preparing Physical Installation Disks with the Windows Operating System

Under Windows, you can use the RaWrite floppy image-writer utility to create disk images from image files.

Step 1 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-11 and save it to your Windows system that has a diskette drive.

Step 2 Extract the dud.img file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

/<OS>/Storage/Intel/C600/

c. Expand the Zip file, which contains the folder with the driver files.

Step 3 Copy the driver update disk image dud-[driver version].img and your file raw write.exe to a directory.

Note RaWrite is not included in the driver package.

Step 4 If necessary, use this command to change the filename of the driver update disk to a name with fewer than eight characters: **copy dud-[***driver version***].img dud.img**

Step 5 Open the DOS Command Prompt and navigate to the directory where raw write.exe is located.

Step 6 Enter the following command to create the installation diskette: **raw write**

Step 7 Press **Enter**.

You are prompted to enter the name of the boot image file.

Step 8 Enter: **dud.img**

Step 9 Press **Enter**.

You are prompted for the target disk.

Step 10 Insert a floppy disk into the system and enter: **A:**

Step 11 Press **Enter**.

Step 12 Press **Enter** again to start copying the file to the diskette.

Step 13 After the command prompt returns and the floppy disk drive LED goes out, remove the disk.

Step 14 Label the diskette with the image name.

Preparing Installation Disks with a Linux Operating System

Under Red Hat Linux and SUSE Linux, you can use a driver disk utility to create disk images from image files.

Note The driver image is too large for a floppy disk, so use a USB thumb drive instead.

Step 1 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-11 and save it to your Linux system that has a disk drive.

Step 2 Extract the dud.img file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

/<OS>/Storage/Intel/C600/

c. Expand the Zip file, which contains the folder with the driver files.

Step 3 Copy the driver update disk image dud-[driver version].img to your Linux system.

Step 4 Insert a blank USB thumb drive into a port on your Linux system.

Step 5 Create a directory and mount the DUD image to that directory:

mkdir <*destination_folder*>

mount -oloop <*driver_image*> <*destination_folder*>

Step 6 Copy the contents in the directory to your USB thumb drive.

Installing the Red Hat Linux Driver

Note This node supports Red Hat Linux 6.5 or later.

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your node release.

This section describes the fresh installation of the Red Hat Enterprise Linux device driver on nodes with the embedded MegaRAID stack.

Step 1 Create a RAID drive group using the LSI Software RAID Configuration utility before you install this driver for the OS. Launch this utility by pressing **Ctrl-M** when `LSI SWRAID` is shown during the BIOS POST.

Step 2 Prepare the dud.img file using one of the following methods:

- To install from a physical disk: Use one of the procedures in Preparing Physical Installation Disks For Linux, page C-14.
  Then return to Step 4 of this procedure.
- To install from a virtual floppy disk: Download and save the Cisco UCS C-Series drivers' ISO, as described in Downloading the LSI MegaSR Drivers, page C-11.
  Then continue with the next step.

Step 3 Extract the dud.img file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

/<OS>/Storage/Intel/C600/

c. Copy the dud-<*driver version*>.img file to a temporary location on your workstation.

Step 4 Start the Linux driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the node and then insert the first RHEL installation disk into the drive.
  Then continue with Step 6.
- To install from remote ISO, log in to the node's Cisco IMC interface. Then continue with the next step.

Step 5 Launch a Virtual KVM console window and click the **Virtual Media** tab.

a. Click **Add Image** and browse to select your remote RHEL installation ISO file.

b. Click **Add Image** again and browse to select your dud.img file.

c. Check the check boxes in the Mapped column for the media that you just added, then wait for mapping to complete.

Step 6 Power cycle the node.

Step 7 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 8 On the Boot Manager window, select the physical disk or virtual DVD and press **Enter**.

The RHEL installation begins when the image is booted.

Step 9 Enter one of the following commands at the boot prompt:

- For RHEL 6.*x* (32- and 64-bit), enter:
  linux dd blacklist=isci blacklist=ahci nodmraid noprobe=<ata*drive number*>
- For RHEL 7.x (32- and 64-bit), enter:
  linux dd modprobe.blacklist=ahci nodmraid

Note The **noprobe** values depend on the number of drives. For example, to install RHEL 6.5 on a RAID 5 configuration with three drives, enter
linux dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1 noprobe=ata2

Step 10 Press **Enter**.

The prompt asks whether you have a driver disk.

Step 11 Use the arrow key to choose **Yes**, and then press **Enter**.

Step 12 Choose **fd0** to indicate that you have a floppy disk with the driver on it.

Step 13 Do one of the following actions:

- If you prepared the IMG file on a physical diskette in Step 2, connect an external disk drive to the target system and then insert the disk in the A:/ drive and press **Enter**.
- If you mapped the IMG file as a virtual floppy in Step 5, choose the location of the virtual floppy.

The installer locates and loads the driver for your device. The following message appears:

Loading megasr driver...

Step 14 Follow the Red Hat Linux installation procedure to complete the installation.

Step 15 Reboot the node.

Installing the SUSE Linux Enterprise Server Driver

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your system release.

This section describes the installation of the SUSE Linux Enterprise Server driver on a node with the embedded MegaRAID stack.

Step 1 Create a RAID drive group using the LSI SWRAID Configuration utility before you install this driver for the OS. Launch this utility by pressing **Ctrl+M** when `LSI SWRAID` is shown during the BIOS POST.

Step 2 Prepare the dud.img file using one of the following methods:

- To install from a physical disk, use one of the procedures in Preparing Physical Installation Disks For Linux, page C-14.
  Then return to Step 4 of this procedure.
- To install from a virtual floppy disk, download and save the Cisco UCS C-Series drivers' ISO, as described in Downloading the LSI MegaSR Drivers, page C-11.
  Then continue with the next step.

Step 3 Extract the dud.img file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

/<OS>/Storage/Intel/C600/

c. Copy the dud-<*driver version*>.img file to a temporary location on your workstation.

Step 4 Start the Linux driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the node and then insert the first RHEL install disc into the drive. Skip to Step 6.
- To install from remote ISO, log in to the node's Cisco IMC interface and continue with the next step.

Step 5 Launch a Virtual KVM console window and click the **Virtual Media** tab.

a. Click **Add Image** and browse to select your remote RHEL installation ISO file.

b. Click **Add Image** again and browse to select your dud.img file.

c. Check the check box in the Mapped column for the media that you just added, and then wait for mapping to complete.

Step 6 Power cycle the node.

Step 7 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 8 On the Boot Manager window, select the physical disk or virtual DVD and press **Enter**. The SLES installation begins when the image is booted.

Step 9 When the first SLES screen appears, choose **Installation**.

Step 10 Enter one of the following in the Boot Options field:

- For SLES 11 and SLES 11 SP1 (32- and 64-bit), enter: **brokenmodules=ahci**
- For SLES 11 SP2 (32-and 64-bit), enter: **brokenmodules=ahci brokenmodules=isci**
- For SLES 12, enter: **brokenmodules=ahci**

Step 11 Press **F6** for the driver and choose **Yes**.

Step 12 Do one of the following actions:

- If you prepared the IMG file on a physical disk in Step 2, insert the USB thumb drive to the target node and then insert the disk in the A:/ drive and press **Enter**.
- If you mapped the IMG file as a virtual floppy in Step 5, choose the location of the virtual floppy.

"Yes" appears under the F6 Driver heading.

Step 13 Press **Enter** to choose Installation.

Step 14 Press **OK**.

The following message is displayed: `LSI Soft RAID Driver Updates added.`

Step 15 At the menu, choose the driver update medium and press the **Back** button.

Step 16 Continue and complete the installation process by following the prompts in the installation wizard.

Restoring RAID Configuration After Replacing a RAID Controller

When you replace a RAID controller, the RAID configuration that is stored in the controller is lost.

Step 1 Replace your RAID controller. See Replacing a PCIe Card, page 3-42.

Step 2 If this was a full chassis swap, replace all drives into the drive bays, in the same order that they were installed in the old chassis.

Step 3 Reboot the system. The RAID configuration is imported automatically.

Step 4 Watch the subsequent screens for confirmation that your RAID configuration was imported correctly.

- If you see the following message, your configuration was successfully imported. The LSI virtual drive is also listed among the storage devices.

  ```
  N Virtual Drive(s) found on host adapter.
  ```

- If you see the following message, your configuration was not imported. This situation can happen if you do not press F quickly enough when prompted. In this case, reboot the system and try the import operation again when you are prompted to press F.

  ```
  0 Virtual Drive(s) found on host adapter.
  ```

For More Information

The LSI utilities have help documentation for more information about using the utilities.

For basic information about RAID and for using the utilities for the RAID controller cards that are supported in Cisco systems, see the Cisco UCS Servers RAID Guide.

Full Avago Technologies/LSI documentation is also available:

- For hardware SAS MegaRAID—Avago Technologies/LSI 12 Gb/s MegaRAID SAS Software User's Guide, Rev. F
- For software embedded MegaRAID—LSI Embedded MegaRAID Software User Guide

APPENDIX D

Installation for Cisco UCS Manager Integration

The Cisco UCS Manager integration instructions have been moved to the integration guides found here:

Cisco UCS C-Series Server Integration with UCS Manager Guides

Refer to the guide that is for the version of Cisco UCS Manager that you are using.

Also refer to the release notes for Cisco UCS Manager software and C-Series software for any special considerations regarding integration in your release.

- Cisco UCS Manager Release Notes
- Cisco C-Series Software Release Notes