Cisco Learning Product

Data Center Unified Computing Implementation

Volume 1

Version 4.0

DCUCI

Data Center Unified Computing Implementation

Volume 1

Version 4.0

Student Guide

Text Part Number: 97-3020-01

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.**

Student Guide

Printed in Canada

Students, this letter describes important course evaluation access information!

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco Systems is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions; therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. We would appreciate a few minutes of your time to complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,

Cisco Systems Learning

Table of Contents

Volume 1

DCUCI

Course Introduction

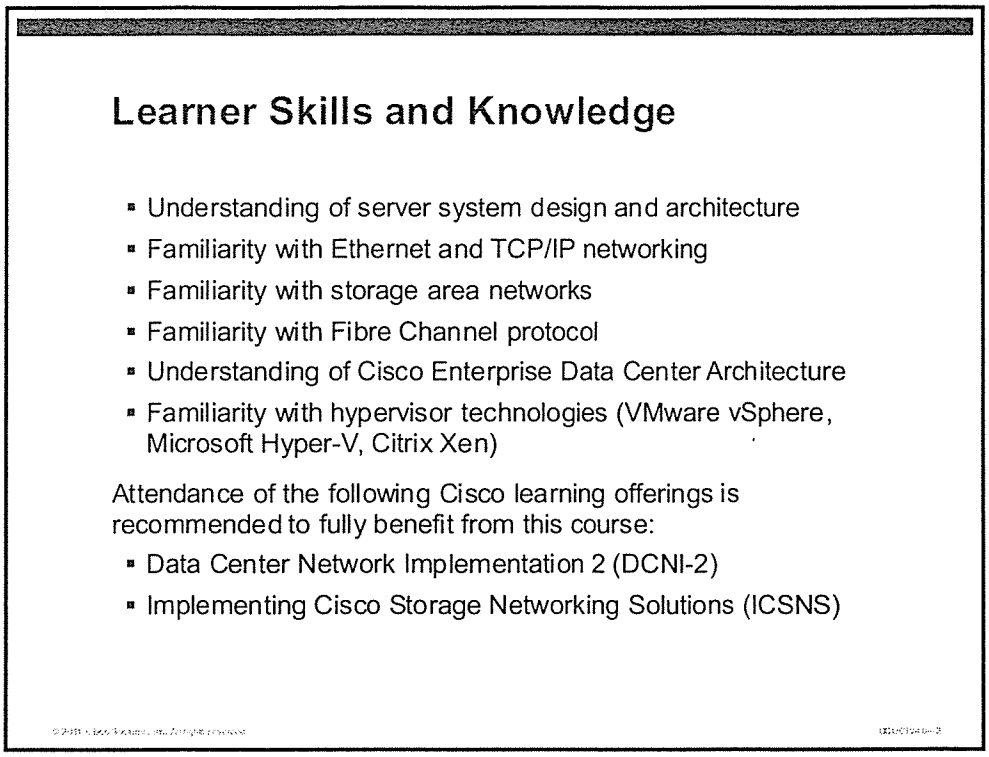
Overview

This intensive five-day, hands-on course focuses on Cisco Unified Computing System (UCS) deployment and operations. You will learn how to install, configure, manage, and troubleshoot Cisco UCS B-Series blade servers and C-Series rack-mount servers with consolidated I/O networking for LAN and SAN connectivity, and how to virtualize server properties to enable simple and rapid mobility of server images between physical servers.

In labs, you will practice implementing a realistic, hierarchical management model, configuring fault tolerance (at the LAN, SAN, and server network interface card [NIC] level), backing up and restoring system configurations, and using the built-in monitoring and troubleshooting tools in Cisco UCS Manager and the Cisco Integrated Management Controller. You will also install and configure the Cisco Nexus 1000V Distributed Virtual Switch and VMware Pass-Through Switching (PTS), leveraging VMware vSphere 4.1 on Cisco UCS B-Series and C-Series infrastructure.

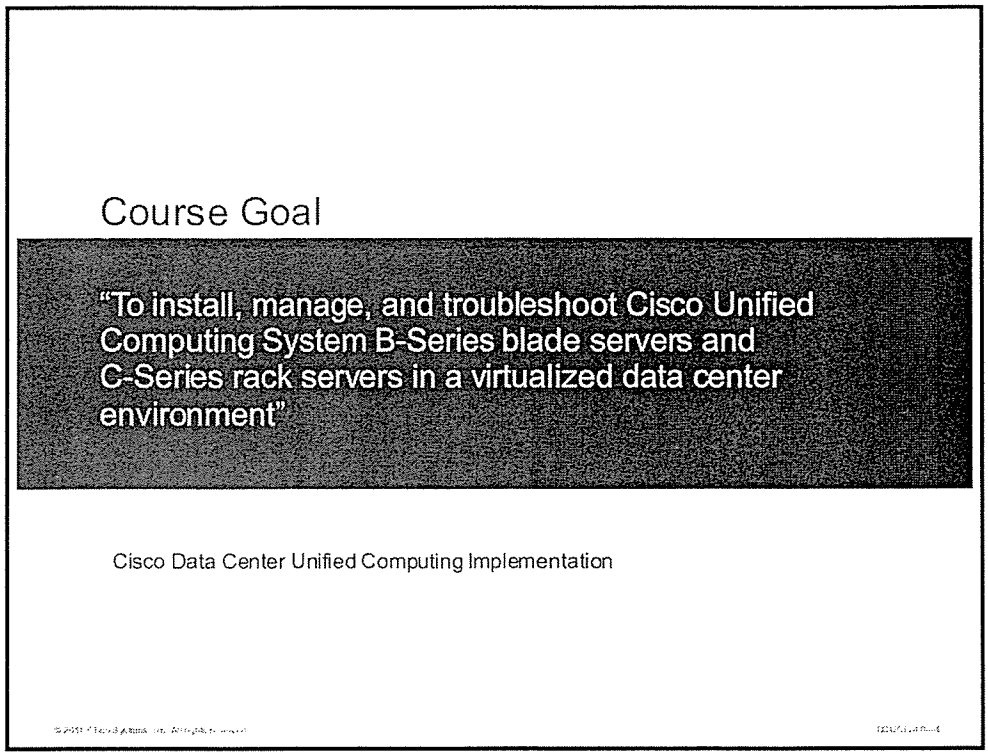
Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.



Course Goal and Objectives

This topic describes the course goal and objectives.

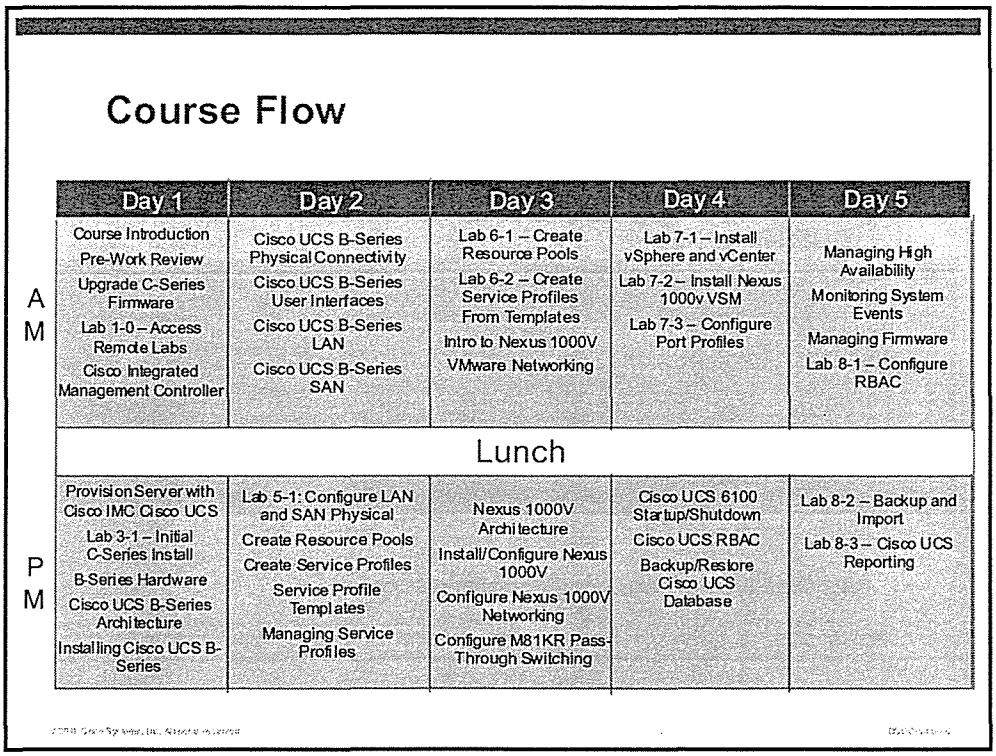


Upon completing this course, you will be able to meet these objectives:

- Explain how Cisco Unified Computing System addresses key management challenges in data center server environments
- Describe the Cisco UCS B-Series and C-Series system architectures, hardware components, and field-installable options
- Explain how to connect to and manage Cisco Unified Computing System components
- Configure Cisco UCS B-Series blade servers with Cisco UCS Manager
- Configure Cisco UCS C-Series blade servers with Cisco Integrated Management Controller
- Explain the connectivity requirements for the Cisco UCS platform
- Configure server profiles to allocate physical resources
- Configure maintenance tasks
- Configure high availability at the LAN, SAN, and server NIC level
- Identify common deployment scenarios for Cisco UCS
- Troubleshoot common LAN and SAN connectivity issues
- Troubleshoot service profile issues
- Configure Cisco Nexus 1000V in a VMware vSphere 4.1 environment
- Configure Cisco UCS Manager to support VMware PTS
- Configure Cisco UCS Manager to support VMware DirectPath I/O

Course Flow

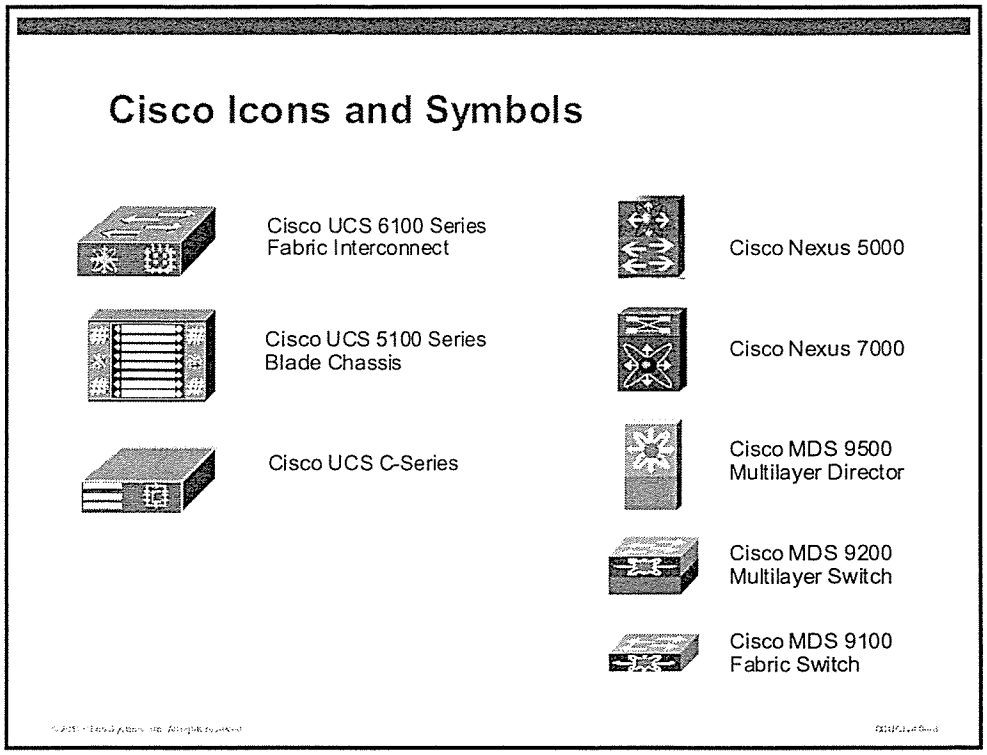
This topic presents the suggested flow of the course materials.

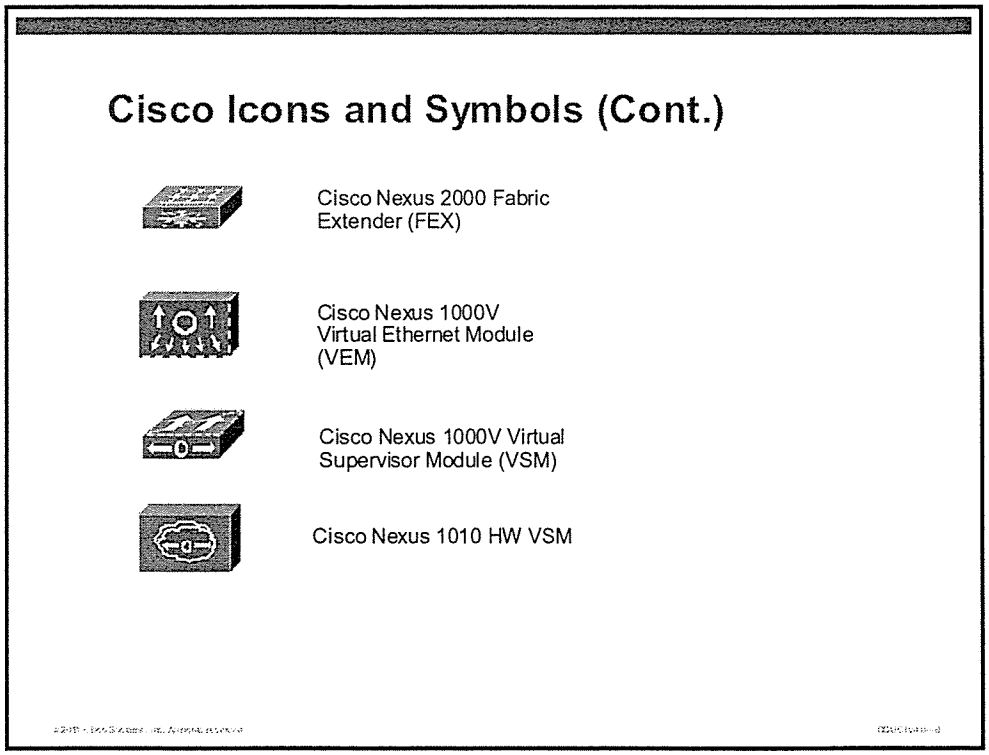


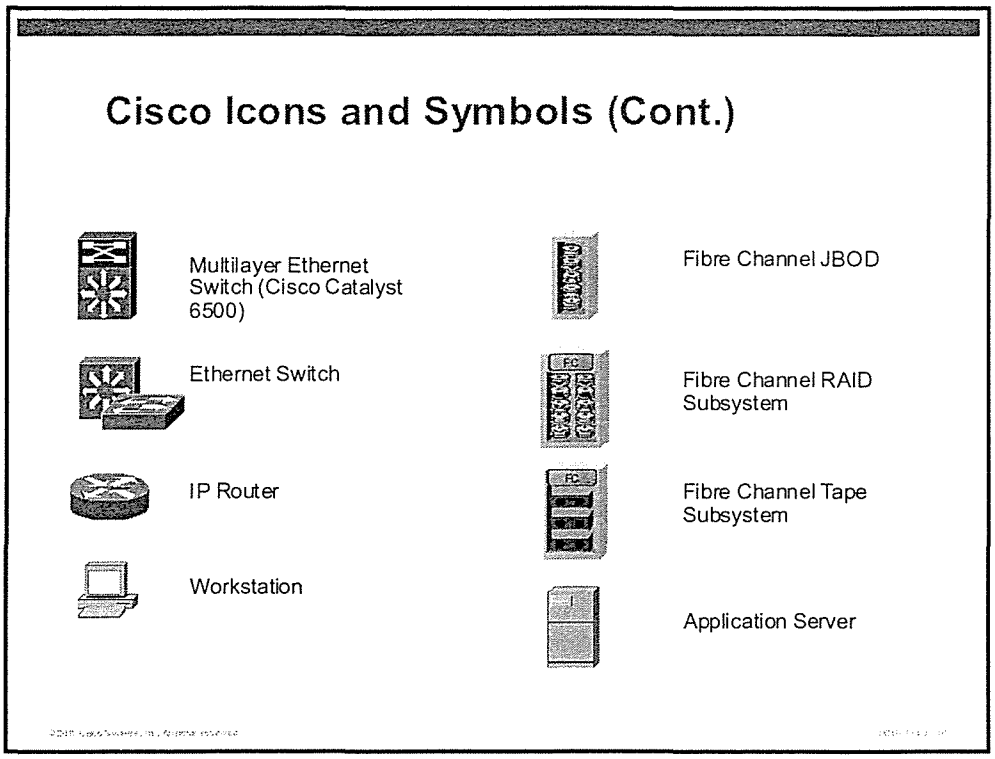
The schedule reflects the recommended topic flow for this course. This structure allows enough time for the instructor to present the course information and for you to perform all lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

This topic presents the Cisco icons and symbols that are used in this course.





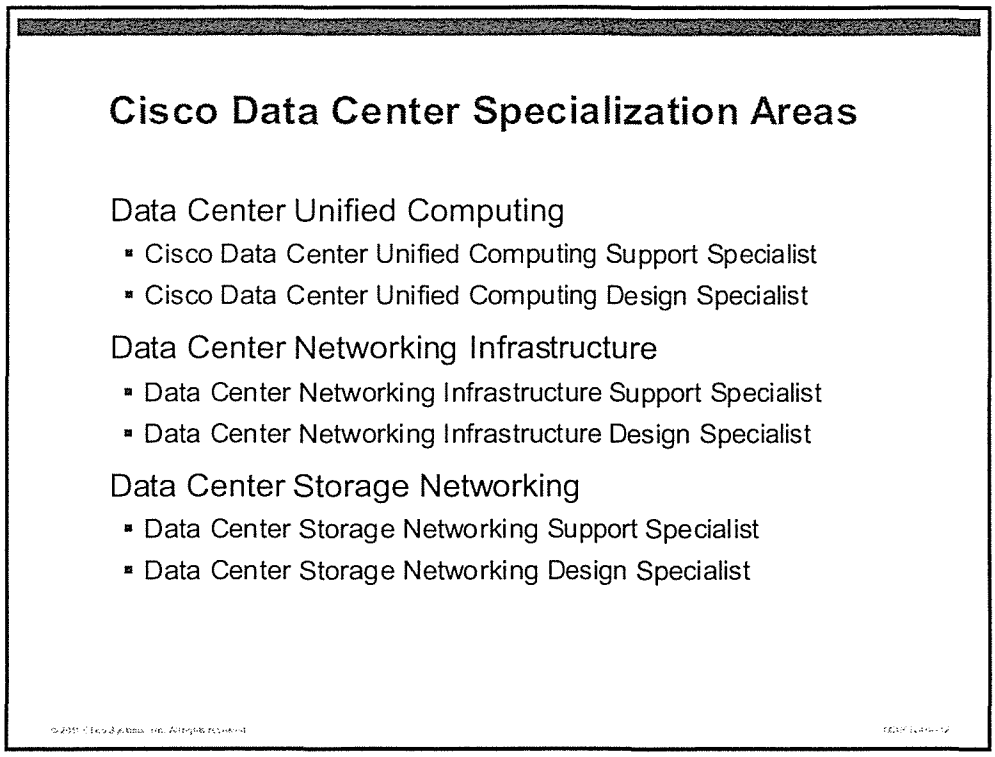


Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_%28ITA%29.

Your Training Curriculum

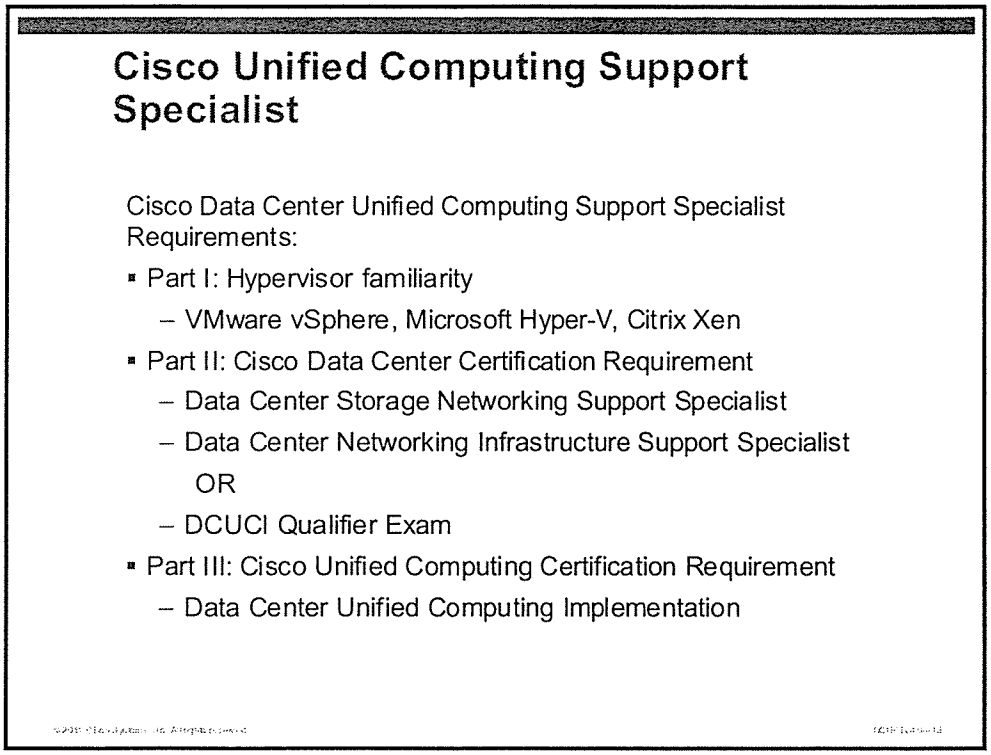
This topic presents Cisco data center certification options available for students to pursue.



For more information on certifications, go to http://www.cisco.com/go/certifications.

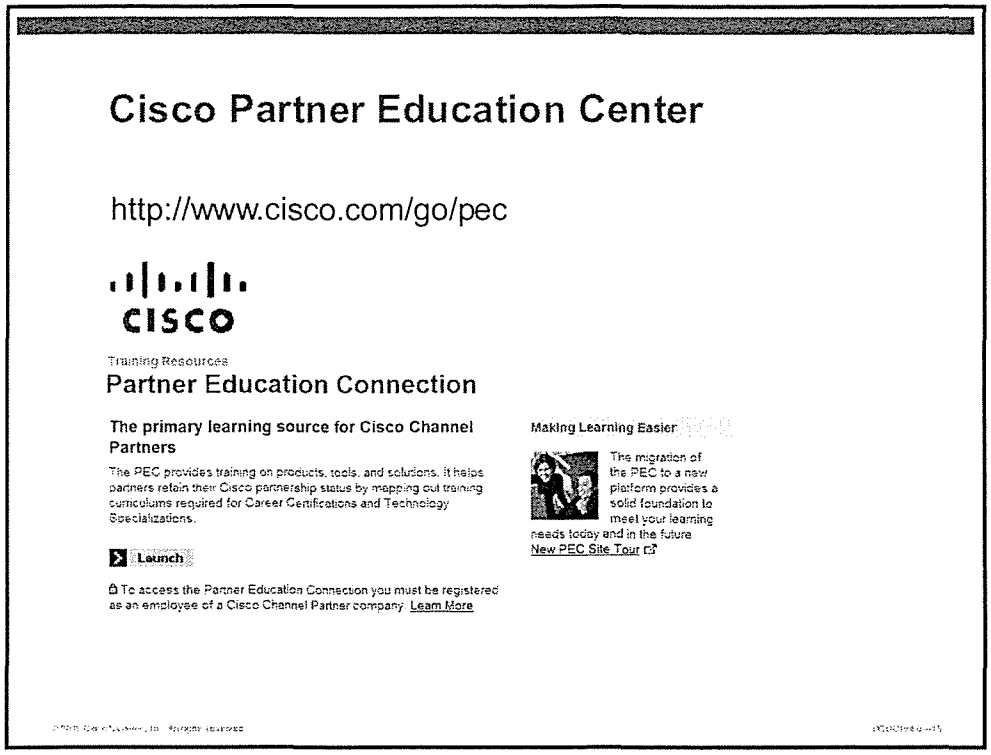
Training Curriculum for Cisco Unified Computing Support Specialist

This subtopic presents the exam requirements to achieve Cisco Data Center Unified Computing Support Specialist certification.

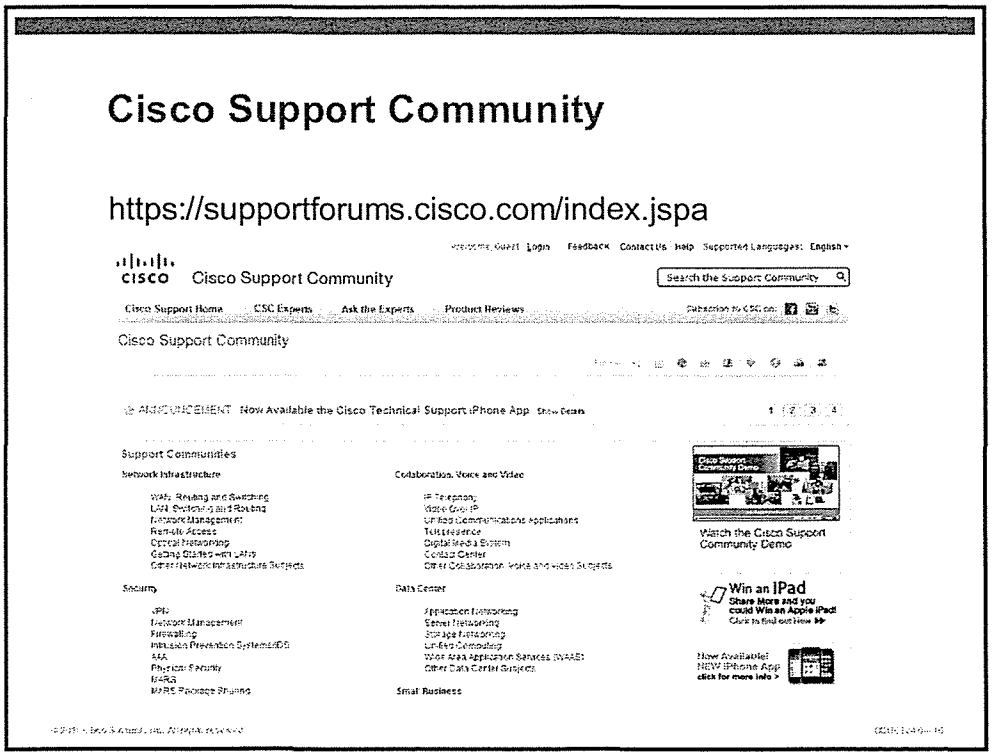


Cisco Online Resources

This topic introduces the Partner Education Center, where you can attend self-paced e-learning about most of the Cisco product lines.



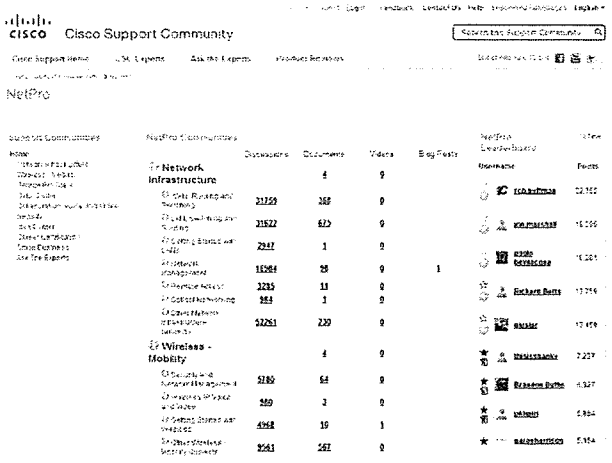
You can also use the Cisco Support Community to research Cisco solutions that are presented to the Cisco community at large.



The Cisco NetPro Forum is another resource where you can ask technical questions and find out how other engineers have solved challenges in their networks.

Cisco NetPro Forums

https://supportforums.cisco.com/community/netpro



Cisco Learning Network

http://www.cisco.com/go/learnnetspace

Introductions

This topic conveys general classroom administration information.

General Administration

Class-related

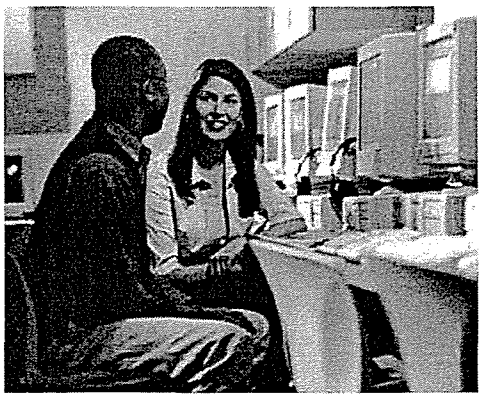
- Sign-in sheet
- Length and times
- Break and lunch room locations
- Attire
- Cell phones and pagers

Facilities-related

- Participant materials
- Site emergency procedures
- Restrooms
- Telephones and faxes

Student Introductions

- Your name
- Your company
- Prerequisite skills
- Brief history
- Objective



Module 1

Review of Data Center Unified Computing Implementation E-Learning

Overview

This module enables the instructor to gauge your comprehension of the DCUCI e-learning material.

Module Objectives

Upon completing this module, you will be able to demonstrate your understanding of the foundational topics that are covered in the DCUCI e-learning presentations. This ability will allow the instructor to adjust the level of lecture detail in subject areas and recommend a supplemental study plan, if necessary.

The review will encompass the following subject areas:

- Challenges of data center server management
- Cisco Unified Computing System
- Cisco UCS C-Series hardware components
- Cisco UCS C-Series hardware installation
- Cisco UCS B-Series hardware components
- Cisco UCS B-Series architecture and features
- Cisco UCS use cases
- Server virtualization
- Cisco Nexus 1000V
- VMware Ethernet networking
- Cisco Nexus 1000V architecture

Lesson 1

Brief Survey of Cisco Data Center Unified Computing Implementation E-Learning

Overview

The Cisco Data Center Unified Computing Implementation (DCUCI) course is designed to satisfy the needs of a diverse range of skills and experience. Approximately 10 hours of Cisco Unified Computing System (UCS) and virtualization foundational topics are included in an e-learning format. It is recommended that all students watch the e-learning component before attending the instructor-led training (ILT). Exam topics for the DCUCI certification exam include material from the ILT and e-learning materials.

Objectives

Upon completing this lesson, you will be able to demonstrate your mastery of Cisco UCS and virtualization fundamentals. The review will encompass the following subject areas:

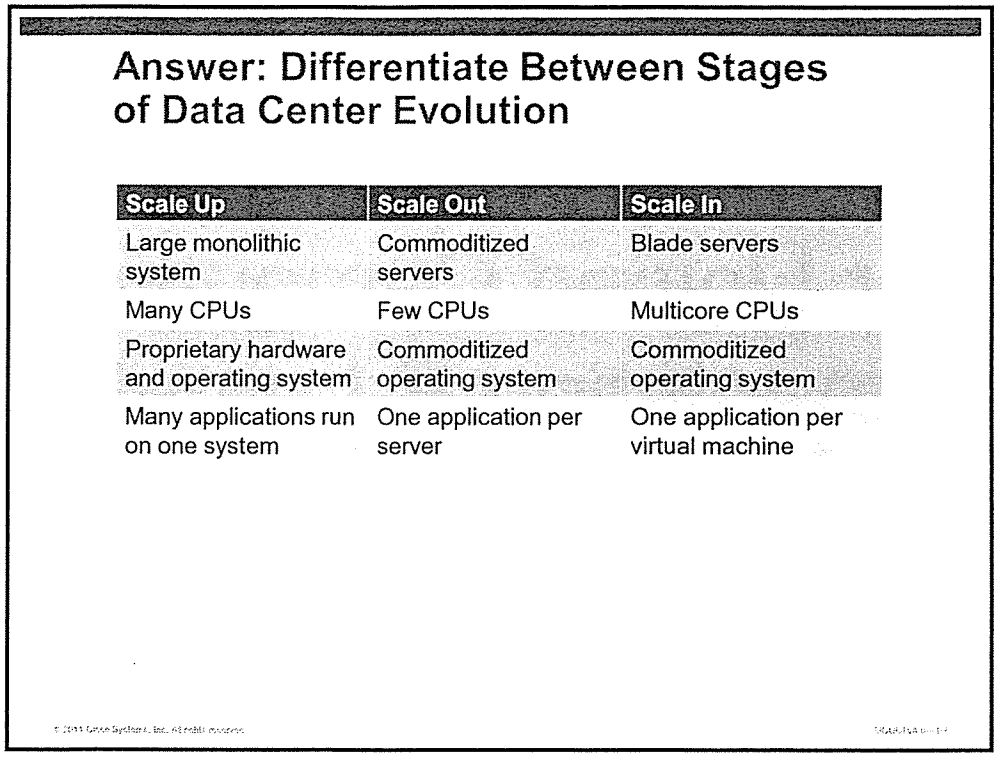
- Describe challenges of data center server management
- Review Cisco Unified Computing System
- Review Cisco UCS C-Series hardware components
- Review Cisco UCS C-Series hardware installation
- Review Cisco UCS B-Series hardware components
- Review Cisco UCS B-Series architecture and features
- Review Cisco UCS use cases
- Review Server virtualization
- Describe Cisco Nexus 1000V Series Switches
- Review VMware Ethernet networking
- Review Cisco Nexus 1000V architecture

Reviewing Evolution of Cisco UCS

This topic describes the evolution of Cisco UCS.

Differentiate Between Stages of Data Center Evolution

This subtopic reviews data center evolution.



Over the last 20 years, the data center has undergone dramatic changes. Some of the underlying reasons for these changes are based on server evolution. Server evolution can be categorized by the hardware and methodology that are used to accommodate the growing demands of applications and users.

To illustrate the server evolution, the process is divided into three distinct approaches:

- Scale Up
- Scale Out
- Scale In

In the 1990s, data centers used computer systems that were large, monolithic enclosures, which were referred to as supercomputers. Manufacturers of these large devices included Sun, DEC, HP, and IBM. These systems traditionally used proprietary hardware and operating systems.

The architectural design of these large systems enabled the systems to scale up to 64 CPUs. This high processing capability allowed many applications to run simultaneously while supporting numerous users. Although these monolithic servers could service many applications and users, components for these systems were expensive, which, of course, made ownership very costly. Furthermore, because of the large number of applications and users that were dependent on these systems, the systems created a significant failure domain.

In the early 2000s, the data center shifted significantly in the type of computing system used for processing applications. The next change in computing resources came in the form of commoditized servers, also referred to as tower- and rack-mounted servers. These smaller servers cost significantly less than the monolithic systems. The main difference was that these servers had fewer processing resources, perhaps only a single CPU. These servers had limited processing capabilities, so they were traditionally dedicated to support single applications per server.

Because of the way applications are distributed across many small servers, this approach is referred to as the Scale Out approach. The increase in server hardware added to overall operational costs. More servers meant higher costs for space, cabling, power, and cooling. Additionally, servers running only single applications were underutilized. This was an inefficient use of hardware, which can have a negative impact on the return on investment (ROI) for a company.

Since 2000, IT has begun to move away from traditional tower- or rack-mounted servers in favor of blade servers. Tower and rack-mounted servers require more space and need their own power supply, networking, and SAN cables. For smaller data centers, these infrastructure requirements are not problematic, but in a large data center, these requirements result in increasing complexity and cost of ownership.

By putting the computing resources of a server in a blade server form factor within a chassis enclosure, administrators gain these advantages:

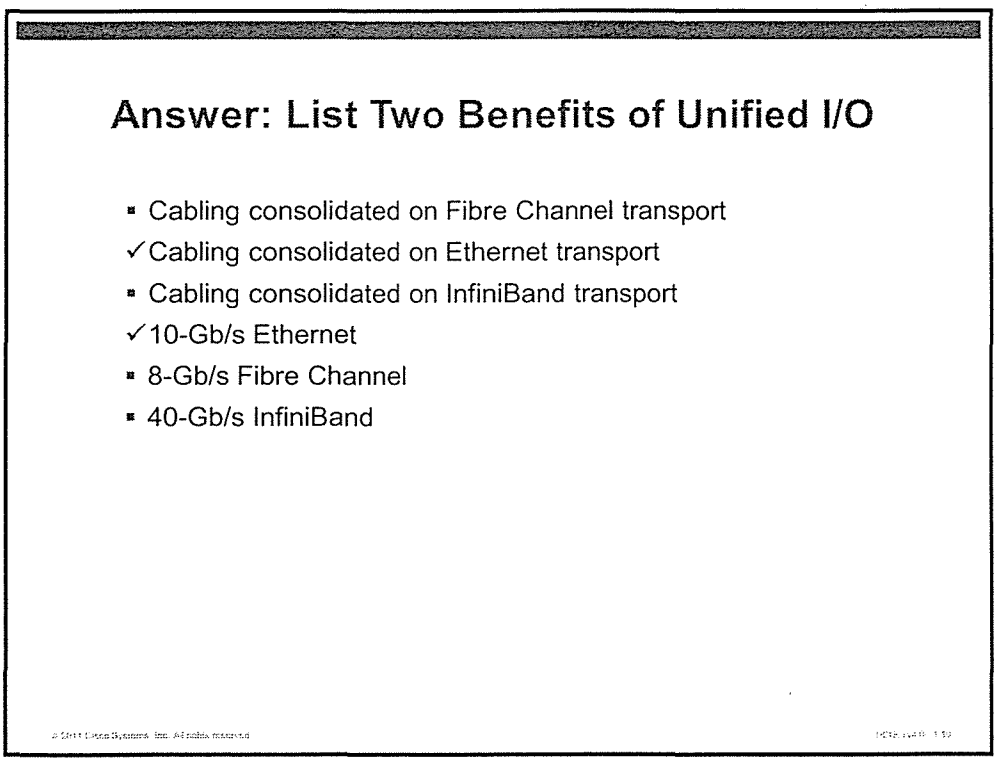
- Maximum use of physical space
- Shared power distribution
- Shared networking and storage access
- More efficient power and cooling

This form of hardware consolidation is the primary concept of the Scale In approach.

Reviewing Cisco UCS

This topic provides a review of Cisco UCS.

List Two Benefits of Unified I/O



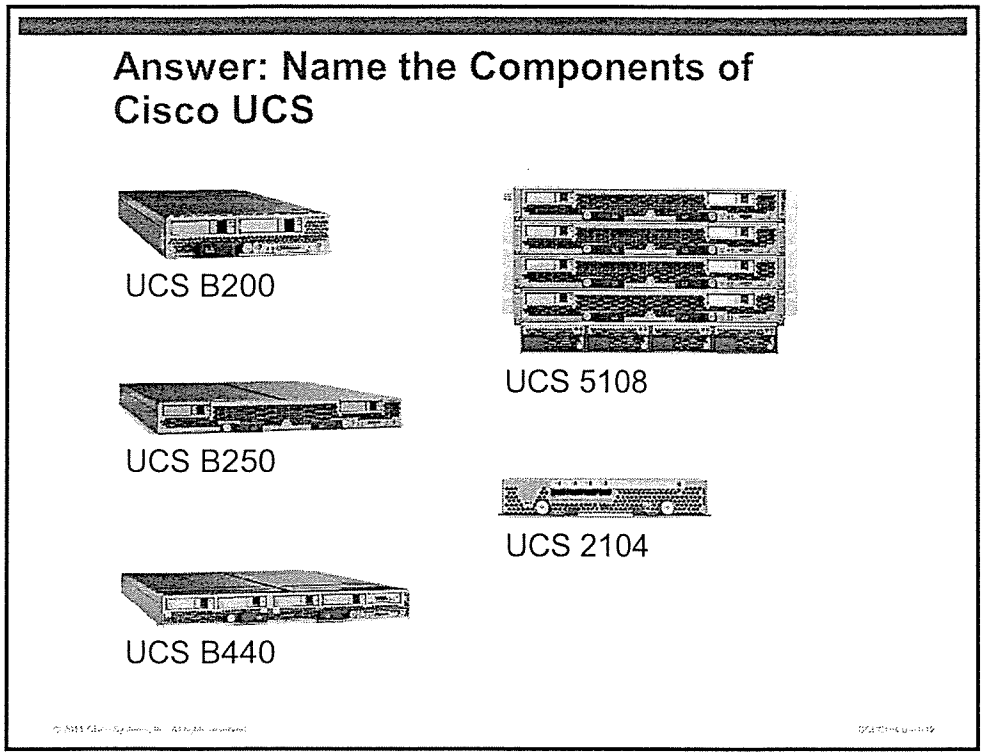
By consolidating the I/O infrastructure for storage, TCP/IP, and interprocess communication (IPC) traffic, data centers can reduce the number and type of devices that require power, cooling, and management.

Consolidated I/O solutions should maintain the same management processes that are available to each network type. Replacing software, skill sets, and procedures would be too disruptive for the technology.

However, most importantly, the consolidated I/O solution must satisfy the physical and logical requirements (bandwidth, throughput, delay, congestion, and management) that the individual protocols support. For example, Ethernet is considered a "lossy" protocol because it relies on higher-level protocols, such as IP and TCP, to respond to a drop in packets or lost packets. Fibre Channel, on the other hand, is a "lossless" protocol because none of the layers of the Fibre Channel stack can tolerate or respond to a drop or lost frames. Fibre Channel has a link-level, buffer-to-buffer signaling mechanism that allows transmitters to know whether receivers can receive frames. Fibre Channel transports Small Computer Systems Interface (SCSI) in SAN environments and SCSI does not tolerate lost data in a timely or efficient manner. A consolidated I/O solution, therefore, must account for and support both lossy and lossless protocols.

Name the Components of Cisco UCS

The figure shows the Cisco UCS B-Series hardware components of the Cisco Unified Computing System.



Differentiate Between IEEE Standards of Data Center Bridging

This section describes the IEEE standards of data center bridging.

Answer: Differentiate Between IEEE Standards of Data Center Bridging

IEEE Standard	Protocol	Purpose
802.1Qbb	Priority flow control	Enable multiple traffic types to share the same link (using CoS values)
802.1Qaz	Enhanced transmission selection	Manage bandwidth between different types of traffic on same link
802.1Qau	Congestion management	Manage end-to-end congestion
802.1Qab	DCBX	Discover and negotiate DCB capabilities

Priority flow control (PFC) provides a link-level flow control mechanism that can be controlled independently for each priority. The goal of this mechanism is to ensure zero loss due to congestion in data center bridging (DCB) networks.

Bandwidth management (also referred to as enhanced transmission selection [ETS]) provides a common management framework for assignment of bandwidth to traffic classes.

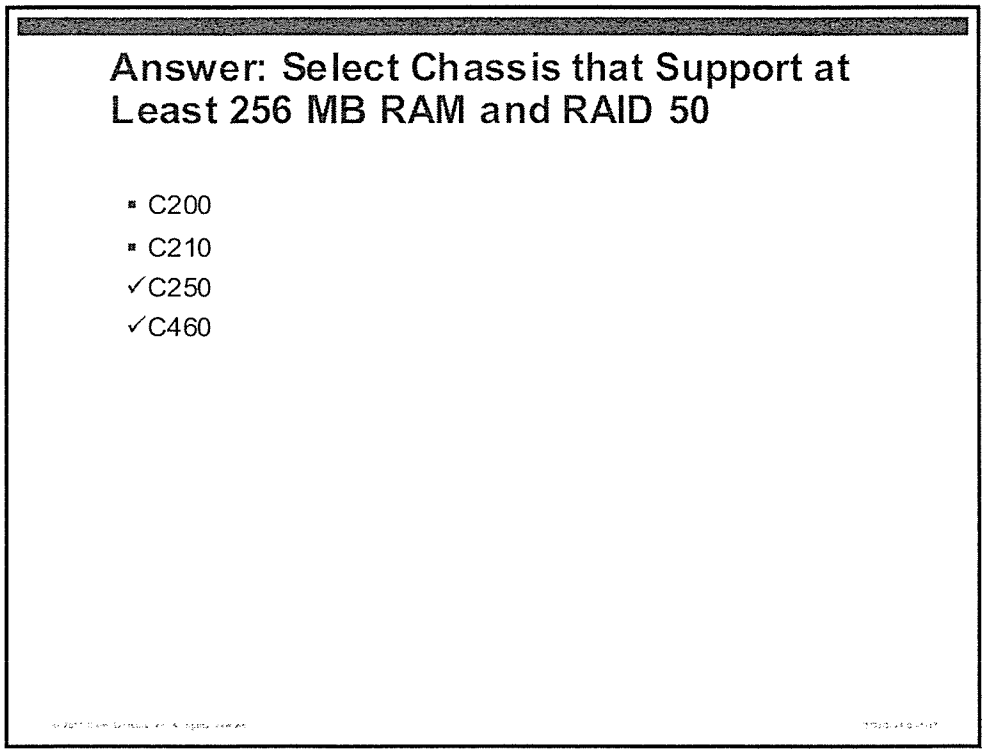
Congestion notification (CN) provides end-to-end congestion management for protocols that do not already have congestion control mechanisms that are built in, such as Fibre Channel over Ethernet (FCoE). It is also expected to benefit protocols that have native congestion management, such as TCP, as it reacts to congestion more efficiently. This is an alternative to using PFC on a hop-by-hop basis.

Data Center Bridging Capacity Exchange Protocol (DCBCXP) is a discovery and capability exchange protocol. It is used for conveying capabilities and configuration of features between neighbors to ensure consistent configuration across the network. This protocol is expected to leverage functionality that is provided by 802.1ab (Link Layer Discovery Protocol [LLDP]).

Reviewing Cisco UCS C-Series Hardware Components

This section focuses on Cisco UCS C-Series hardware specifications and capabilities.

Select the Chassis That Support at Least 256 MB RAM and RAID 50



The Cisco UCS C-Series offers four server models: C200, C210, C250, and C460.

The C200 was the first model introduced. It is a 1-rack unit (RU) rack-mount server that is designed to balance simplicity, performance, and density for production-level virtualization, web infrastructure, and other mainstream data center workloads.

The C200 supports up to two Intel Xeon 5500 Series multicore processors. With two processors, the C200 can support up to 96 GB of double data rate 3 (DDR3) memory. Regarding local storage, the C200 supports up to four internal Serial Attached SCSI (SAS) or Serial Advanced Technology Attachment (SATA) disk drives, up to 2 terabytes (TB) total.

The C210 is a large internal storage model. It is designed to balance performance, density, and efficiency for workloads requiring economical, high-capacity, reliable internal storage.

The C210 M1 supports up to two Intel Xeon 5500 Series multicore processors. With the two processors, the C210 can support up to 96 GB of DDR3 memory. Regarding local storage, the C210 M1 can support up to 16 internal small form factor (SFF), SAS, or SATA disk drives, up to 8 TB total.

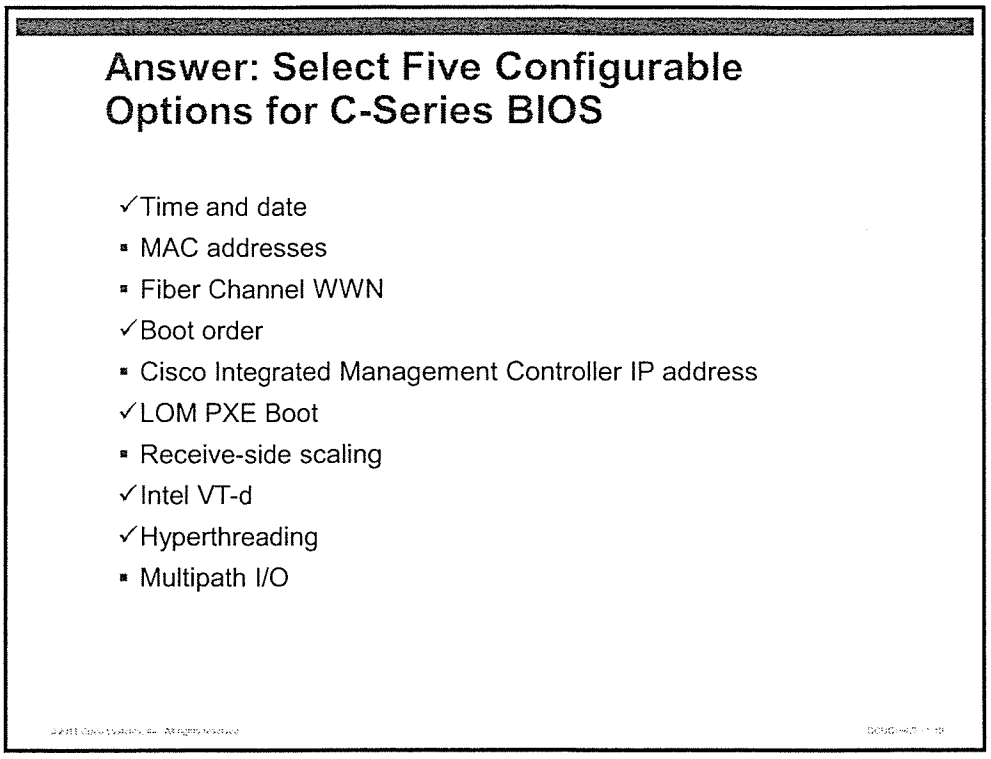
The C250 is a large memory server that is designed to increase performance and capacity for demanding virtualization and large data-set workloads.

The C250 M1 supports up to two Intel Xeon 5500 Series multicore processors. With the two processors, the C250 M1 can support up to 384 GB of DDR3 memory. Cisco Extended Memory Technology provides access up to 384 GB of memory with two processors.

The C460 is a high-performance rack-mount server that is designed with the performance and reliability to power compute-intensive, enterprise-critical, standalone applications and virtualized workloads.

C460 M1 supports two or four Intel Xeon 7500 Series multicore processors, for up to 32 processing cores. Also with 64 DIMM slots of DDR3 memory, the C460 M1 can support up to 512 GB of memory. This combination allows for fast processing and a large memory footprint, which is ideal for virtualization applications. Regarding local storage, the C460 M1 supports up to 12 front-accessible, hot-swappable, 2.5-inch (6.35 cm) SAS or SATA drives.

Select Five Configurable Options for C-Series BIOS

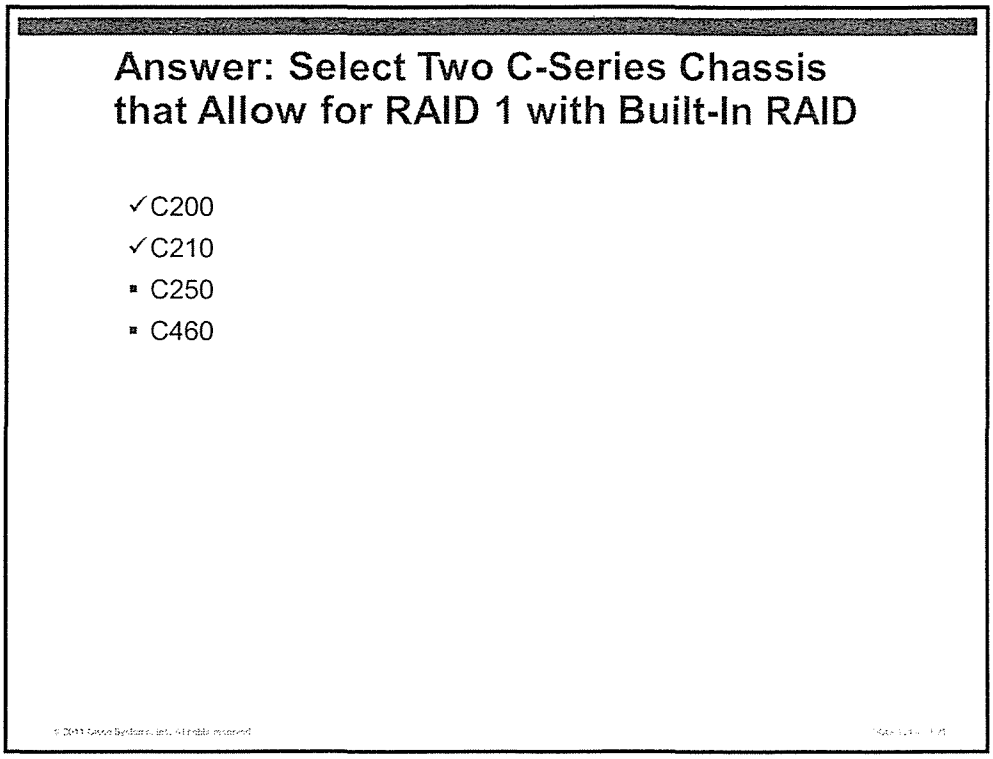


The BIOS is responsible for hardware initialization. It starts with the CPU and continues on to the other chips on the motherboard. The BIOS also discovers all of the I/O devices in the system and initializes them, such as Peripheral Component Interconnect Express (PCIe) devices. It boots the operating system and configures hardware for the operating system to use.

BIOS provides the following main features:

- Option ROM to provide PCI-connected device boot
- Manage boot devices (SCSI, Fibre Channel, Network, USB)
- Processor settings
- Memory settings
- Power management

Select Two C-Series Chassis That Allow for RAID 1 with Built-In RAID



The Cisco UCS C200 and C210 models come with an integrated onboard SATA controller. The built-in SATA controller is the Intel ICH10R. The controller takes advantage of proven Intel RAID controller technology. It is capable of providing RAID 0 and 1. In addition, it can support up to four SATA drives. However, SAS drives are not supported on the onboard SATA controller. The onboard SATA controller is integrated on the motherboard of the C200 and C210 models.

The LSI 1064-based controller is from LSI, one of the leading manufacturers of RAID controller technology. It only takes up one PCIe slot. This adapter provides support for both RAID 0 and 1 as well as 1E, a variation of RAID 1. This adapter can support up to four SAS or SATA drives. The LSI 1064-based controller is supported on the C200 and C210 models.

The LSI SAS 3081E-based controller card can provide high throughput to internal storage arrays. The LSI 3081 can support up to eight SAS or SATA drives with eight internal 3-Gb/s ports. In addition, this RAID controller card supports both RAID 0 and 1. This is an ideal controller for servers requiring medium- to high-capacity internal storage.

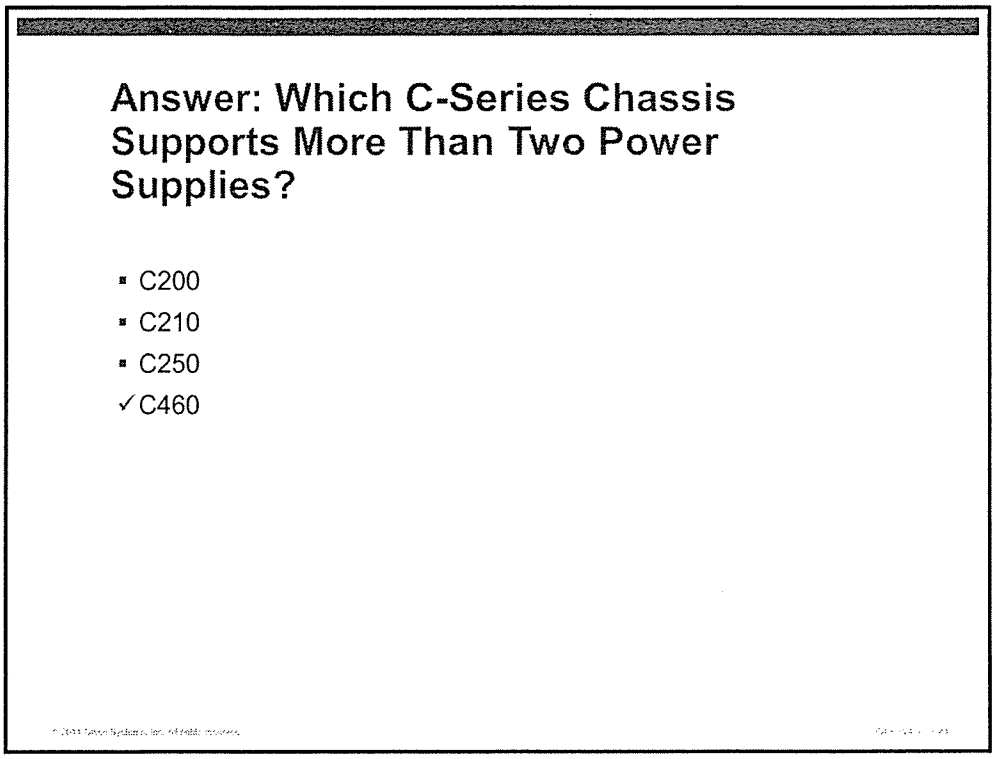
The LSI 6G MegaRAID 9260-4i Controller has features that can provide fault tolerance for critical data. This controller can support up to four SAS or SATA drives. It supports RAID 0, 1, 5, 6, 10, and 50. It requires only one PCIe slot and includes 512 MB of write cache. In addition, an optional battery backup can be installed. The card is supported on the C200 model.

The LSI 6G MegaRAID 9261-8i Controller has features that can provide fault tolerance for critical data. This controller can support up to 16 SAS or SATA drives. It supports RAID 0, 1, 5, 6, 10, 50, and 60. This card requires only one PCIe slot and includes 512 MB of write cache. In addition, an optional battery backup can be installed. The card is supported on the C210 and C250 servers.

The LSI MegaRAID 9240-8i RAID Controller can support up to 12 SAS or SATA drives. It only supports RAID 0 and 1. This card must be installed in a dedicated SAS riser PCIe slot and is supported on the C460 server.

The LSI MegaRAID 9260-8i RAID Controller is one of the higher performance adapters that can be installed in the C-Series servers. The features of this controller can provide high performance as well as fault tolerance for critical data. This controller can support up to 12 SAS or SATA drives, and can provide this with 6-Gb/s throughput per board. It currently supports RAID 0, 1, 5, 6, 10, and 50. This adapter also has the ability to perform auto resume or rebuild. These feature options can minimize the delay in reconstructing or recovering from hardware failure.

Which C-Series Chassis Supports More Than Two Power Supplies?



The C200 and C210 use a 650 W power supply unit with an added 5 A standby. One power supply always comes standard with the base chassis.

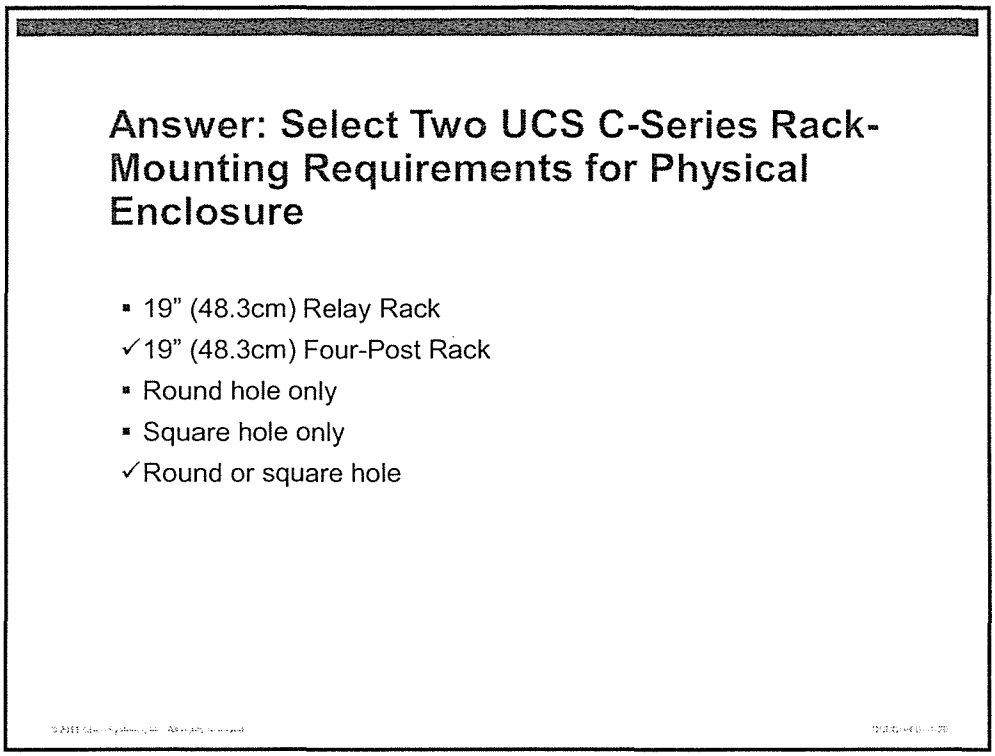
The Cisco UCSC 250 model uses an 850 W power supply unit. Similar to the other models, one power supply unit comes standard with the base chassis. The C250 server supports two power supply units for redundancy, but the redundant unit must be ordered.

The Cisco UCS C460 uses an 850 W power supply unit. In addition, it can support up to four power supplies. If the unit is initially ordered with two processors, then two power supplies come standard with the base chassis. Up to two redundant power supplies can be ordered. However, in a four-processor configuration, four power supplies come standard with the base chassis and no extra power supplies are needed.

Installing Cisco UCS C-Series Hardware

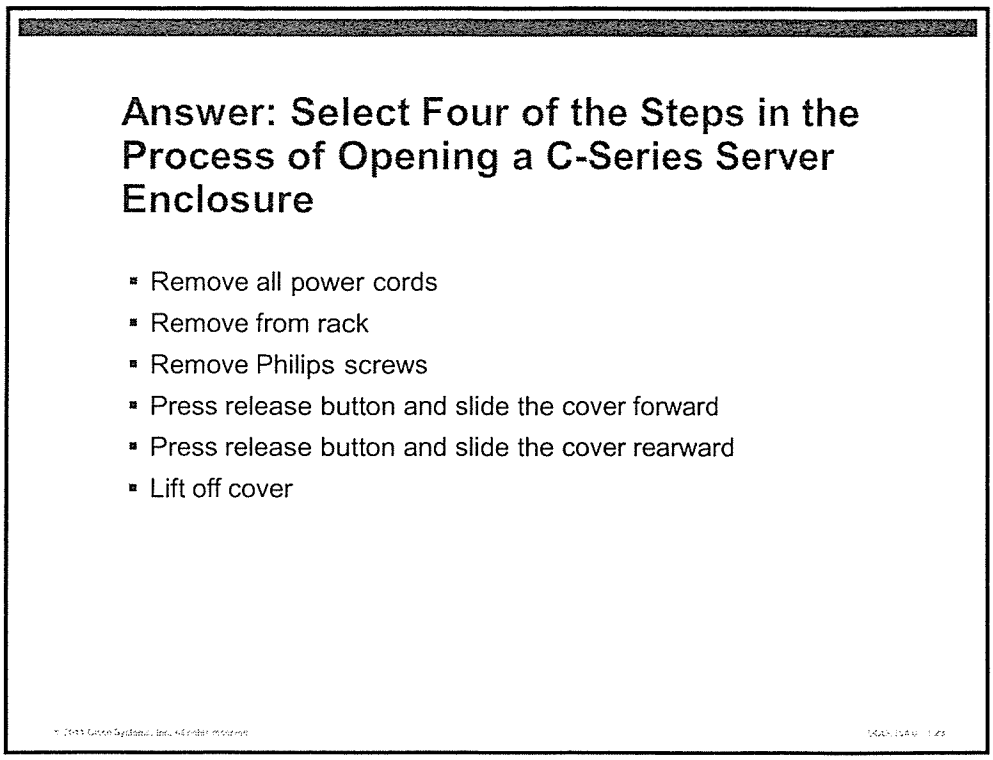
This topic reviews installation of Cisco UCS C-Series hardware.

Select Two C-Series Rack-Mounting Requirements for Physical Enclosure



Like Cisco UCS B-Series components, C-Series hardware requires mounting in a 19 inch (48.3 cm) four-post rack or cabinet. Unlike the B-Series, however, C-Series mounting brackets can be installed in a rack or cabinet with square or round holes.

Select Four of the Steps in the Process of Opening the C-Series Server Enclosure

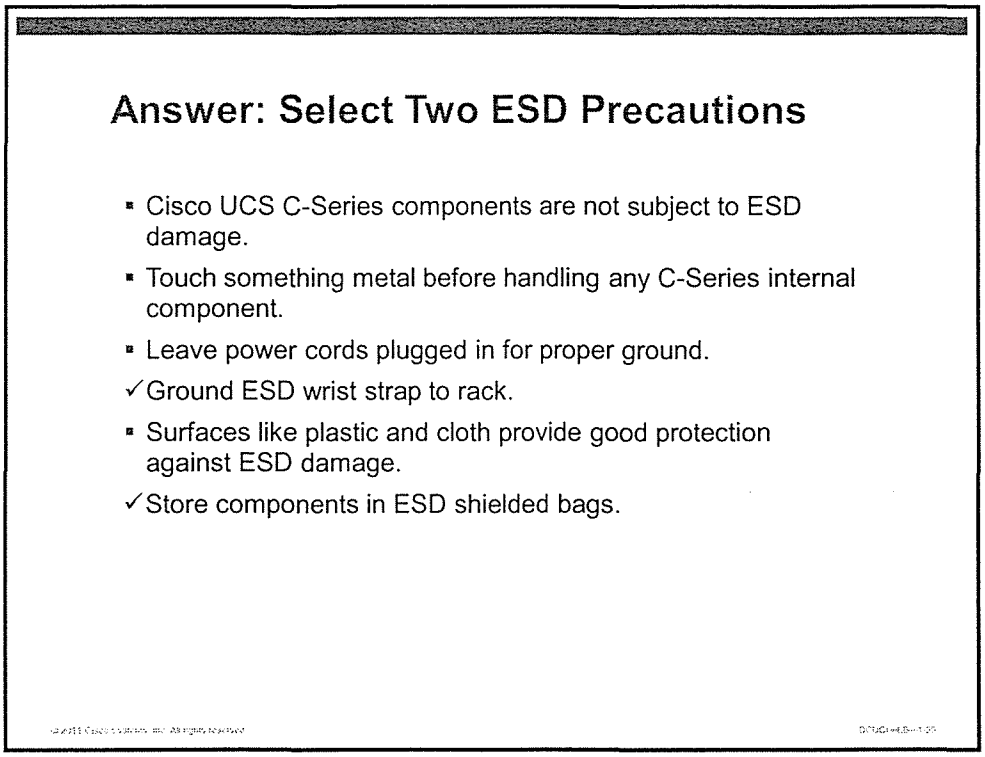


There are up to four steps that are required to open a C-Series server enclosure:

- To reduce the risk of electrical shock, remove all power cords.
- On C200 M1 and C210 M1, remove the Philips screws that hold the cover in place.
- Press the release button or buttons and slide the cover to the rear.
- Lift off the cover of the chassis.

Note	Though it is not necessary to remove the chassis from the rack, a ladder may be required to reach the top of the enclosure.

Select Two ESD Precautions

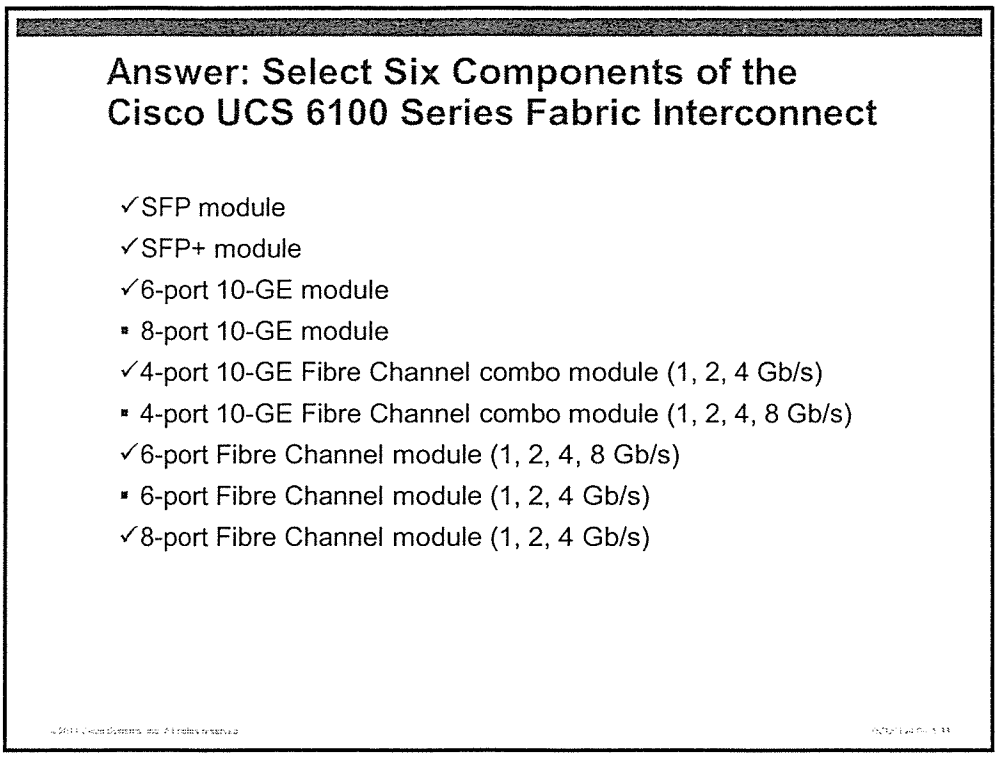


Nearly every component inside of a C-Series chassis can be damaged or degraded by ESD. Always wear an ESD wrist strap that is grounded to the server chassis. Always store components that are not installed in the chassis in an ESD-shielded bag or box.

Reviewing Cisco UCS B-Series Hardware Components

This topic reviews Cisco UCS B-Series hardware components.

Select Six Components of the Cisco UCS 6100 Series Fabric Interconnect

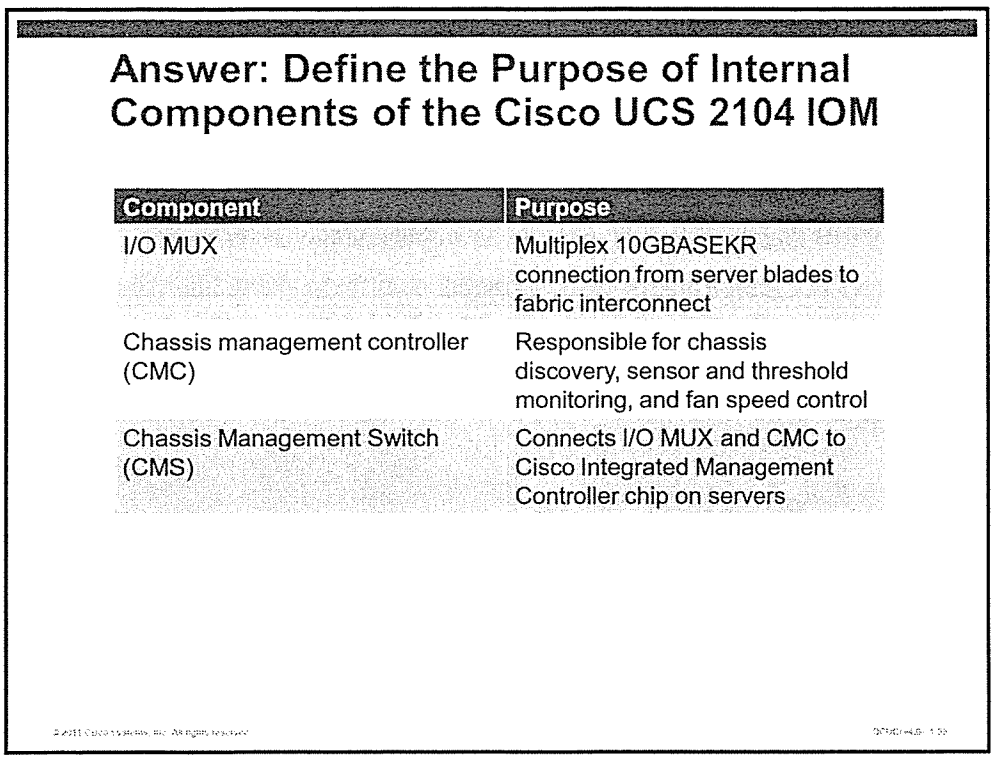


Small form-factor pluggable (SFP+) modules are required for external 10-Gb Ethernet connectivity to the aggregation layer of the network. SFP modules are required for Fibre Channel connectivity to Cisco Multilayer Director Switch (MDS) switches.

The Cisco UCS 6100 Series is equipped to support several expansion module options. The expansion modules provide connectivity into your enterprise Ethernet LAN and Fibre Channel SAN networks. There are currently four expansion modules from which to choose: Fibre Channel-only, combination Fibre Channel and Ethernet, and Ethernet-only.

- The Fibre Channel-only expansion module contains eight SFP ports that support 1-, 2-, and 4-Gb/s Fibre Channel.
- The combination expansion module contains four SFP+ ports that support 10-Gb Ethernet and four SFP ports that support 1-, 2-, and 4-Gb/s Fibre Channel.
- The Ethernet-only expansion module contains six SFP+ ports that support 10-Gb Ethernet.
- The Fibre Channel module provides six ports of 1-, 2-, 4-, and 8-Gb/s native Fibre Channel using the SFP or SFP+2.

Define the Purpose and Internal Components of the Cisco UCS 2104 IOM



The Cisco UCS 2104XP I/O module (IOM) also manages the chassis environment—the power supply and fans as well as the blades—with the fabric interconnect, which eliminates the need for separate chassis management modules.

This management is performed by a chassis management controller (CMC). The CMC collects status data from the IOM using the Intelligent Platform Management Interface (IPMI) protocol over the inter-integrated circuit (I2C) serial bus. This information is then communicated to the management node using the Ethernet server link. The CMC also serves as a proxy for the Cisco UCS Manager to the blade servers for certain functionality. It has a role in the high-availability protocols. Also, if two IOMs are present in a chassis, they will cluster in an active-passive configuration.

Moreover, the CMC performs the following functions:

- Controls the chassis fan
- Monitors and logs fan speed
- Monitors and logs ingress and egress temperatures
- Powers up and powers down power supplies
- Monitors and logs voltages, currents, and temperatures inside the chassis
- Detects presence, insertion, and removal of Cisco UCS blades
- Reads the IDs of the chassis, Cisco UCS blades, and IOM

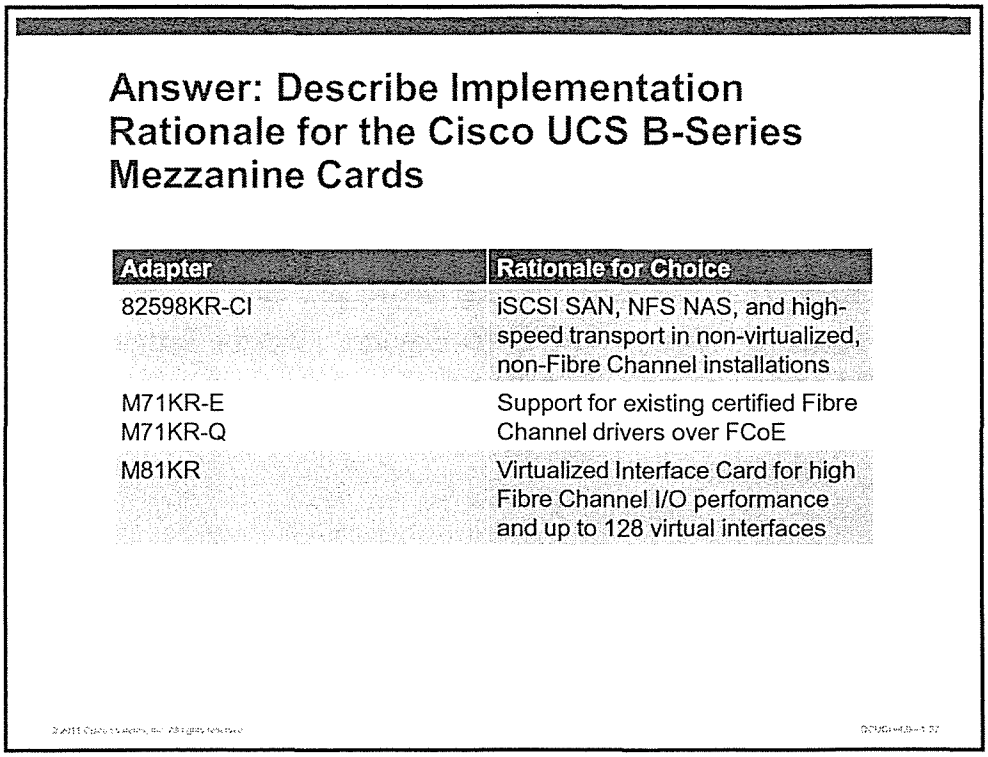
Another important component of the Cisco 2104 IOM is the Chassis Management Switch (CMS). The CMS provides connectivity to the Cisco Integrated Management Controller (IMC) on each server blade. The CMS has eight 100-Mb/s dedicated connections to the Cisco IMC. In addition, the CMS has a 1-Gigabit Ethernet connection to the I/O MUX. The CMS provides the vital connection to facilitate the monitoring and configuring of each blade server.

The IOM provides a bridge between server blades and fabric interconnect. The IOM hosts the ASIC that implements the data plane of the IOM.

The IOM provides the following:

- Eight 10-Gigabit Ethernet external downlink ports to server blades
- Four 10-Gigabit Ethernet external uplink ports to the fabric interconnect
- One 1-Gigabit Ethernet internal port to connect to the CMC
- Eight 100-Mb/s internal ports from the Cisco Integrated Management Controllers to the CMS

Describe Implementation Rationale for the Cisco UCS B-Series Mezzanine Cards

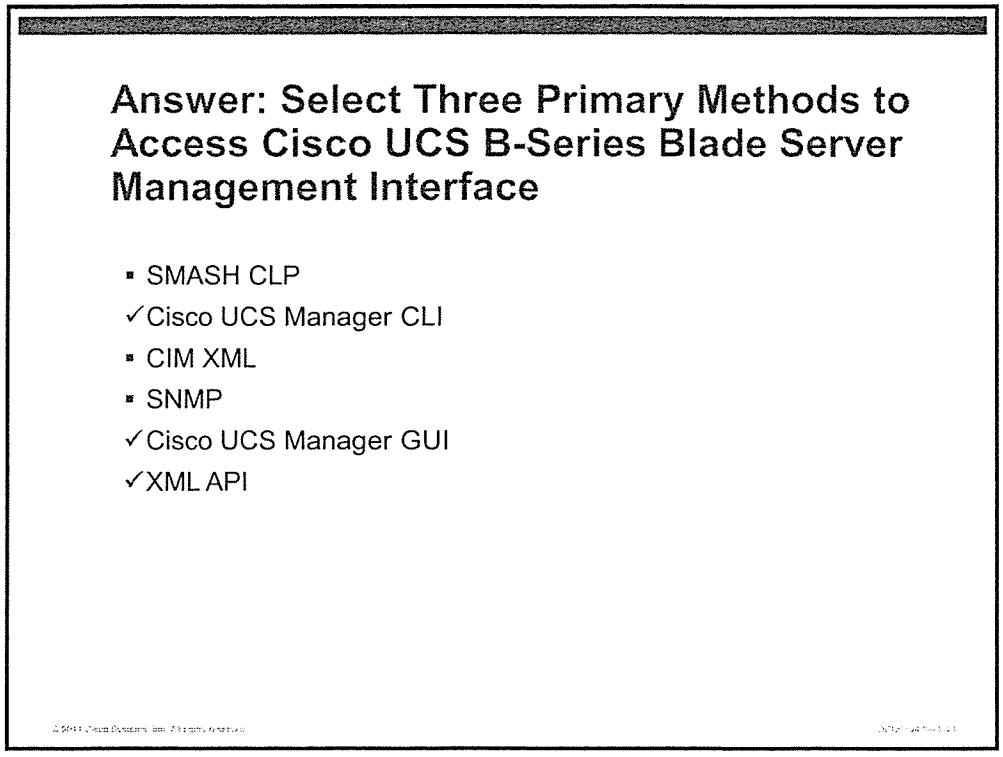


The choice of network adapter is based on operating system, application requirements, and whether adapter virtualization is required.

Reviewing B-Series Blade Server Architecture and Features

This section reviews Cisco UCS B-Series Blade Servers features and architecture.

Select Three Primary Methods to Access Cisco UCS B-Series Blade Server Management Interface

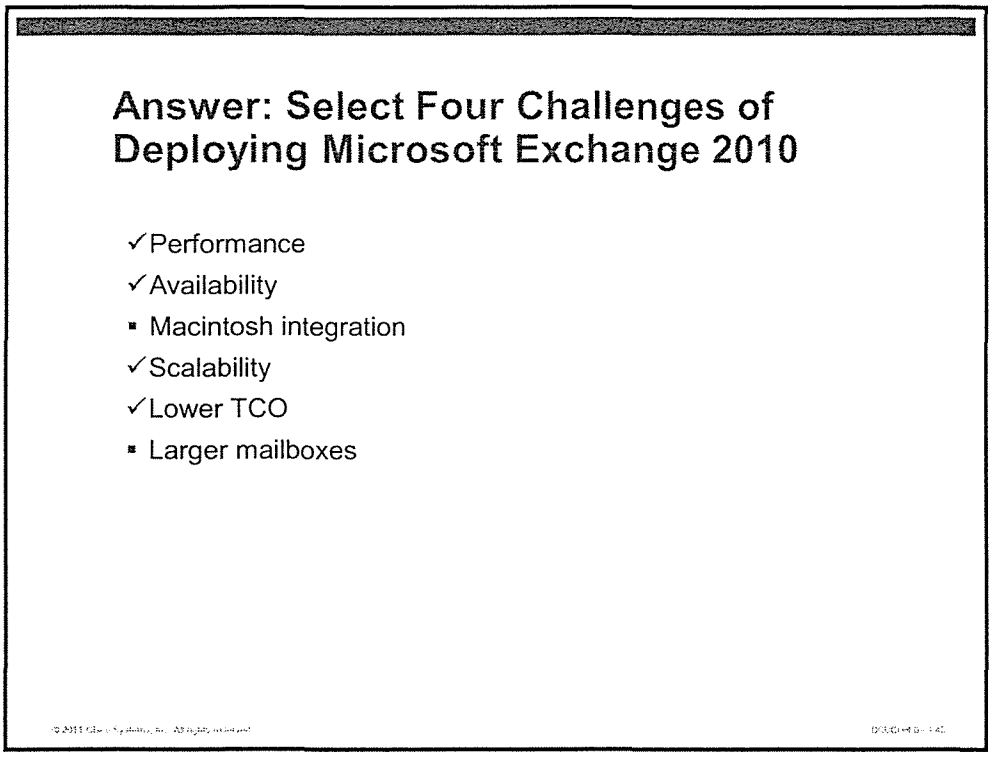


The three primary methods to access the management interface on a Cisco UCS B-Series Blade Server are the Cisco UCS Manager GUI, Cisco UCS Manager CLI, or the XML API.

Reviewing Cisco UCS Use Cases

This topic reviews Cisco UCS case studies.

Select Four Challenges of Deploying Microsoft Exchange 2010

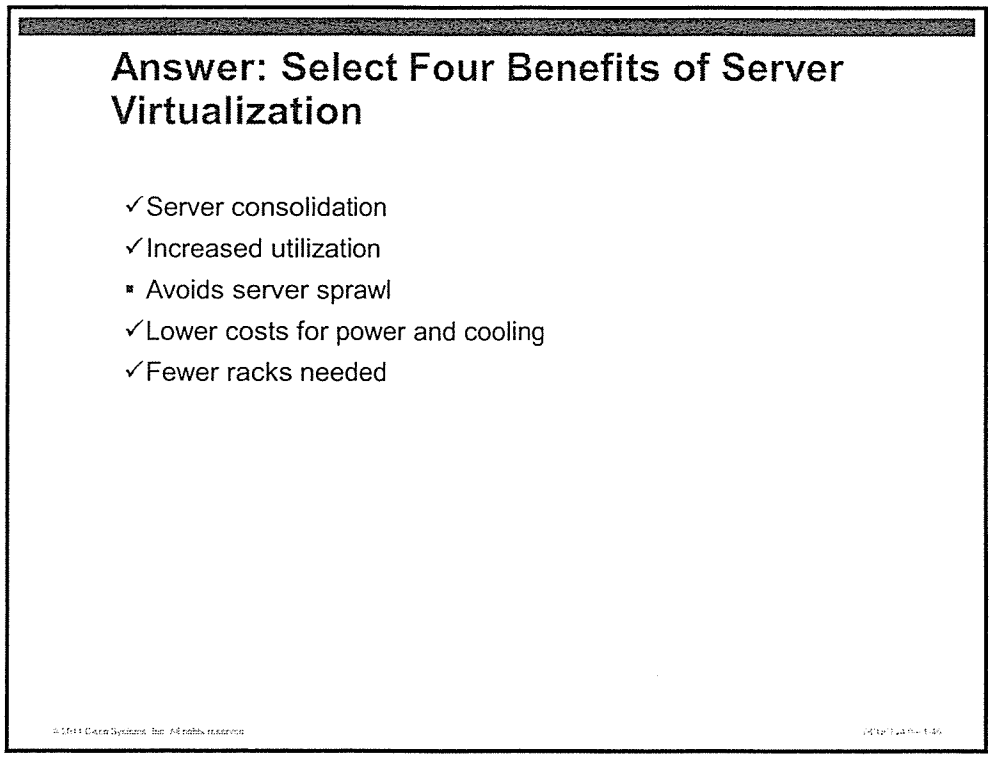


When deploying an application such as Microsoft Exchange 2010 in the data center, there is always pressure to increase the productivity of end users by using high-performance hardware and software. Also, there is the challenge to decrease downtime and maintain business continuity. In addition, designs must increase capacity without implementing a new architecture or management tools. Another challenge is to simplify application and infrastructure management to reduce support efforts. Most importantly, there is the goal of decreasing total cost of ownership (TCO).

Reviewing Server Virtualization

This topic reviews server virtualization concepts.

Select Four Benefits of Server Virtualization

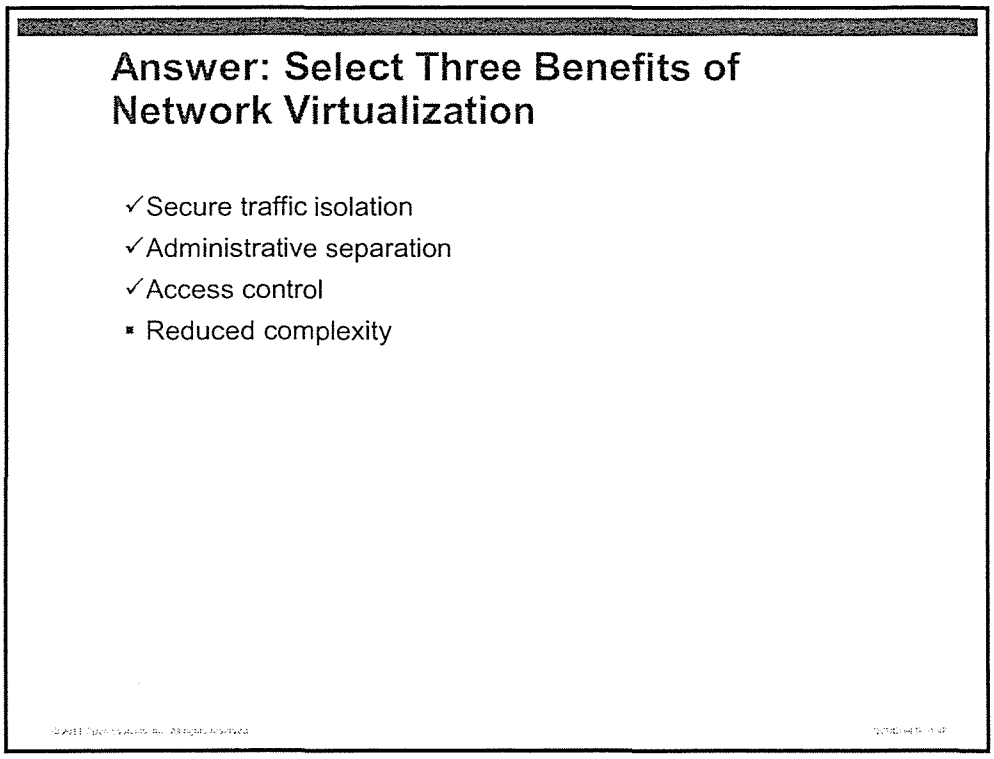


When server virtualization is used, operating systems and applications become independent of the underlying hardware, which enables a virtual machine to be provisioned to any physical server. The operating system and application are encapsulated in a virtual machine, so multiple virtual machines can be run on the same physical server. Thus, server virtualization offers significant benefits when compared to physical server deployment, including the following:

- Physical hardware can be consolidated.
- Resources of a physical machine can be shared among virtual machines.
- Resource utilization is improved, so fewer resources are wasted.

The figure describes application deployment in a physical server environment compared to a virtualized server environment. A physical server configuration uses three servers with a low average load, ranging from 10 percent to 40 percent. A virtualized solution uses just one server with three virtual machines that are deployed significantly better than with the former configuration, which means that the total physical server average load is the sum of virtual machine average loads, or approximately 70 percent.

Select Three Benefits of Network Virtualization

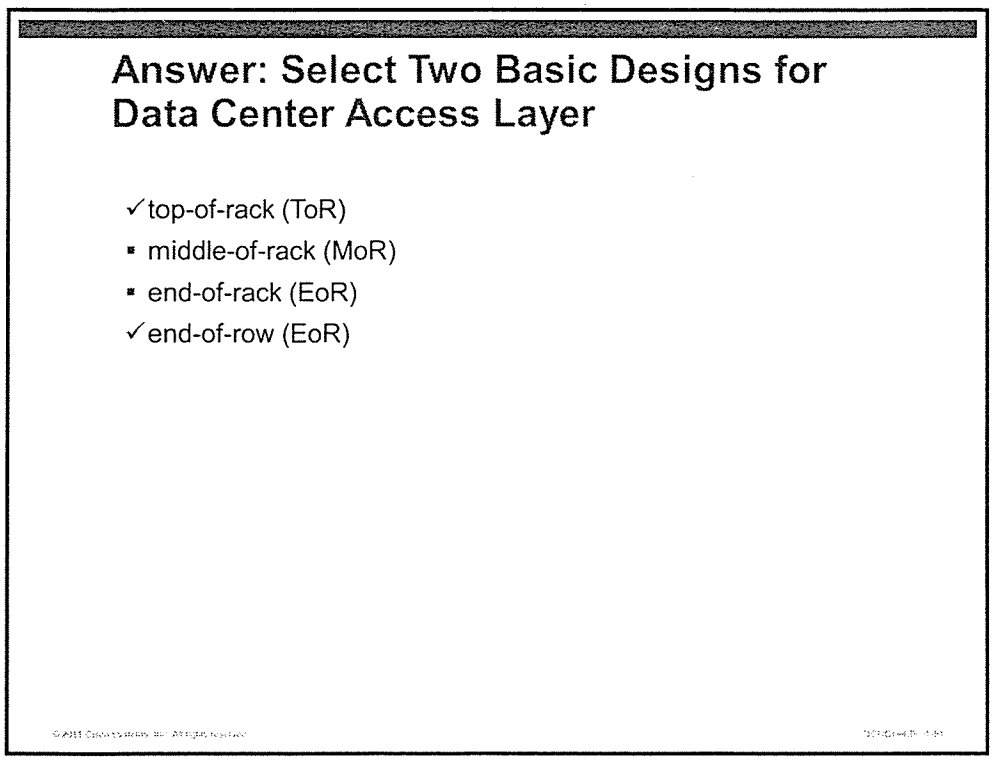


The use of virtual device contexts (VDCs) provides a number of benefits, including the following:

- Offers a secure network partition between different user department traffic
- Provides departments with the ability to administer and maintain their own configuration
- Provides a device context for testing new configuration or connectivity options without impacting production systems
- Consolidates multiple department switch platforms to a single physical platform while still maintaining independence from the operating system, administration, and traffic perspective
- Uses a device context for network administrator and operator training purposes

Designing the Data Center Access Layer

This topic reviews the data center access layer.



Typical data center access layers are built in one of two ways. Top-of-rack (ToR) architectures place switches at the top of each rack for server access. End-of-row (EoR) architectures place switches at the end of server rack rows for server connections.

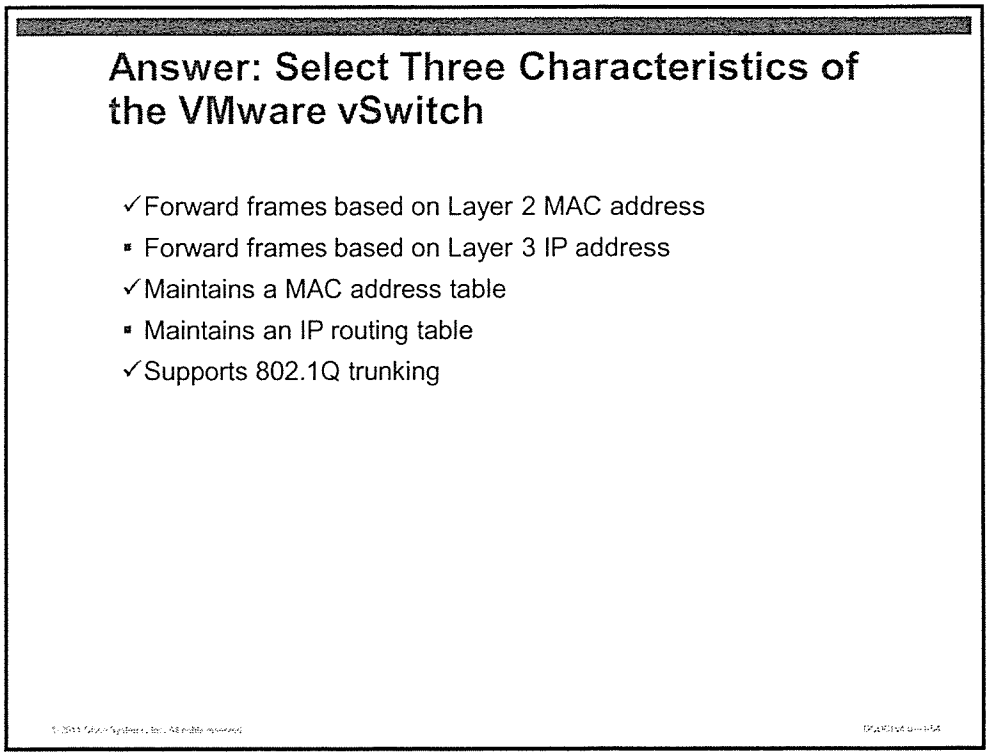
In a ToR network design, redundant switches are placed at the top of each server rack. This allows top-down cabling with fewer uplinks to aggregation switches. This design minimizes cabling complexity, but adds management complexity and power and cooling costs.

In an EoR design, servers are cabled to access switches placed at the end of each server row. This design increases the complexity of cabling while reducing the management complexity.

Reviewing VMware Ethernet Networking

This topic reviews VMware Ethernet networking.

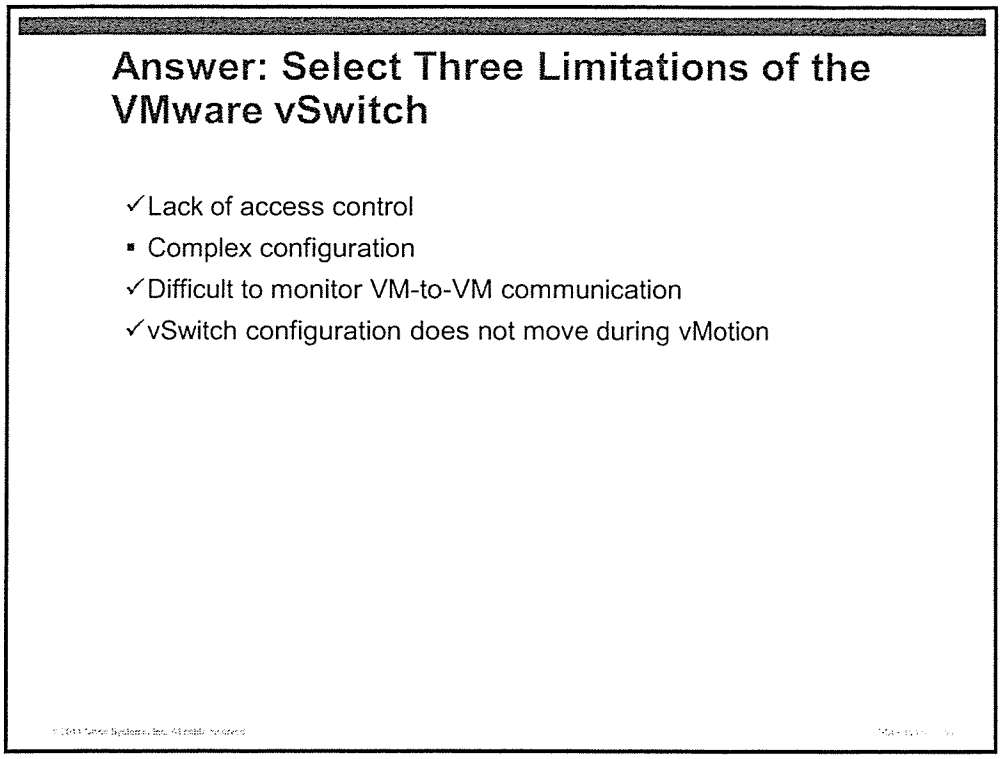
Select Three Characteristics of the VMware vSwitch



A VMware vSwitch is a software construct that provides both internal virtual machine (VM) communication and outbound uplinks for VMs. vSwitches operate in a manner similar to that of a physical switch. The VMware vSwitch provides the following features:

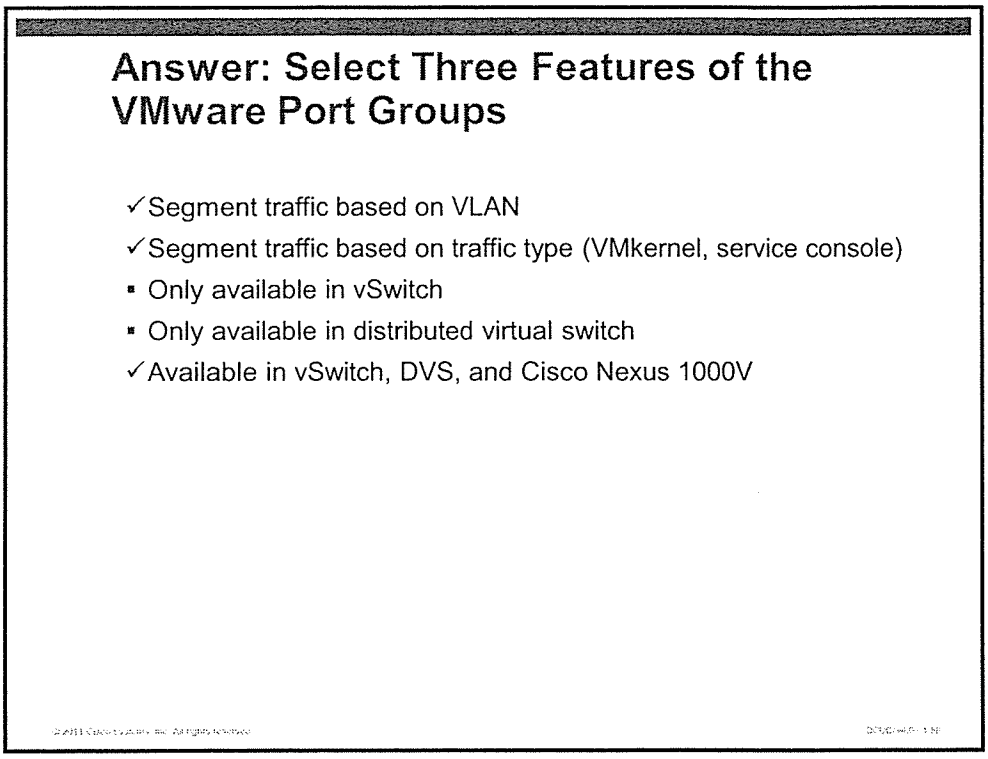
- Forwards frames that are based on Layer 2 information using MAC addresses
- Maintains a MAC address table
- Supports internal switching for virtual machines
- Tags frames with a VLAN ID using 802.1Q tagging
- Supports port channels for active-active network interface card (NIC) teaming only

Select Three Limitations of the VMware vSwitch



The vSwitch provides basic connectivity between virtual machines and physical switches, but this is not a perfect solution. The vSwitch does not provide the capability of creating access control lists (ACLs) to filter virtual machine communications. The vSwitch also does not provide a flexible facility for monitoring virtual machine-to-virtual machine traffic within the same vSwitch. vSwitch configurations have to be manually synchronized on a host-by-host basis because network configuration does not move with the virtual machine during vMotion.

Select Three Features of the VMware Port Groups

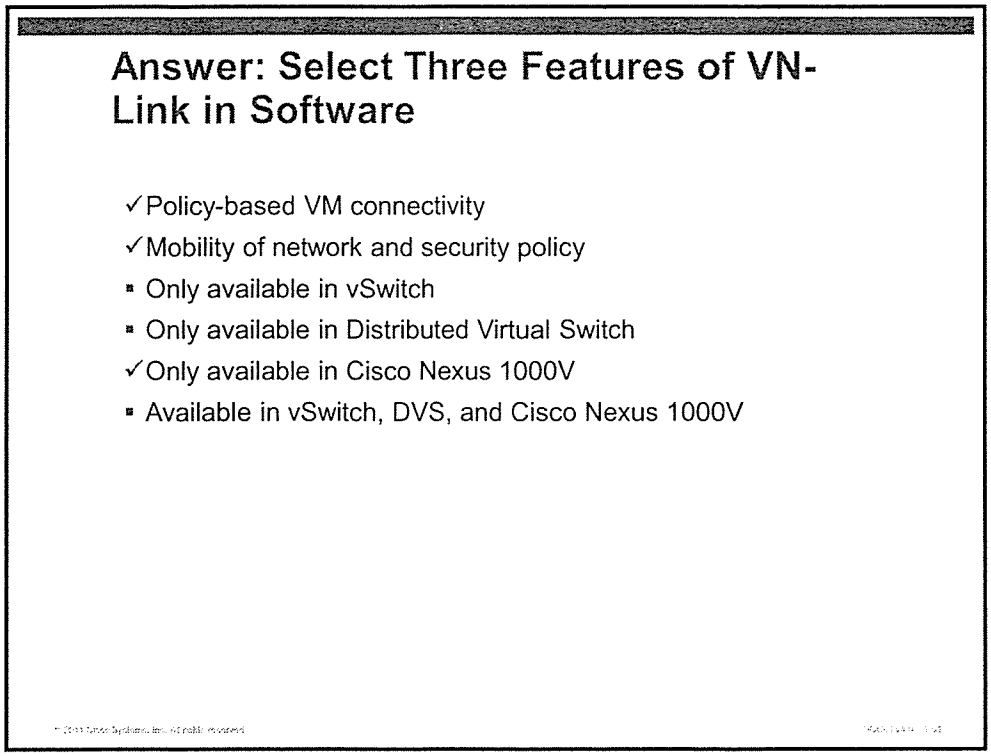


Port groups are configured on vSwitches to segregate traffic that is based on type or VLAN.

Reviewing Cisco Nexus 1000V Series Switch Architecture

This topic reviews the architecture of the Cisco Nexus 1000V Series Switch.

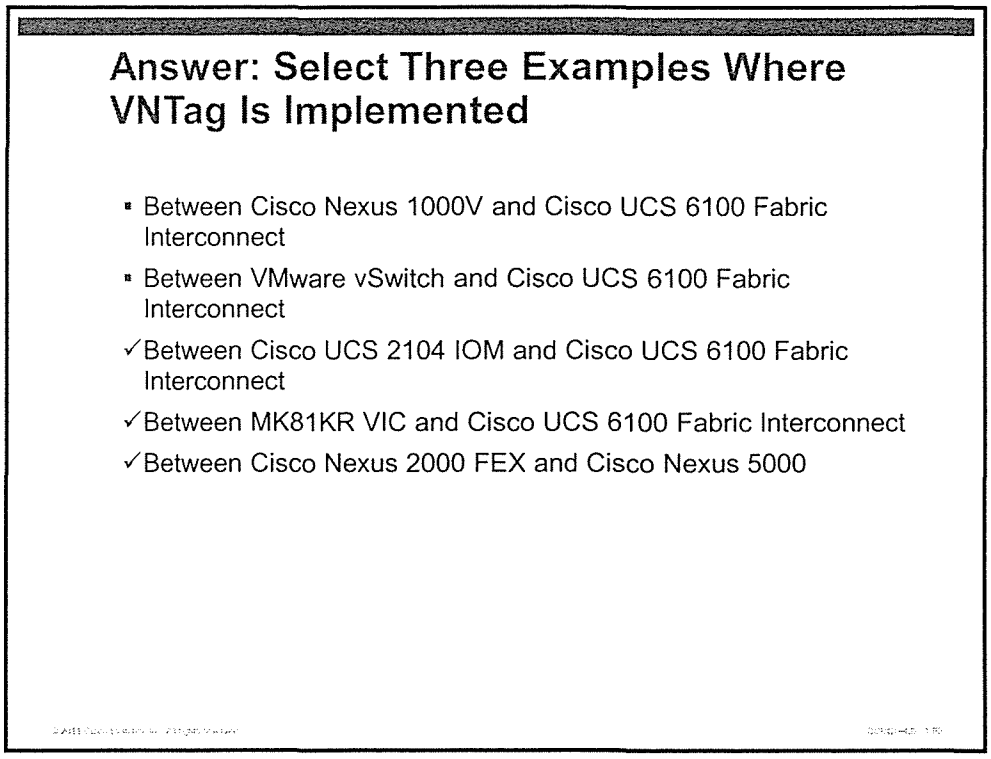
Select Three Features of Cisco VN-Link in Software



The Cisco Nexus 1000V Series Switch is a software-based solution providing VM-level network configurability and management. The Cisco Nexus 1000V Series Switch works with any upstream switching system to provide standard networking controls to the virtual environment.

Cisco Virtual Network Link (VN-Link) technology was jointly developed by Cisco and VMware. It has been proposed to the IEEE for standardization. The technology is designed to move the network access layer into the virtual environment in order to provide enhanced network functionality at the VM level. Cisco VN-Link is deployed as a hardware-based solution offering VM visibility, policy-based VM connectivity, policy mobility, and a nondisruptive operational model.

Select Three Examples Where VNTag Is Implemented



Cisco VNTag is required where network interface virtualization is present. Examples of network interface virtualizers include the Cisco UCS 2104 I/O module, UCS MK81KR VIC, and Cisco Nexus 2000 Fabric Extender (FEX).

Summary

Summary

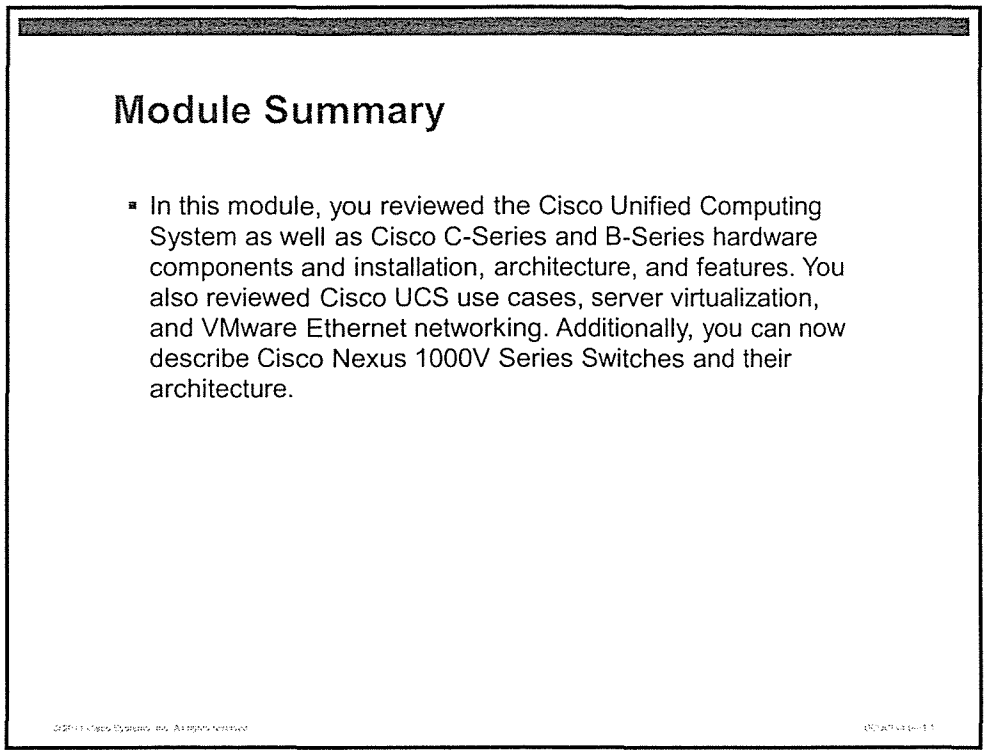
- Cisco UCS Manager relieves many challenges to data center server management by providing a single point of management for server provisioning.
- The Cisco Unified Computing System is a family of integrated components that include computer and switching resources.
- Cisco UCS C-Series hardware components include rack mountable chassis, CPU, RAM, RAID controller, hard drives, and network adapters.
- Cisco UCS C-Series hardware installation requires knowledge of proper ESD precautions and rack-mounting procedures.
- Cisco UCS B-Series hardware components include blade servers, fabric extenders, and fabric interconnects.

Summary (Cont.)

- Cisco UCS B-Series architecture includes integrated management, FCoE, and N-Port Virtualization.
- Cisco UCS use cases highlight the attributes of successful implementations of operating systems and applications on the Cisco UCS platform.
- Server virtualization allows for better utilization and return on investment for computer resources.
- VMware standard Ethernet networking architecture implements the concept of virtual switches that interconnect virtual machines and physical switches.

Module Summary

This topic summarizes the key points that were discussed in this module.



The review of the DCUCI e-learning material allows the instructor to gauge the experience level of incoming students to make adjustments in the level of detail to deliver in the instructor-led course.

The DCUCI e-learning material provides the fundamental knowledge of Cisco UCS B-Series, C-Series, and virtualization topics that students need to be successful in the DCUCI instructor-led training (ILT). The DCUCI certification exam contains questions that are drawn from the e-learning and ILT course.

References

For additional information, refer to these resources:

- Cisco, Inc. *Hardware and Software Interoperability Matrix* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/interoperability/matrix/hw_sw_interop_matrix_seriesBl1.2_v1.pdf
- Cisco, Inc. *BIOS Setting on UCS C-Series Rack-Mount Servers* at: http://www.cisco.com/en/US/products/ps10493/products_configuration_example09186a0080b0a578.shtml.
- Cisco, Inc. *RAID Controller Considerations* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C200M1/install/RAID.html.
- Cisco, Inc. *Cisco UCS C-Series Rack-Mount Servers Data Sheets* at: http://www.cisco.com/en/US/products/ps10493/products_data_sheets_list.html.
- Cisco, Inc. *C-Series Install and Upgrade Guides* at: http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html.

- Cisco, Inc. *Cisco ESD Training Program* at: *http://www.cisco.com/web/learning/le31/esd/WelcomeP.html*.
- Cisco, Inc. *Cisco UCS B-Series Blade Servers Data Sheets* at: http://www.cisco.com/en/US/products/ps10280/products_data_sheets_list.html.
- Cisco, Inc. *UCS Case Studies* at: http://www.cisco.com/en/US/netsol/ns944/networking_solutions_customer_success_stories_list.html.
- Cisco, Inc. *Cisco Design Zone* at: http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

Module 2

Installation of Cisco UCS C-Series Rack-Mount Servers

Overview

This module describes installation and configuration of the Cisco Unified Computing System (UCS) C-Series rack-mount servers.

Module Objectives

Upon completing this module, you will be able to locate, download, and manage Cisco UCS C-Series management and BIOS firmware. Firmware updates include feature updates and resolve outstanding issues.

This ability includes being able to meet this objective:

- Manage firmware updates on Cisco UCS C-Series rack-mount servers.

Lesson 1

Updating Firmware Components of the Cisco UCS C-Series Rack-Mount Servers

Overview

For ease of management, and to facilitate feature improvements and new functionality, many components of the Cisco Unified Computing System (Cisco UCS) C-Series platform include flash memory that you can update with little or no impact on server operation. Customers with valid service contracts can download updated firmware from Cisco.com. In this lesson, you will learn about updating firmware components of the Cisco UCS C-Series platform via the Cisco Integrated Management Controller, the host operating system, and methods that do not require a host operating system.

Objectives

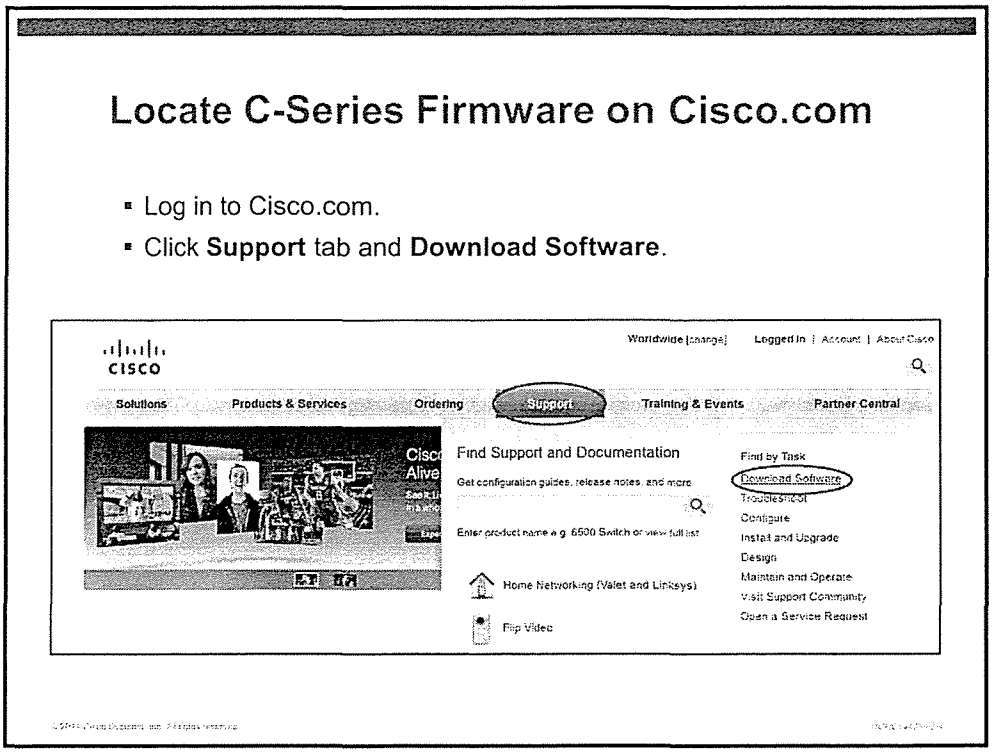
Upon completing this lesson, you will be able to define the updatable hardware components of the Cisco UCS C-Series rack-mount servers. This includes being able to meet these objectives:

- Locate and download C-Series firmware on Cisco.com
- Install and activate C-Series Cisco Integrated Management Controller firmware
- Update C-Series BIOS firmware
- Update C-Series BIOS prior to operating system load
- Recover from a corrupted BIOS

Locate and Download C-Series Firmware on Cisco.com

In this topic, you will learn how to locate and download C-Series firmware on Cisco.com.

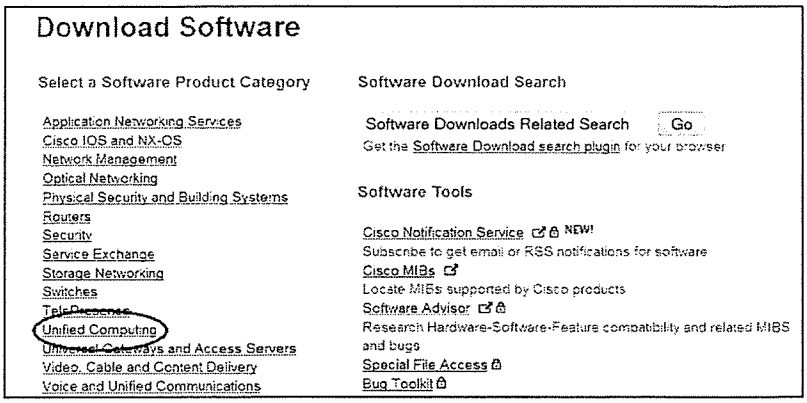
Locate C-Series Firmware on Cisco.com



To download software or firmware from Cisco.com, you must have a Cisco.com login that is associated with a valid service contract for the C-Series server that needs to be updated. If you download software or firmware updates for a device without entitlement, Cisco reserves the right to bill you for the cost of the update.

Locate C-Series Firmware on Cisco.com (Cont.)

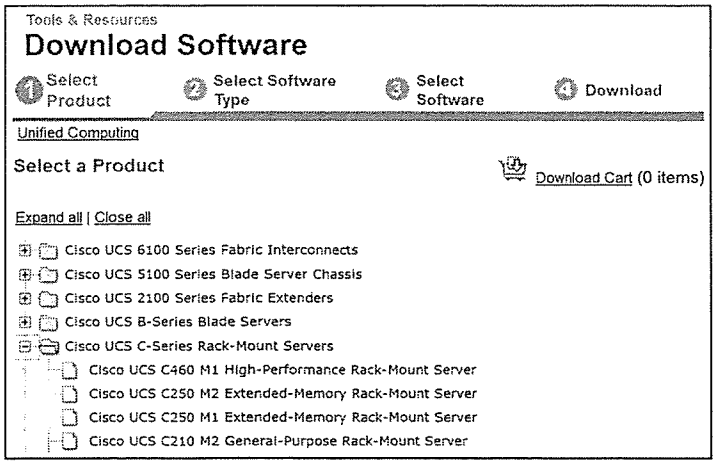
- Click **Unified Computing**.



Select Unified Computing from the Product Category.

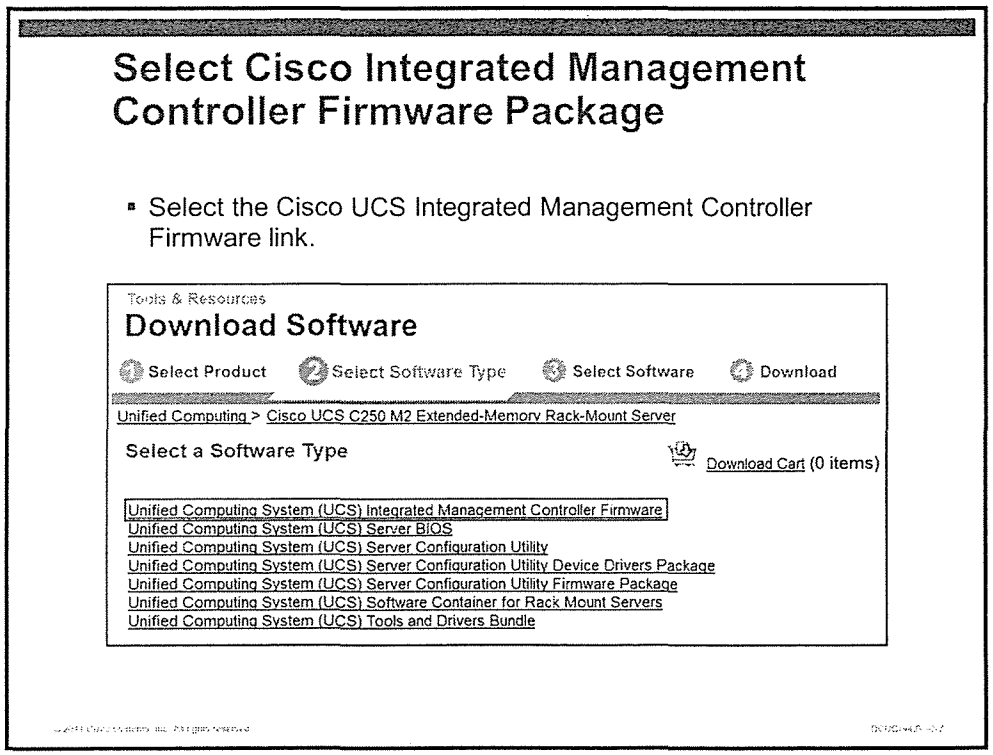
Locate C-Series Firmware on Cisco.com (Cont.)

- Click the + in the folder structure and select the model.



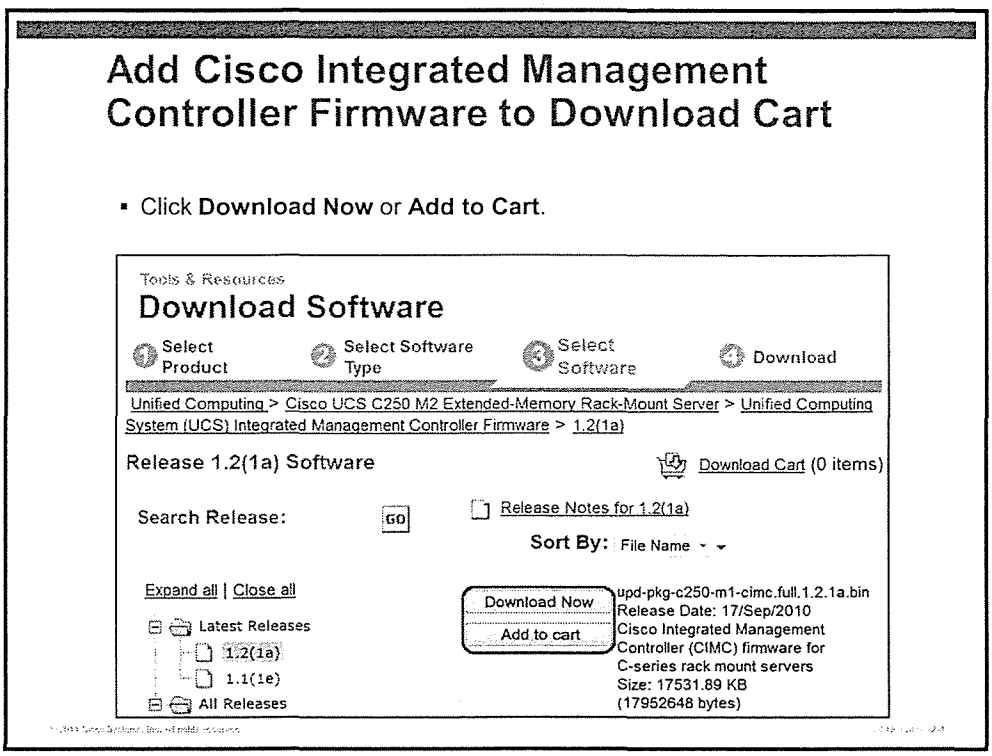
Scroll down to Cisco UCS C-Series Rack-Mount Servers and click the + sign to the left of the category to expand the list of C-Series models. At the time of this writing, there are three different model-specific Cisco Integrated Management Controller firmware packages. The four C200 and C210 models (M1 and M2) share a common package. The two C250 models (M1 and M2) share a common package and the C460 uses another specific package. Always assume that a model-specific package is required and download firmware accordingly.

Select Cisco Integrated Management Controller Firmware Package



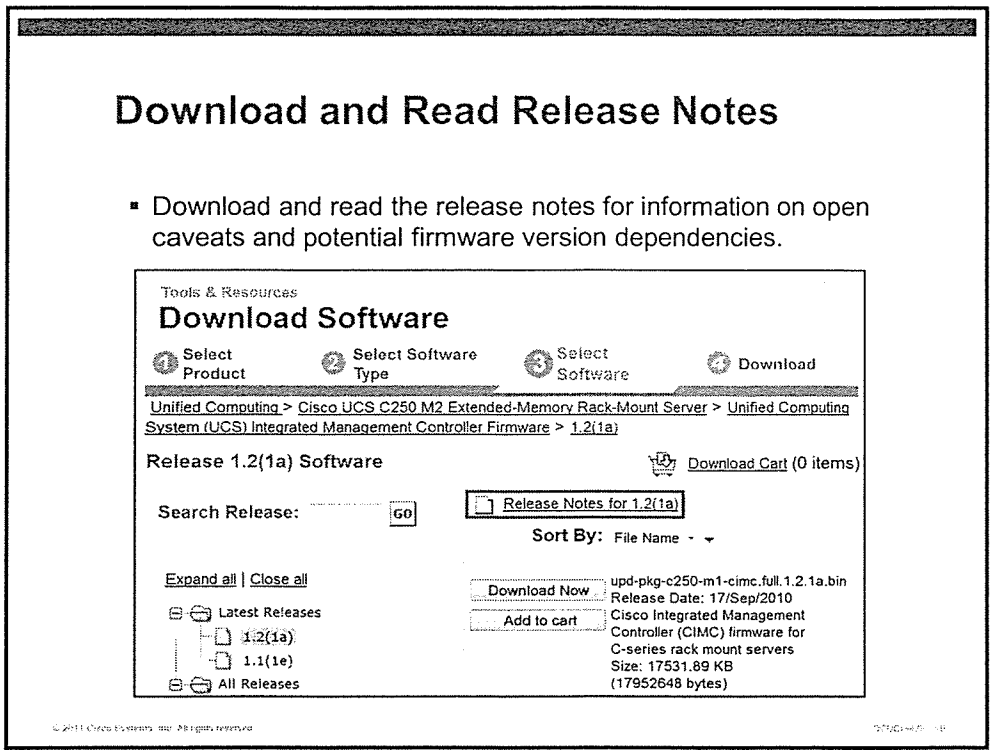
Select the Cisco UCS Integrated Management Controller Firmware link from the list of packages.

Add Cisco Integrated Management Controller Firmware Package to Download Cart



Click **Download Now** or **Add to Cart**. The download cart is convenient if you intend to download multiple firmware packages. Cisco.com offers two methods of completing the download: Java and non-Java. The Java version is preferable because it allows you to batch download in one operation. If you have difficulties with the Java version, the non-Java version allows you to manually download each of the files in your cart.

Download and Read Release Notes



Before applying any firmware update, it is important to read the release notes. They contain critical information about compatibility, version dependencies, and open caveats that may impact your production network. In some cases, upgrading to the latest firmware may be contraindicated by the release notes.

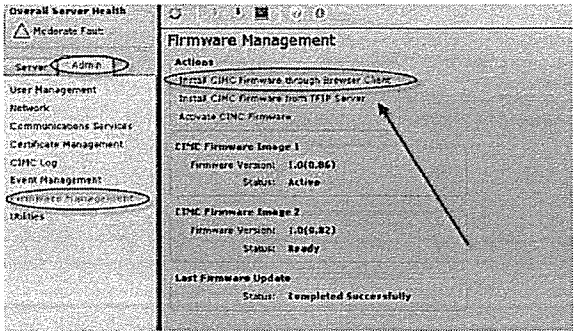
Install and Activate Cisco UCS C-Series IMC Firmware

This topic discusses how to install and activate Cisco UCS C-Series Integrated Management Controller (IMC) firmware.

Cisco IMC Firmware Update Options

Cisco Integrated Management Controller Firmware Update Options

- Cisco Integrated Management Controller firmware can be updated via web browser or CLI.

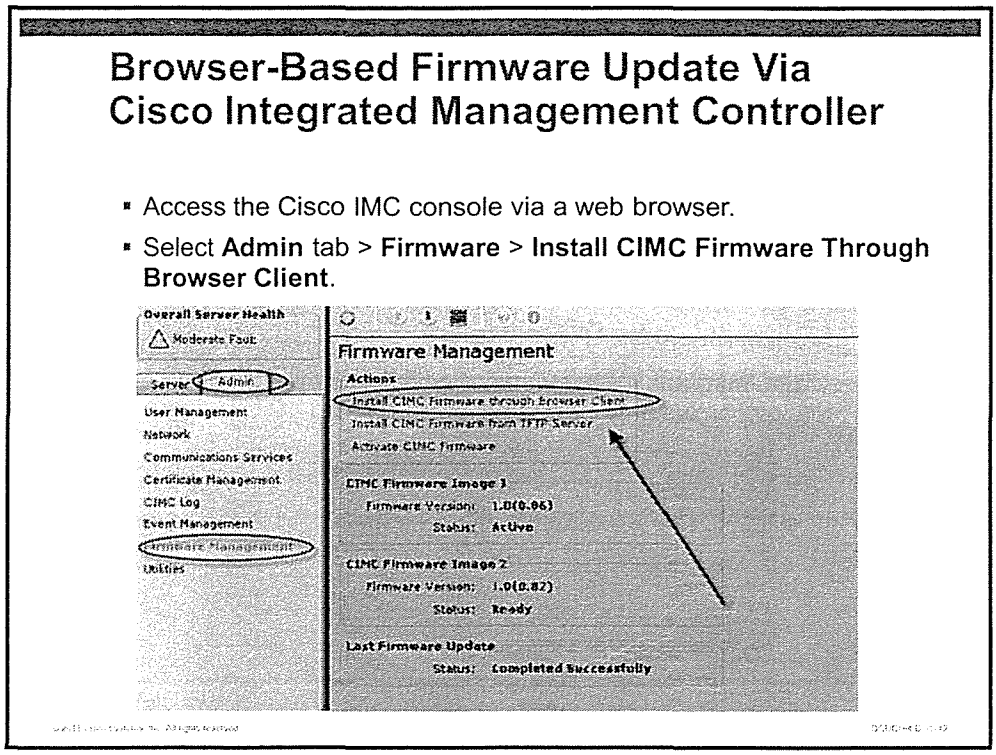



```
ucs-c2xx# scope cimc
ucs-c2xx /cimc # scope firmware
ucs-c2xx /cimc/firmware # update
Usage: update <tftp server address> <path>
```

Cisco IMC firmware can be updated via Cisco IMC GUI or the command-line interface (CLI). The GUI supports either HTTP transfer from the local machine running Cisco IMC, or the update files can be staged on a remote server and transferred by TFTP protocol. If there are intermediate firewalls or filtering routers between the Cisco IMC PC and the TFTP server, those devices need to allow User Datagram Protocol (UDP) port 69 to the management IP address of the server running Cisco IMC.

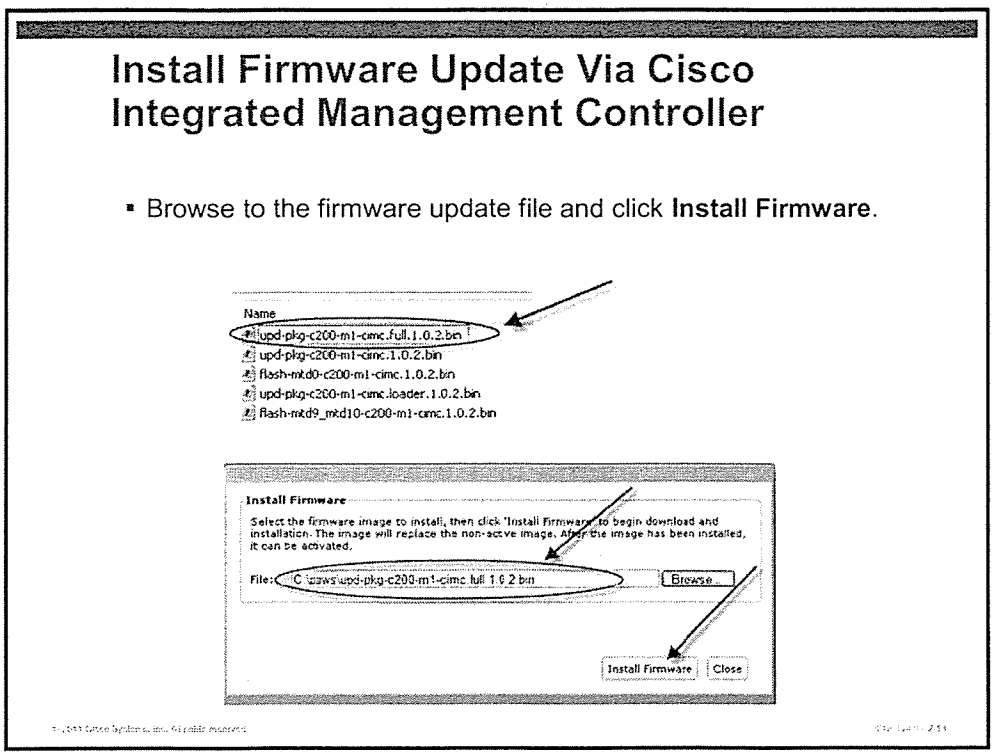
The CLI is accessed via Secure Shell (SSH) protocol. Firewalls and filtering routers must allow TCP port 22 to the management IP address of the C-Series server being updated.

Browser-Based Firmware Update Via Cisco Integrated Management Controller



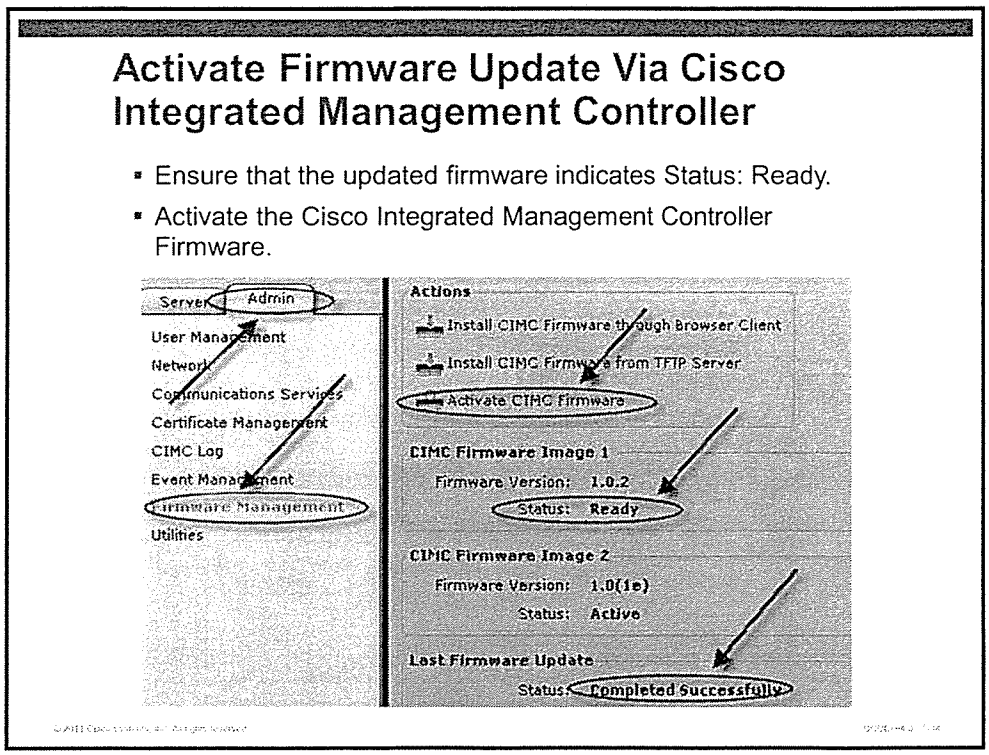
The simplest method to update the Cisco Integrated Management Controller Firmware is from the already-open browser session. Click **Install CIMC Firmware through Browser Client**.

Install Firmware Update Via Cisco Integrated Management Controller



Use the Browse button to locate the Cisco Integrated Management Controller firmware update file and click **Install Firmware**, which will upload the new image into the inactive Cisco Integrated Management Controller flash partition. There is no impact to the operation of Cisco Integrated Management Controller until the new image is activated.

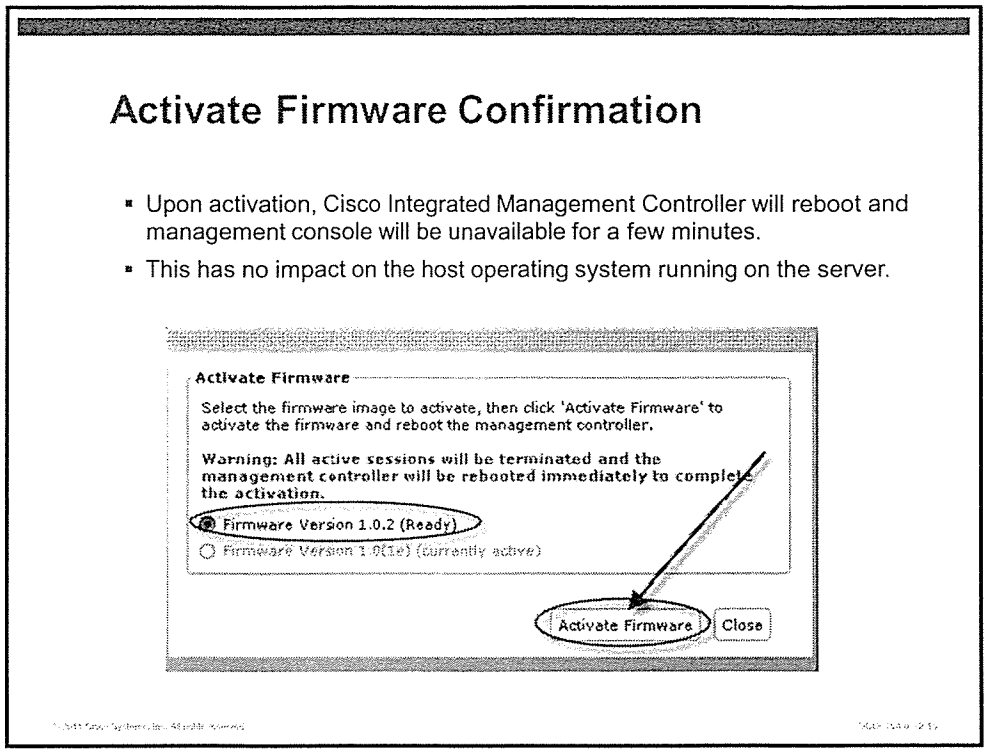
Activate Firmware Update Via Cisco Integrated Management Controller



Before activating the new firmware, ensure that the package was successfully copied into the standby flash partition and that its status indicates "Ready."

If the file transfer failed due to a checksum error, download another copy from Cisco.com and validate the MD5 hash with a tool such as MDFiveCheck for Windows (http://www.md5check.de).

Activate Firmware Confirmation



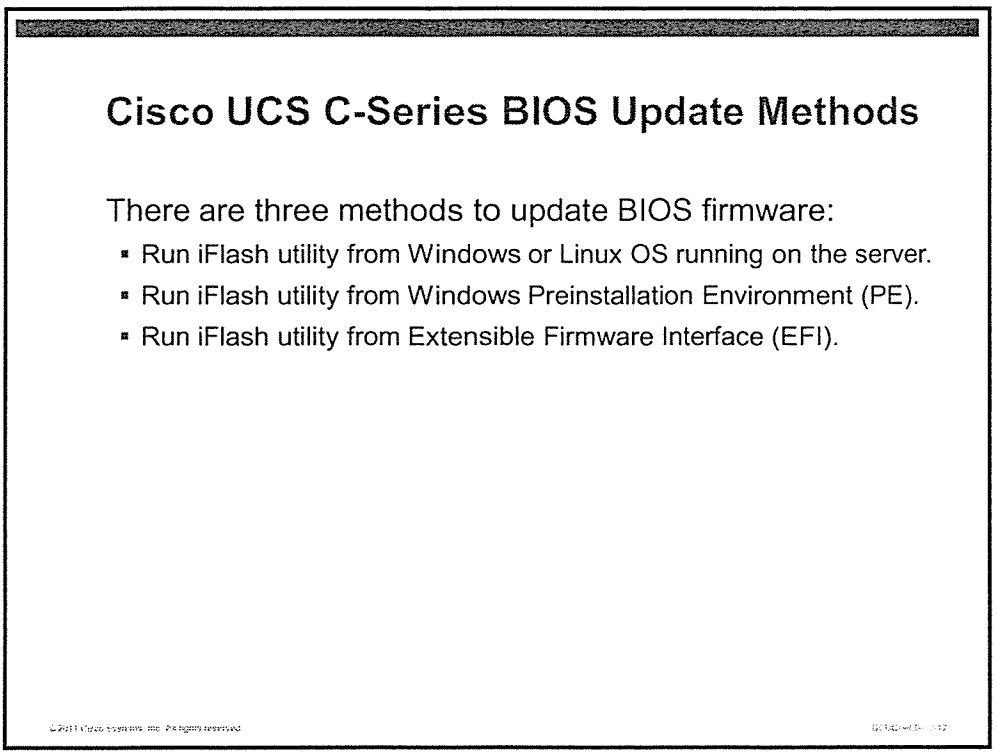
When you click **Activate Firmware**, all Cisco Integrated Management Controller sessions via browser and SSH will be terminated while Cisco Integrated Management Controller loads the updated firmware. If the new image cannot be loaded, the standby (previous) image will be booted and will become the active image.

It is important to understand that update and activation of the Cisco Integrated Management Controller firmware has no impact on the operation of the operating system running on the C-Series server. Cisco Integrated Management Controller has its own management CPU, RAM, and flash memory that is isolated from the host operating system.

Update C-Series BIOS Firmware

This topic discusses the process for updating Cisco UCS C-Series BIOS firmware.

Cisco UCS C-Series BIOS Update Methods

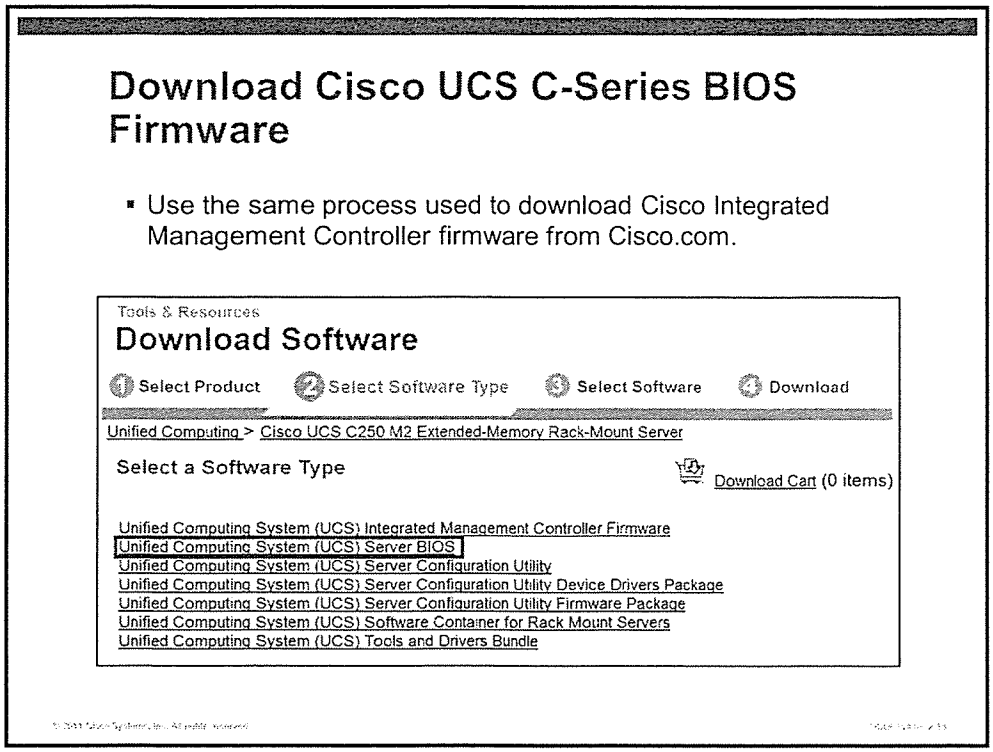


There are three techniques to update the BIOS on Cisco UCS C-Series servers. The first method requires that a supported operating system is installed and running on the server. The other techniques can be employed before an operating system is deployed.

All update methods require downloading a BIOS firmware bundle (.zip format) from Cisco.com.

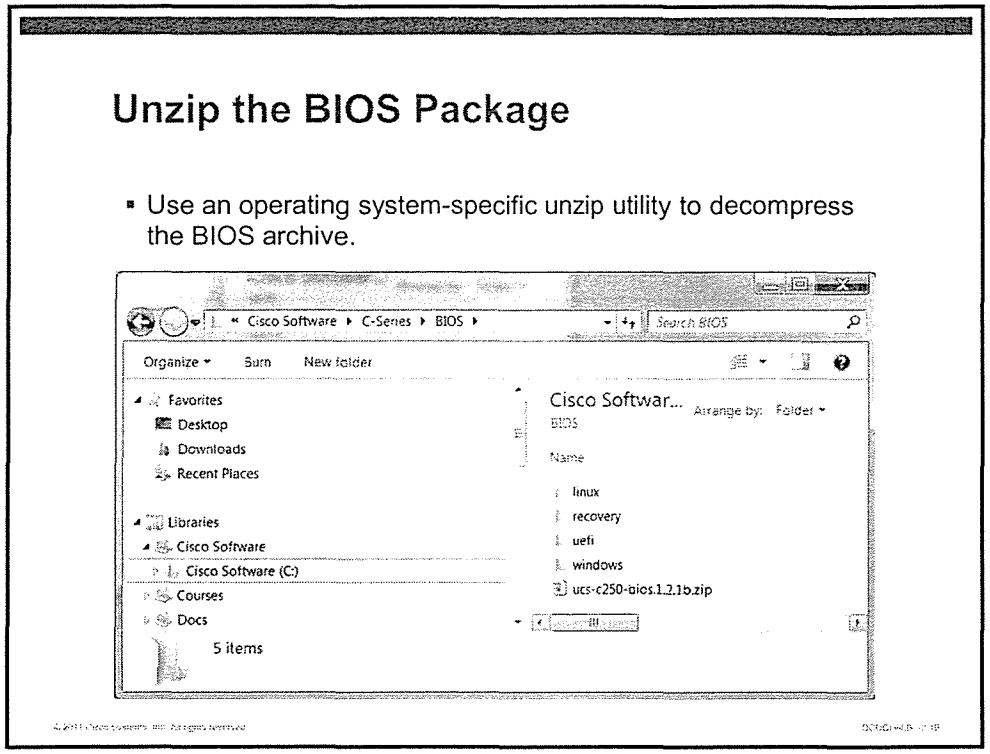
- Run iFlash utility from Windows or Linux operating system running on the server.
- Run iFlash utility from Windows Preinstallation Environment (Windows PE).
- Run iFlash utility from Extensible Firmware Interface (EFI).

Download Cisco UCS C-Series BIOS Firmware



Following the steps to download the Cisco Integrated Management Controller firmware, download the model-specific BIOS package for your server.

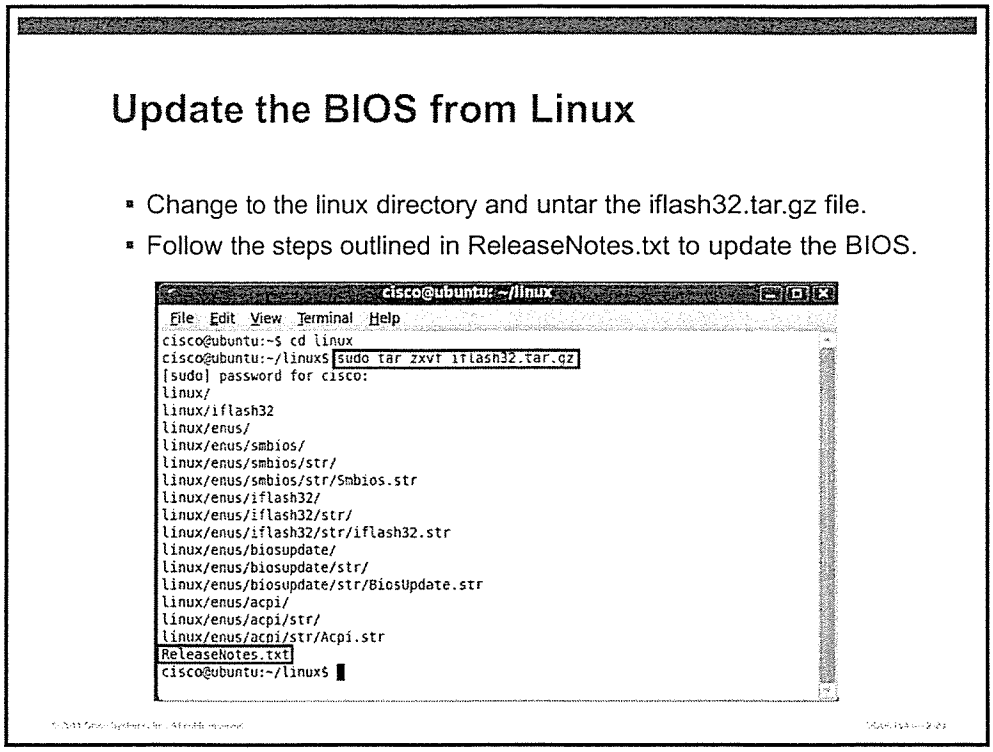
Unzip the BIOS Package



There are four subdirectories that are created after the archive is expanded:

- linux: This directory contains the iFlash utility for supported Linux operating systems and the BIOS image.
- recovery: This directory contains an .iso file that is used to recover from a corrupted BIOS.
- uefi: This directory contains the iFlash utility and BIOS image for use with the Unified Extensible Firmware Interface (UEFI).
- windows: This directory contains the iFlash utility for supported Microsoft Windows operating systems and the BIOS image.

Update the BIOS from Linux



To update the BIOS from a supported Linux running on the C-Series server, follow these steps:

Step 1 Download and expand the BIOS.zip archive to the local file system.

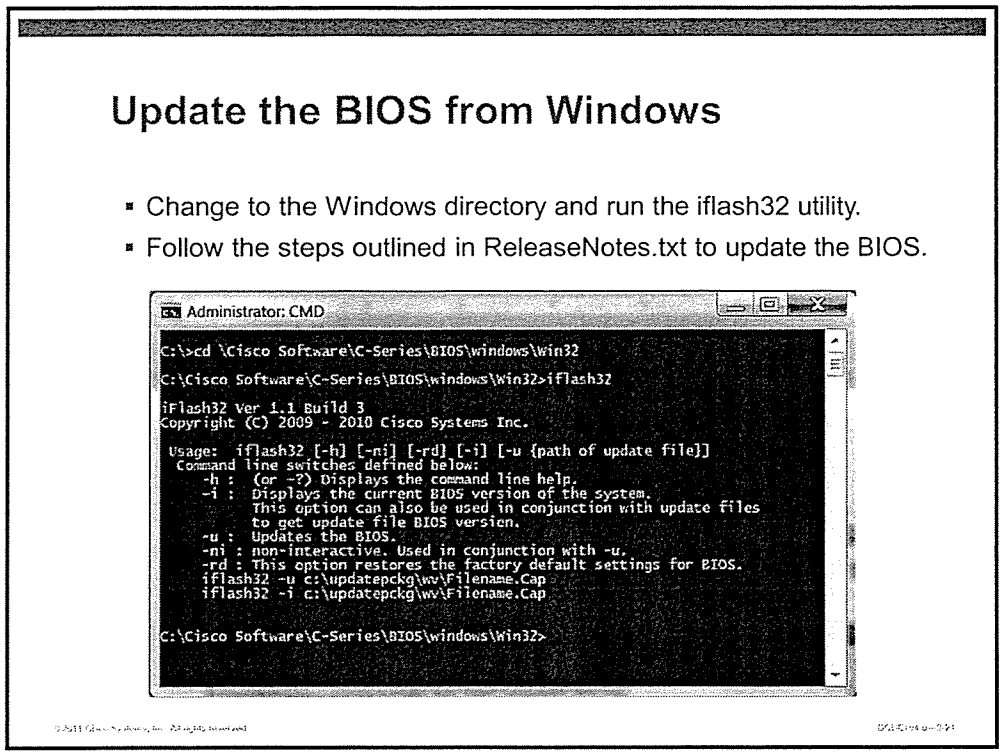
Step 2 Change to the Linux directory and untar the iflash32.tar.gz archive.

Step 3 Change into the new Linux directory and read the ReleaseNotes.txt file for the live update procedure.

Step 4 Restart the server for the new BIOS update to take effect.

Note This method requires downtime while the server reboots and executes the new BIOS.

Update the BIOS from Windows



To update the BIOS from a supported Microsoft Windows operating system running on the C-Series server, follow these steps:

Step 1 Download and expand the BIOS .zip archive to the local file system.

Step 2 Change to the "windows" directory and read ReleaseNotes.txt.

Step 3 Open a command line window with Administrator privileges and change into the x64 directory.

Step 4 Run the iFlash32 utility to update the BIOS.

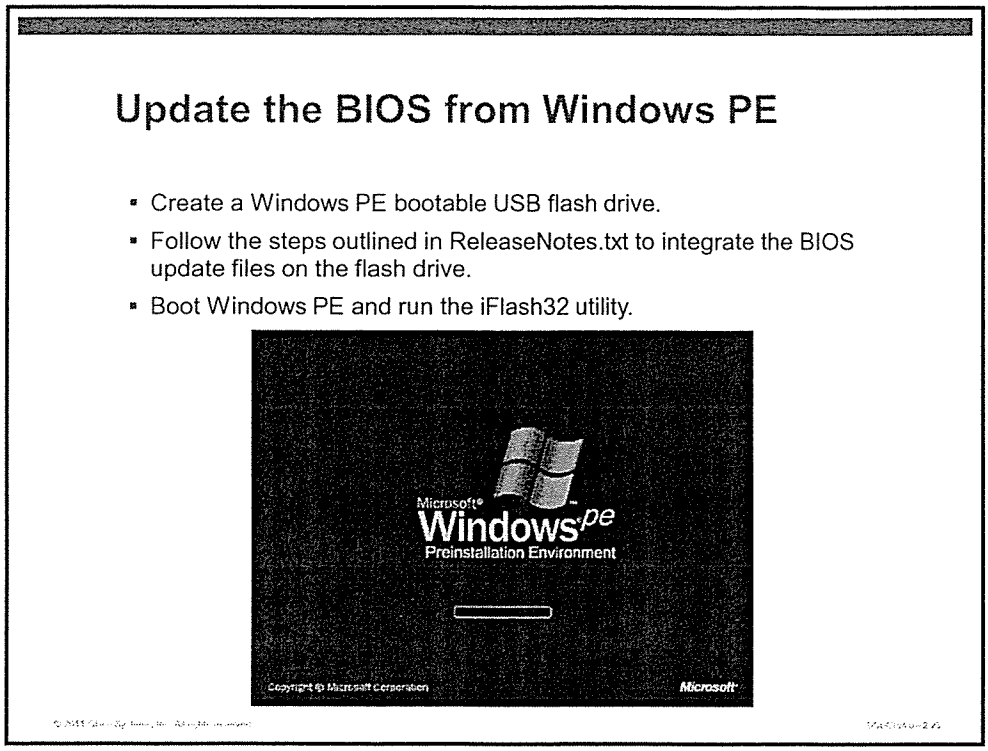
Step 5 Restart the server for the new BIOS update to take effect.

Note This method requires downtime while the server reboots and executes the new BIOS.

Update C-Series BIOS Before Loading Operating System

This topic discusses how to update the C-Series BIOS before loading the operating system.

Update the BIOS from Windows PE



Windows Preinstallation Environment is a lightweight version of Windows XP, Windows Server 2003, Windows Vista, Windows 7, or Windows Server 2008 R2. It is used as a replacement for booting from floppy disks to run firmware updates or load an operating system.

Windows PE can be used to update Cisco UCS C-Series BIOS from USB flash memory, USB hard drive, or Preboot Execution Environment (PXE).

The process to update the BIOS from Windows PE is beyond the scope of this course. Here is an outline of the procedures necessary to create a bootable Windows PE BIOS update on USB flash memory:

Step 1 Download the Windows Automated Installation Kit (Windows AIK).

Step 2 Refer to the Windows AIK User Guide for installation instructions on USB flash memory (http://technet.microsoft.com/en-us/library/cc749528%28WS.10%29.aspx).

Step 3 Download and expand the BIOS .zip archive to the local file system.

Step 4 Change to the Windows directory and read ReleaseNotes.txt.

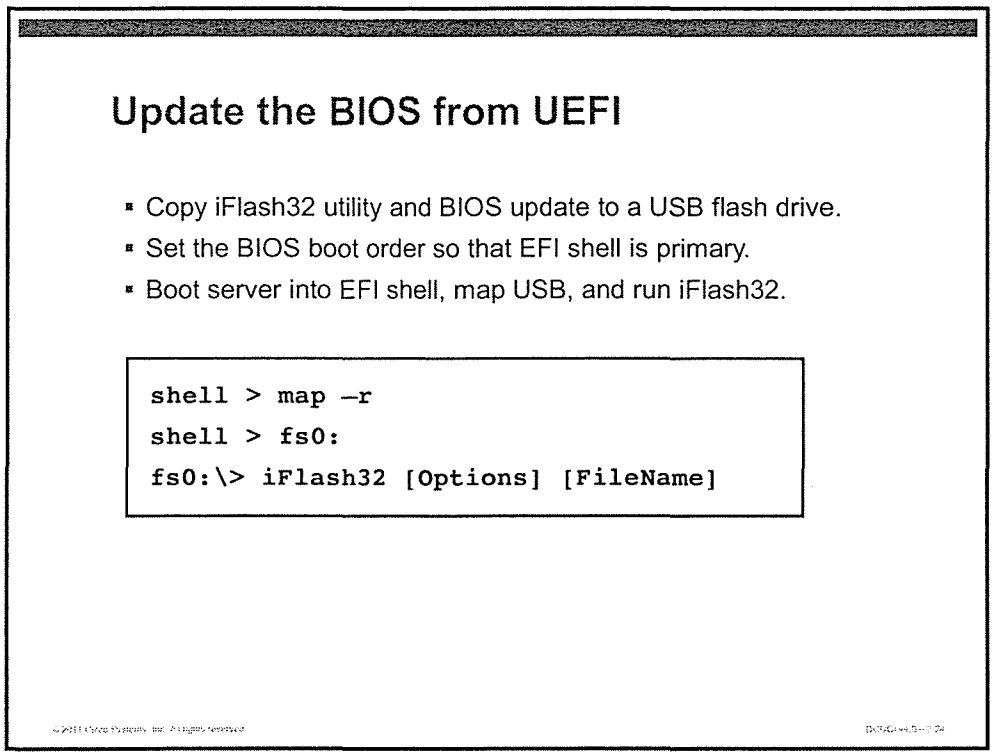
Step 5 Integrate the necessary iFlash32 utility, drivers, and BIOS update on the Windows PE bootable USB flash drive.

Step 6 Boot the server and set USB as the first item in the boot order, save changes, and reboot.

Step 7 Run the iFlash32 utility to update the BIOS.

Step 8 Restart the server for the new BIOS update to take effect.

Update the BIOS from UEFI



In the event of BIOS corruption (failure to power-on self-test [POST], and so on), the dedicated Cisco Integrated Management Controller interface allows for recovery without the need to process a Return Materials Authorization (RMA) on the server.

Use the following process to recover a corrupted BIOS:

Step 1 Download the model-specific BIOS firmware package from Cisco.com.

Step 2 Boot the system to EFI Shell.

Step 3 Copy IFlash32.efi and BIOS update file (also referred as capsule file) to a USB flash drive.

Step 4 Map the respective storage device in the system with the command:

```
shell > map -r
```

Step 5 Change the shell to the mapped device file system.

```
shell > fs0: (or fs1:)
```

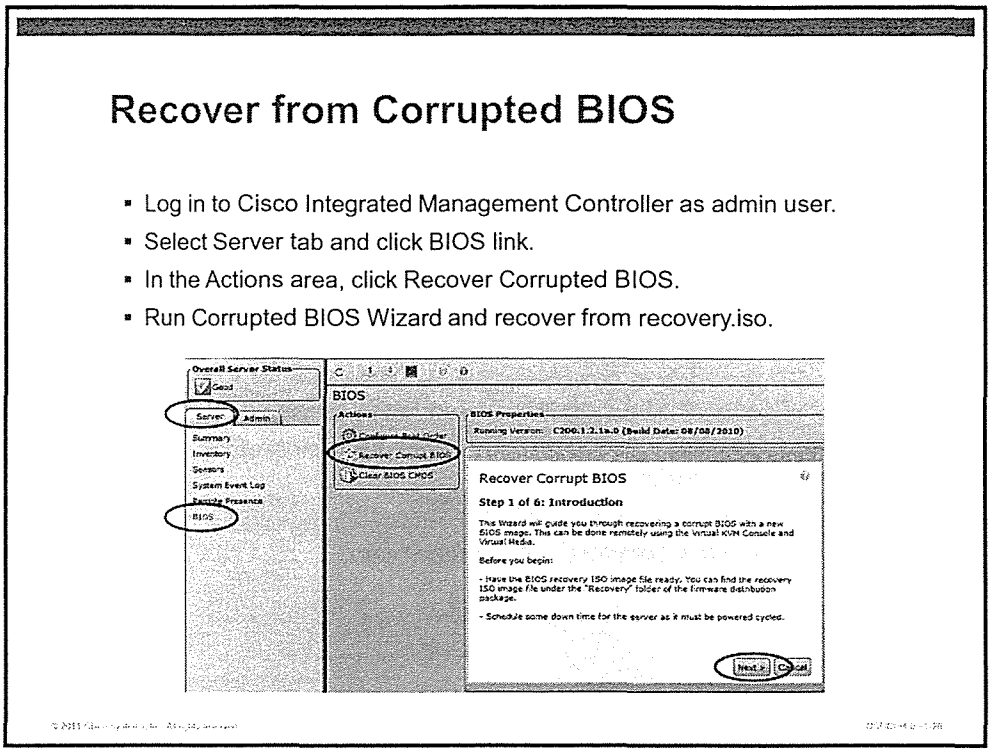
Step 6 Run the Iflash32 utility on the prompt.

```
fs0:\> iFlash32 [Options] [FileName]
```

Step 7 Reboot the server for the new BIOS update to take effect.

Recover from Corrupted BIOS

This topic discusses how to recover from a corrupted BIOS.



If there is BIOS corruption (failure to POST, incomplete BIOS update, and so on), the dedicated Cisco Integrated Management Controller interface allows for recovery without the need to process a RMA on the server.

Use the following process to recover from a corrupted BIOS:

Step 1 Download the model-specific BIOS firmware package from Cisco.com.

Step 2 Unzip the package and burn a copy of the recovery.iso file to a CD-ROM or copy it to a USB flash device.

Step 3 Select the **Server** tab and click the **BIOS** link.

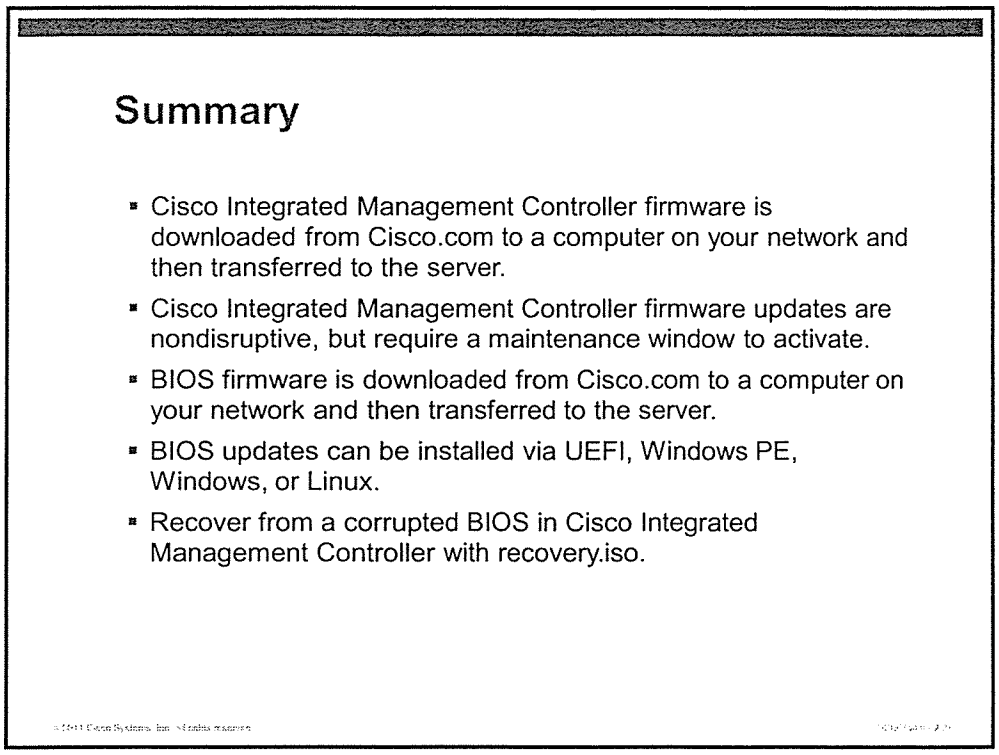
Step 4 In the Actions area, click **Recover Corrupted BIOS**.

Step 5 Run the Corrupted BIOS Wizard and recover from recovery.iso.

Step 6 Reboot the server for the new BIOS update to take effect.

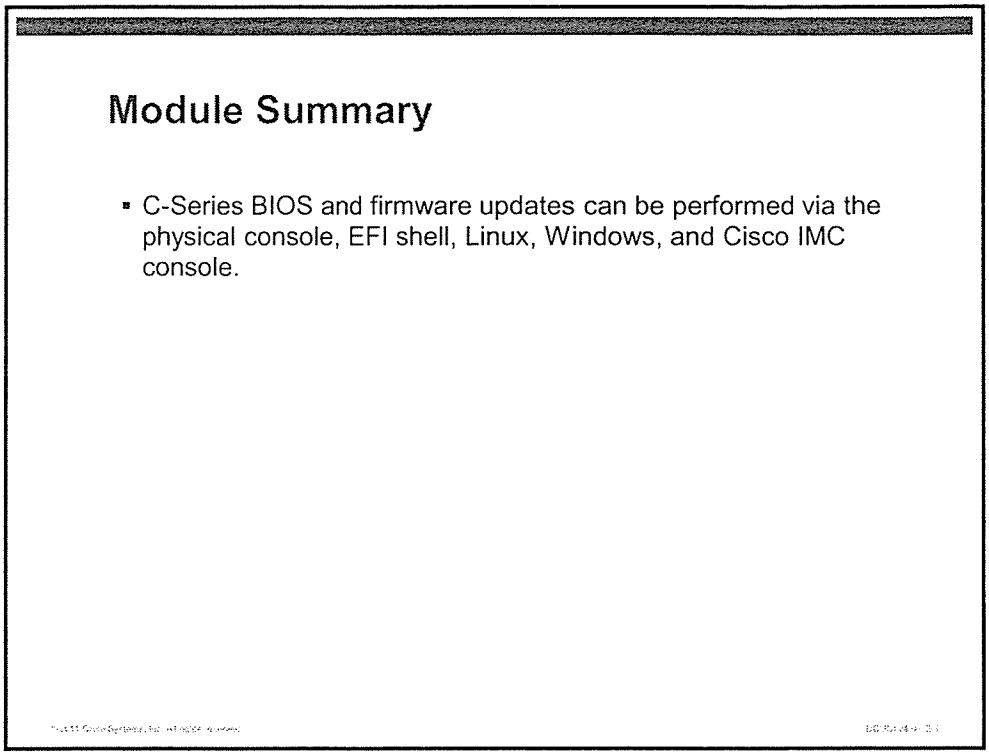
Summary

This topic summarizes the key points that were discussed in this lesson.



Module Summary

This topic summarizes the key points that were discussed in this module.



Cisco Unified Computing System (UCS) C-Series firmware and BIOS can be updated via a rich set of tools, including Extensible Firmware Interface (EFI) shell, Linux or Windows operating system, and Cisco Integrated Management Controller console.

For ease of management, and to facilitate feature improvements and new functionality, many components of the Cisco UCS C-Series platform include flash memory that can be updated with little or no impact on server operation. Customers with valid service contracts can download updated firmware from Cisco.com. In this module, you learned about updating firmware components of the Cisco UCS C-Series platform via the Cisco Integrated Management Controller, Cisco UCS Configuration Utility, the host operating system, and methods that do not require a host operating system installed.

References

For additional information, refer to this resource:

- Cisco, Inc. *Enterprise CIMC Firmware Management* at: http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/c/sw/gui/config/guide/1.1.2/Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_2_chapter12.html.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) What are three valid methods of configuring the Cisco Integrated Management Controller BIOS? (Choose three.) (Source: "Upgrading Firmware Components of the Cisco UCS C-Series Rack-Mount Servers")

A) BOOTP
B) DHCP
C) PXE boot
D) EFI shell
E) direct console configuration
F) Cisco UCS Server Configuration Utility

Q2) Which four methods can be used to update the Cisco UCS C-Series BIOS? (Choose four.) (Source: "Upgrading Firmware Components of the Cisco UCS C-Series Rack-Mount Servers")

A) replace BIOS EEPROM on motherboard
B) DHCP
C) Windows utility
D) Windows PE
E) Linux utility
F) bootable BIOS recovery CD
G) EFI shell

Q3) Which two protocols can be used to update the Cisco Integrated Management Controller firmware? (Choose two.) (Source: "Upgrading Firmware Components of the Cisco UCS C-Series Rack-Mount Servers")

A) FTP
B) TFTP
C) HTTP
D) SCP
E) HTTPS

Q4) What is the impact on an operating system running on the Cisco UCS C-Series server when Cisco Integrated Management Controller firmware is activated? (Source: "Upgrading Firmware Components of the Cisco UCS C-Series Rack-Mount Servers")

A) An ACPI call is made from the BIOS to the server operating system to perform a graceful shutdown.
B) A Network Connection-Sideband Interface (NC-SI) management connection gracefully shuts down the server operating system.
C) There is no impact to the server operating system. Only the management processor is unavailable.
D) You must manually shut down the server operating system to avoid downtime.

Q5) How do you recover from a corrupted BIOS? (Source: "Upgrading Firmware Components of the Cisco UCS C-Series Rack-Mount Servers")

A) Use Cisco Integrated Management Controller console to perform BIOS recovery.
B) Use a bootable BIOS recovery CD.
C) Press F9 during power-on to load backup BIOS.
D) Replace BIOS EEPROM on motherboard.

Module Self-Check Answer Key

Q1) B, D, E

Q2) C, D, E, G

Q3) B, E

Q4) C

Q5) A

Module 3

Cisco IMC Configuration

Overview

To facilitate lights-out management, maintenance, Remote Monitoring, and server hardware provisioning, Cisco created Cisco Integrated Management Controller (IMC) as a central console that can be accessed via web browser or Secure Shell (SSH) command-line interface (CLI).

Unlike the server BIOS, which is only accessible at the time of power-on self-test (POST), Cisco Integrated Management Controller runs on a dedicated "server within the server" with its own CPU, RAM, and flash memory complex. Because it is not tied to the operating system running on the C-Series host, it operates autonomously. However, Cisco Integrated Management Controller can control which server hardware resources are available to the host operating system.

This module illustrates the use of the Cisco Integrated Management Controller to provision Cisco Unified Computing System C-Series rack servers for Remote Monitoring, management, and initial operating system load.

Module Objectives

Upon completing this module, you will be able to perform startup configuration of a new Cisco UCS C-Series server from initial power-up to operating system load through virtual keyboard, video, mouse (KVM) or physical DVD media.

This ability includes being able to meet these objectives:

- Configure the Cisco Integrated Management Controller to allow secure remote management of Cisco UCS C-Series servers
- Provision Cisco UCS C-Series hardware with Cisco Integrated Management Controller to prepare for operating system installation and management

Lesson 1

Configuring Cisco IMC

Overview

Access to server management resources is required, whether the device is running or not. In this lesson, you will learn how to configure initial in-band management and explore services available in the Cisco Integrated Management Controller (IMC) via web browser and command-line interface (CLI).

Objectives

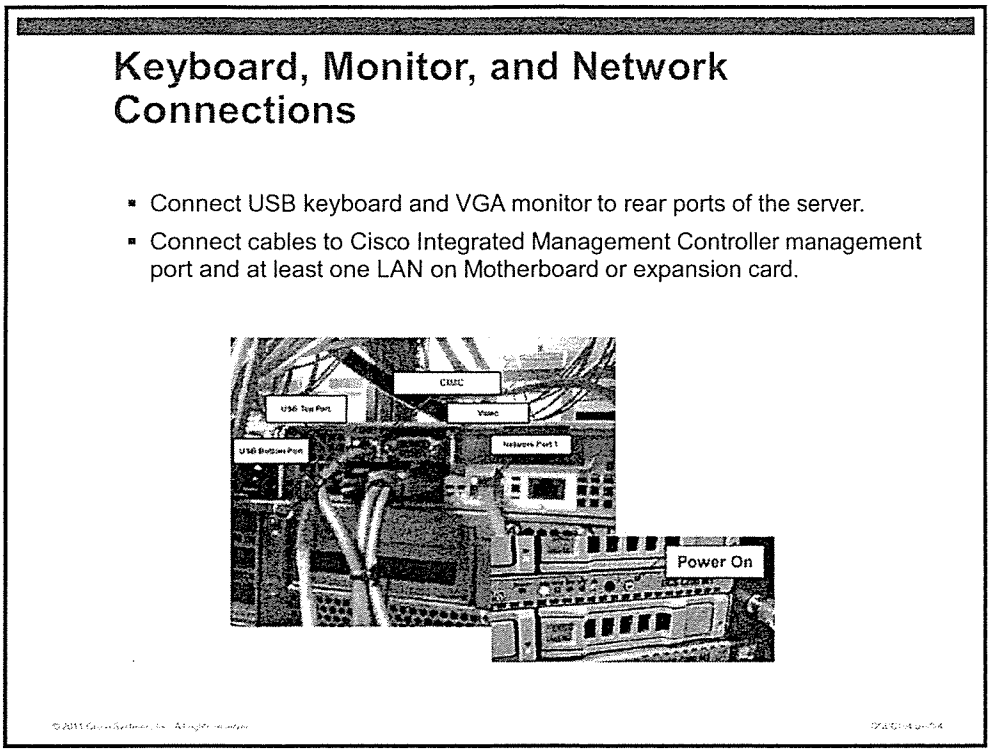
Upon completing this lesson, you will be able to configure in-band access to Cisco Integrated Management Controller. This includes being able to meet these objectives:

- Access the server BIOS
- Configure Cisco IMC with an IP address to enable in-band management access
- Monitor sensor and log data in Cisco IMC
- Define actions that are based on sensor thresholds
- Export technical support data to TFTP server

Access the Server BIOS

This topic describes the initial connections that are necessary to access the server BIOS in order to validate time and date settings and allow all diagnostic messages to appear on the console during power-on self-test (POST).

Keyboard, Monitor, and Network Connections



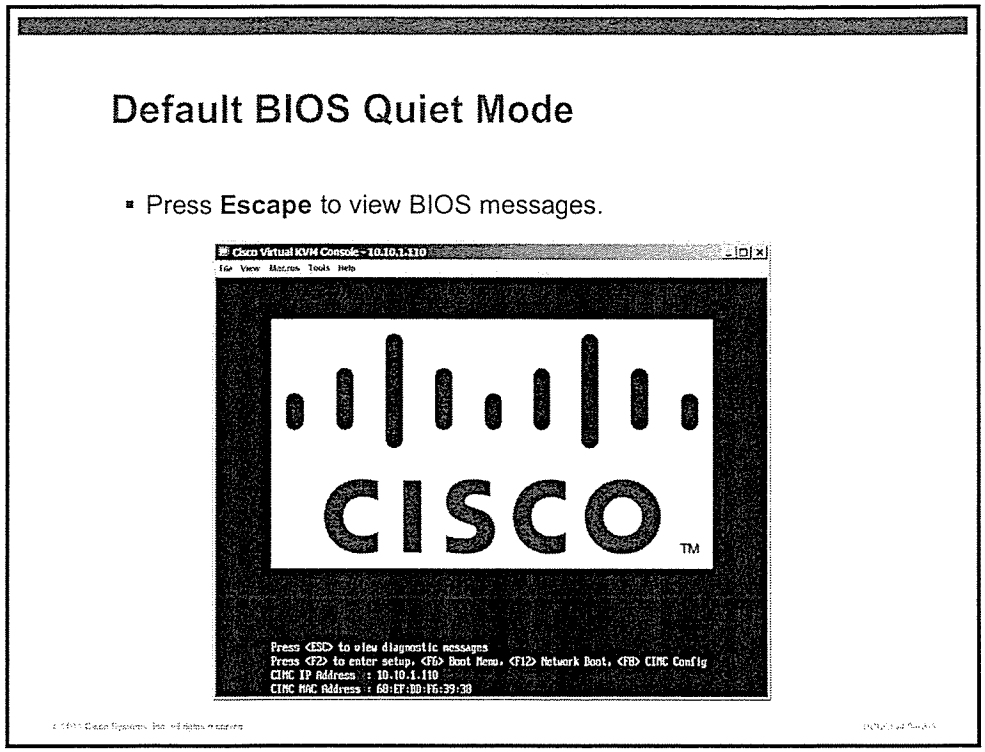
The initial connection to your C-Series server must be made with a physical keyboard and monitor to interact with the BIOS setup. The figure illustrates a Cisco UCS C200 server that is viewed from the rear and front. Although not shown, there is a port on the front of the server to connect a keyboard, video, mouse (KVM) dongle that supplies a DB-15 VGA port, a two-port USB, and a DB-9 serial port. It can also be used for initial setup.

Note The KVM dongle has priority over the rear panel connections. The rear monitor, USB, and serial ports are disabled when the KVM dongle is attached to the front panel. After the KVM dongle is removed, control reverts to the rear panel KVM connections.

The Cisco Integrated Management Controller management port is a 10/100/1000BaseTX port and requires a Category 6 Ethernet cable to operate in a Gigabit switchport. The two LAN-on-motherboard (LOM) connections on the C200, C210, and C250 are also 10/100/1000BaseTX and similarly require Category 6 cabling. The number and type of LOM ports vary by C-Series model.

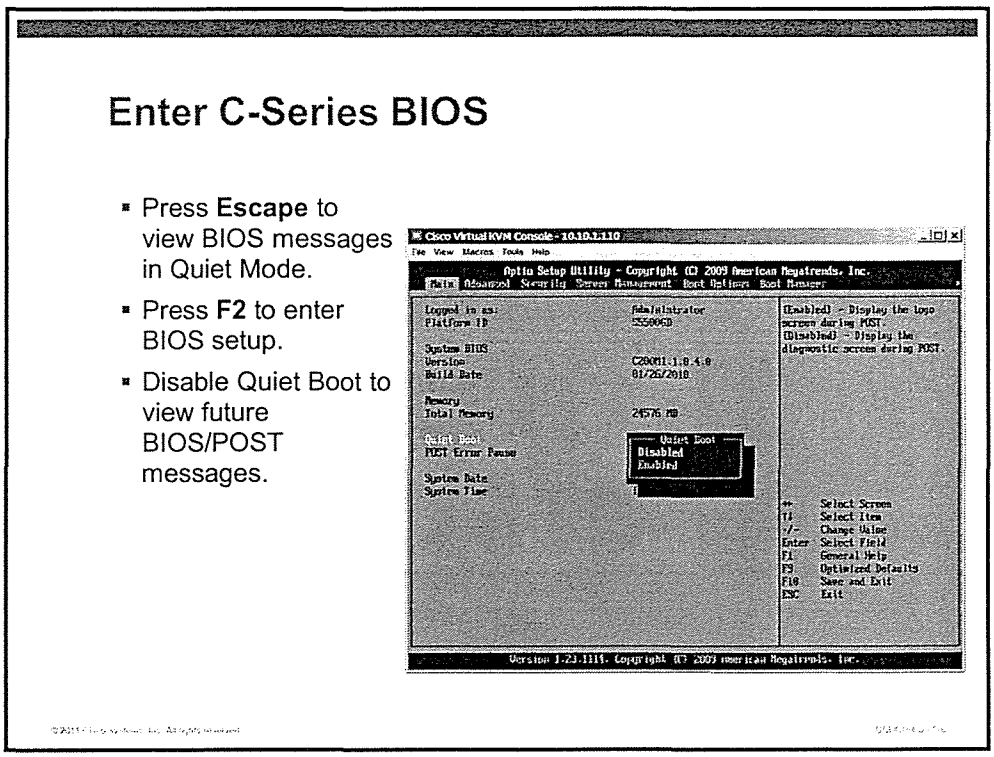
A network connection to the Cisco Integrated Management Controller port is required to remotely access Cisco Integrated Management Controller management and monitoring services. At least one connection to a LOM or expansion card is necessary for a host operating system or hypervisor to communicate externally. Note that 10-Gigabit Ethernet ports require either copper twin-axial or optical small form-factor pluggable plus (SFP+) connections.

Default BIOS Quiet Mode



A C-Series server with a factory default BIOS loads with "Quiet Mode" enabled. You will recognize Quiet Mode by the large Cisco logo banner during POST. Quiet Mode suppresses all of the startup messages and, in the initial setup phase, it can mask configuration issues that you need to address. You may temporarily disable Quiet Mode by pressing **Escape** during POST.

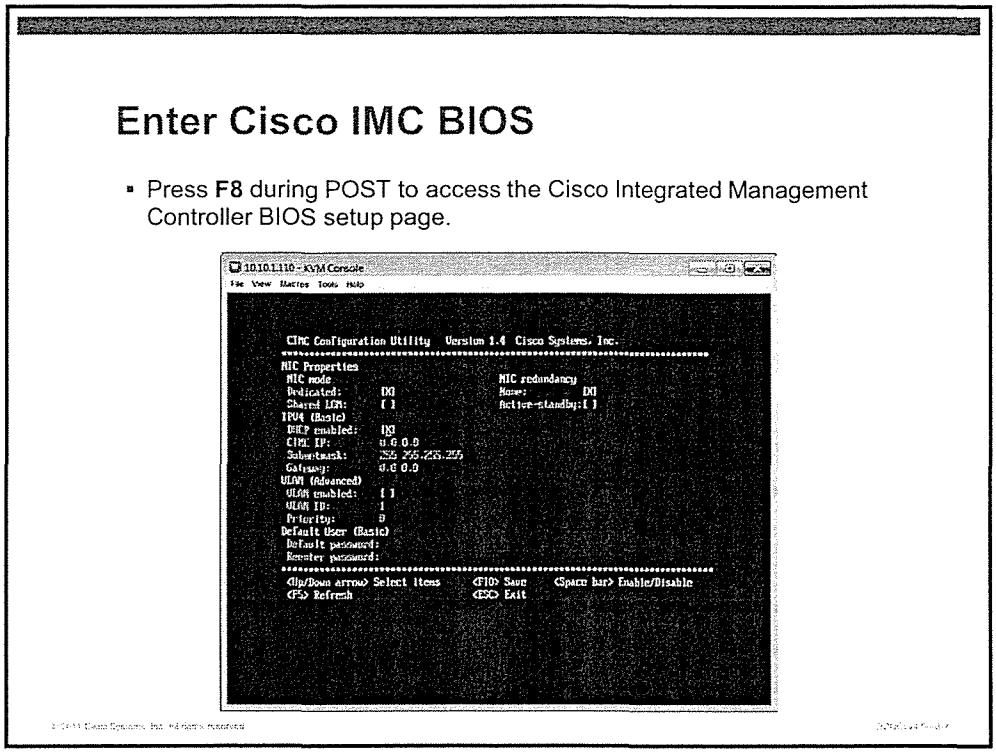
Enter C-Series BIOS



You should disable Quiet Mode until you have achieved a stable configuration. Press **Enter** on the Quiet Mode selection, use the arrow key to select **Disabled**, and press **Enter** again.

Validate that time and date settings are correct and make adjustments as necessary. Be sure to press **F10** to save settings before exiting BIOS setup.

Enter Cisco Integrated Management Controller BIOS



Press **F8** during POST to access the Cisco Integrated Management Controller BIOS. The Cisco Integrated Management Controller BIOS is specific to the management processor and is completely isolated from the server BIOS.

This screen allows you to configure the necessary TCP/IP information (IP address, subnet mask, and default gateway) to establish remote connectivity to the server. The default configuration is for the Cisco Integrated Management Controller to use DHCP to obtain its IP address. To enter a static IP address, select that item and use the spacebar to uncheck the box for DHCP.

The Cisco Integrated Management Controller interface default is to use an access VLAN. If the Cisco Integrated Management Controller interface connects to an 802.1Q trunk port, select the **VLAN Enabled** item and use the spacebar to toggle an X. Enter the VLAN associated with the Cisco Integrated Management Controller IP address.

The default username is "admin" and the default password is "password." This should be changed immediately following the guidelines of your organization password policy.

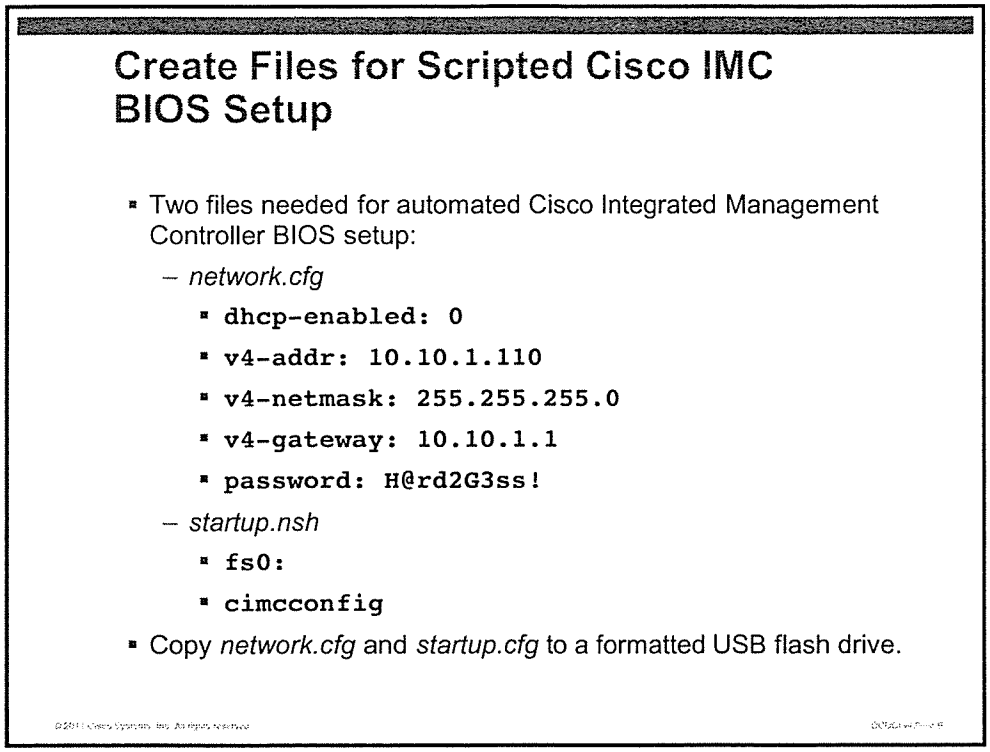
When you can reach the server Cisco Integrated Management Controller via a browser, the physical connections for keyboard, monitor, and mouse can be unplugged. Any Cisco Integrated Management Controller session can open a KVM-over-IP window, as if you were on the physical console.

In Dedicated NIC mode, Cisco Integrated Management Controller is available from the dedicated Cisco Integrated Management Controller 10/100/1000 port on the rear of the server. In Shared LOM mode, the LOM ports are dedicated for access to Cisco Integrated Management Controller. They can be configured for no redundancy (one link active), active-standby (one link active, the other active upon failure), and active-active (two links active). Active-active links require a unique IP address on the same subnet.

Perform Scripted Setup of Cisco IMC BIOS

This topic describes a scripted configuration of the Cisco Integrated Management Controller BIOS.

Create Files for Scripted Cisco Integrated Management Controller BIOS Setup



The Unified Extensible Firmware Interface (UEFI) can be leveraged to automate and speed the deployment of servers by scripting the Cisco Integrated Management Controller BIOS setup.

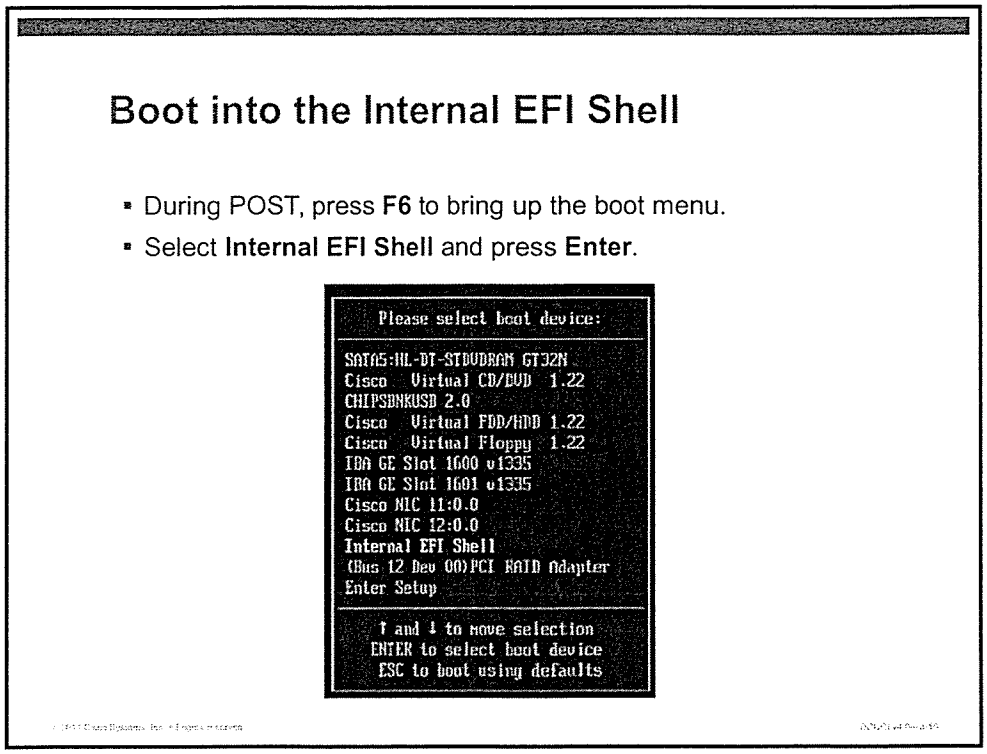
Two files must be created and copied to a blank USB flash drive:

- network.cfg: This file contains all of the configurable values for the Cisco Integrated Management Controller BIOS.
- starup.nsh: This file directs EFI to point the shell to the USB flash drive (fs0:) for input and execute the **`cicmconfig`** command, which reads the network.cfg file and configures the Cisco Integrated Management Controller BIOS. Administrators can immediately connect to the Cisco Integrated Management Controller IP address via a web browser.

To configure another C-Series server, simply edit the IP address information in the network.cfg file and repeat the process.

For complete syntax information for script files, refer to the Cisco publication, *Cisco UCS C200 Server Installation and Service Guide.*

Boot into the Internal EFI Shell



When prompted during POST, press **F6** to access the boot menu. Use the arrow key to select **Internal EFI Shell** and press **Enter**. This will launch the EFI shell process and interrupt normal booting so that you can configure the Cisco Integrated Management Controller BIOS via the simple script files that you created.

startup.nsh Executes in the EFI Shell

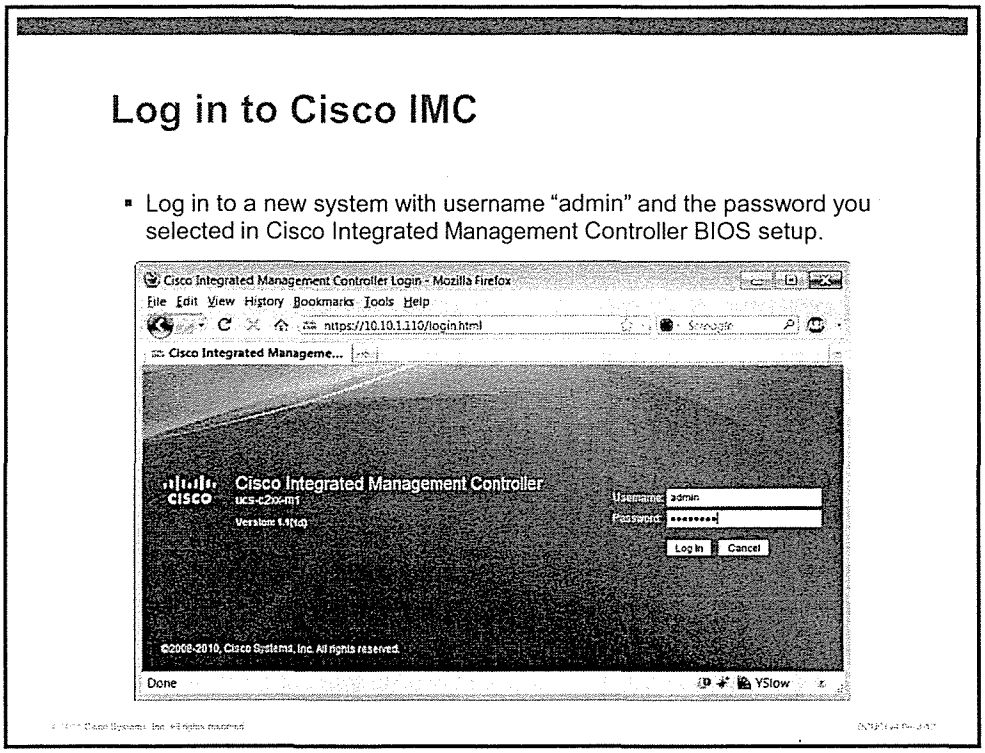
Startup.nsh Executes in the EFI Shell

- The EFI Shell reads the startup.nsh file and executes the **`cimcconfig`** script that loads the network.cfg file to program the Cisco Integrated Management Controller BIOS settings.

If you do not press **Escape** within 5 seconds of loading the EFI shell, it automatically scans for a USB flash or hard drive that contains startup.nsh and executes the commands in the file. When the script finishes, it indicates that the Cisco Integrated Management Controller configuration was successful. If there was a problem with the script, EFI shell writes the errors to errors.txt on the USB flash drive or hard disk. Type "**exit**" and press **Enter** to exit the EFI shell and boot the server.

For information on all of the commands available in the EFI shell, refer to the official *UEFI Shell Specification* (http://www.uefi.org/home).

Log in to Cisco Integrated Management Controller



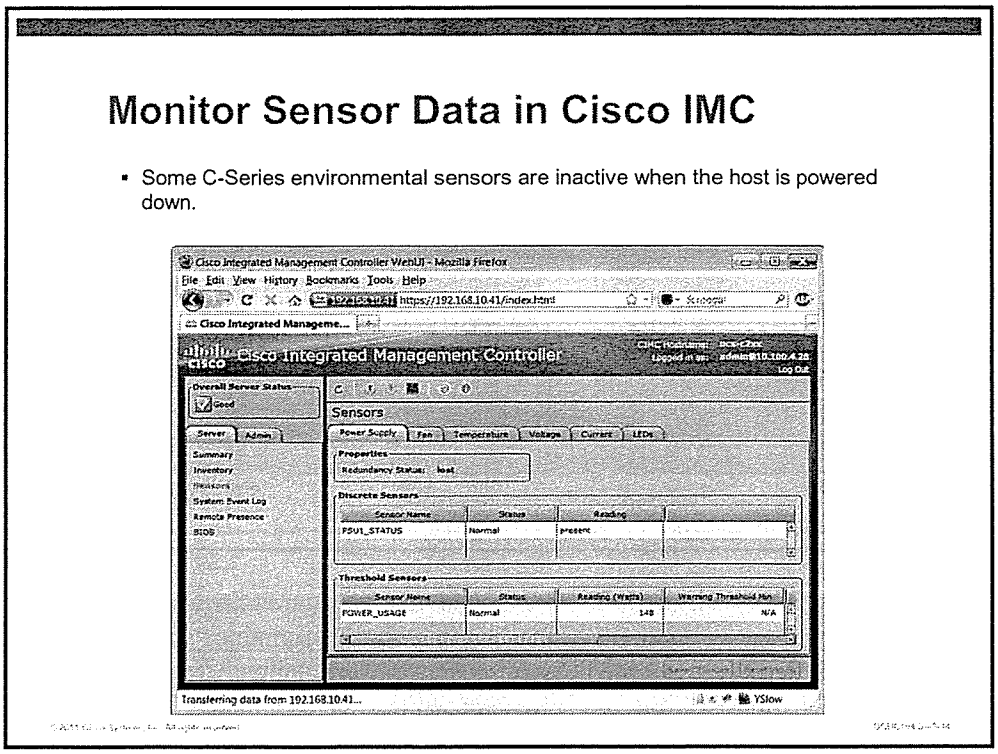
Point your web browser to the IP address that you configured for Cisco Integrated Management Controller management using HTTPS. Log in with the username "admin" and the password that you specified in the scripted Cisco Integrated Management Controller BIOS setup. If you did not change the password, the default credentials are username = "admin" and password = "password."

If you cannot reach the Cisco Integrated Management Controller login page, reboot the server and press **F8** to validate that your IP address, subnet mask, and default gateway are set correctly.

Monitor Sensor and Log Data in Cisco IMC

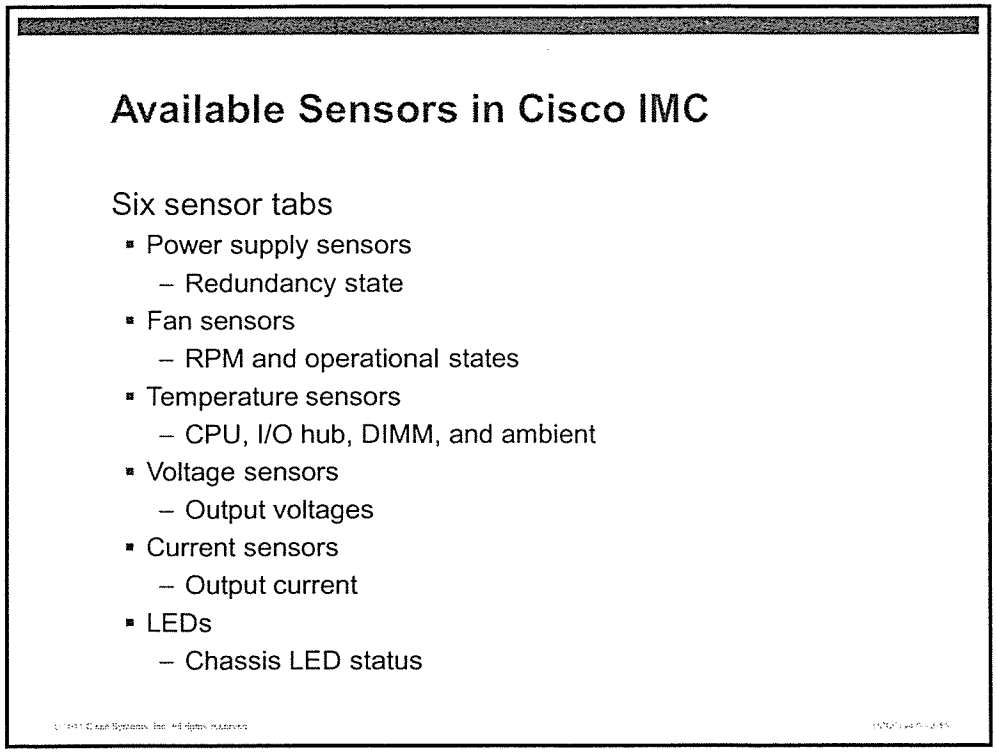
This topic describes how to monitor sensor and log data in Cisco Integrated Management Controller. You will learn about the available sensors in Cisco Integrated Management Controller and the functions of each.

Monitor Sensor Data in Cisco IMC



Although the Cisco Integrated Management Controller operates when the server is in standby mode (system has input power, but only the management plane is operational), sensor data is unavailable until the server exits standby mode and boots.

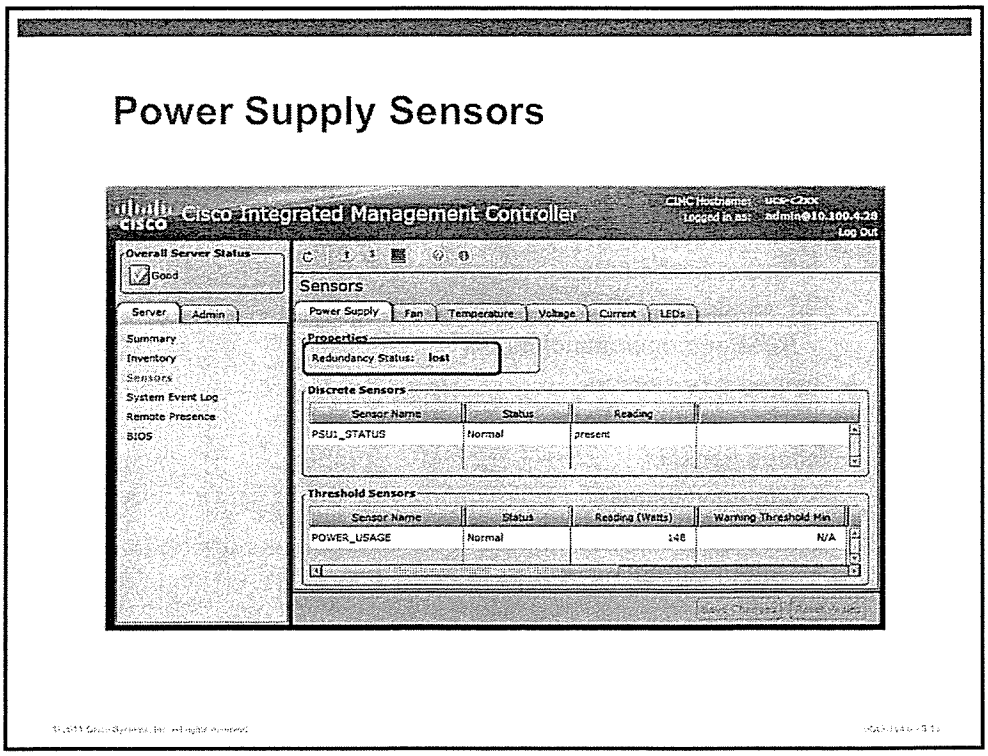
Available Sensors in Cisco IMC



As of Cisco Integrated Management Controller version 1.2(1a), there are six categories of sensors that are monitored while an operating system or hypervisor is running:

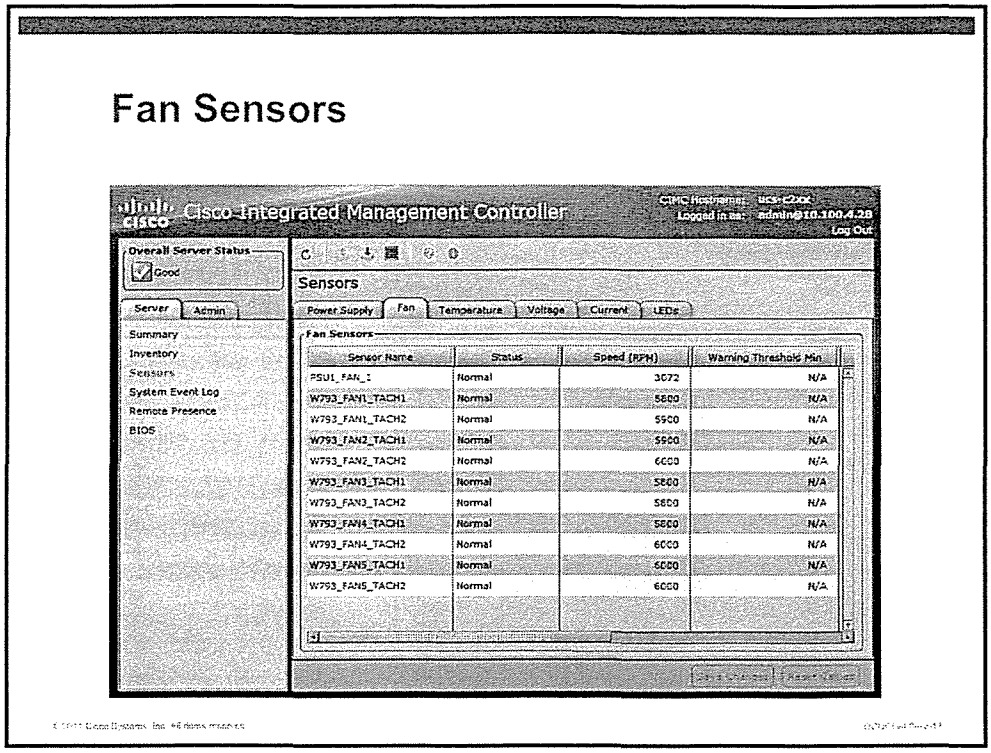
Sensor	Description
Power supply	Monitor the power redundancy state, and input and output wattage of installed power supplies.
Fan	Monitor RPM and operational states of power supply fans and chassis fans. The CPU heat sinks are passive and rely on the chassis fans to route enough cool air to maintain safe operating temperature.
Temperature	Monitor CPU, I/O Hub, DIMM, and ambient chassis temperature.
Voltage	Monitor the output voltages of all DC voltage sources.
Current	Monitor CPU voltage regulator and power supply DC current.
LEDs	Monitor the current state of chassis LED colors.

Power Supply Sensors



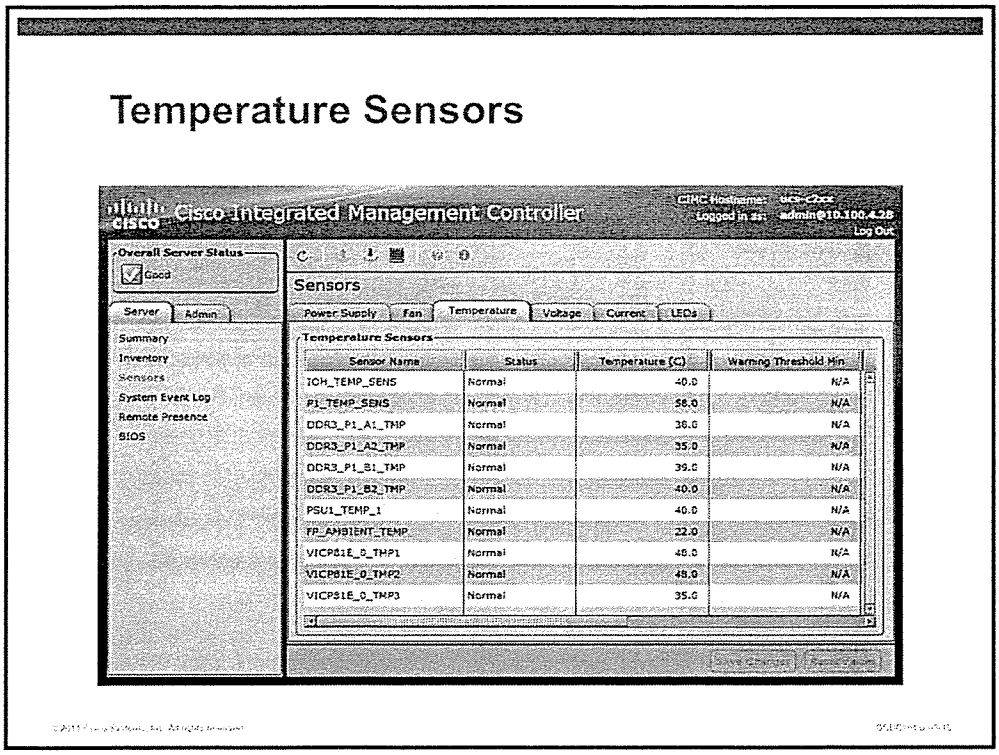
The Power Supply Sensor tab lists the current state of redundancy, the input and output wattage of both power supplies, and the factory-configured Warning and Critical thresholds for those values.

Fan Sensors



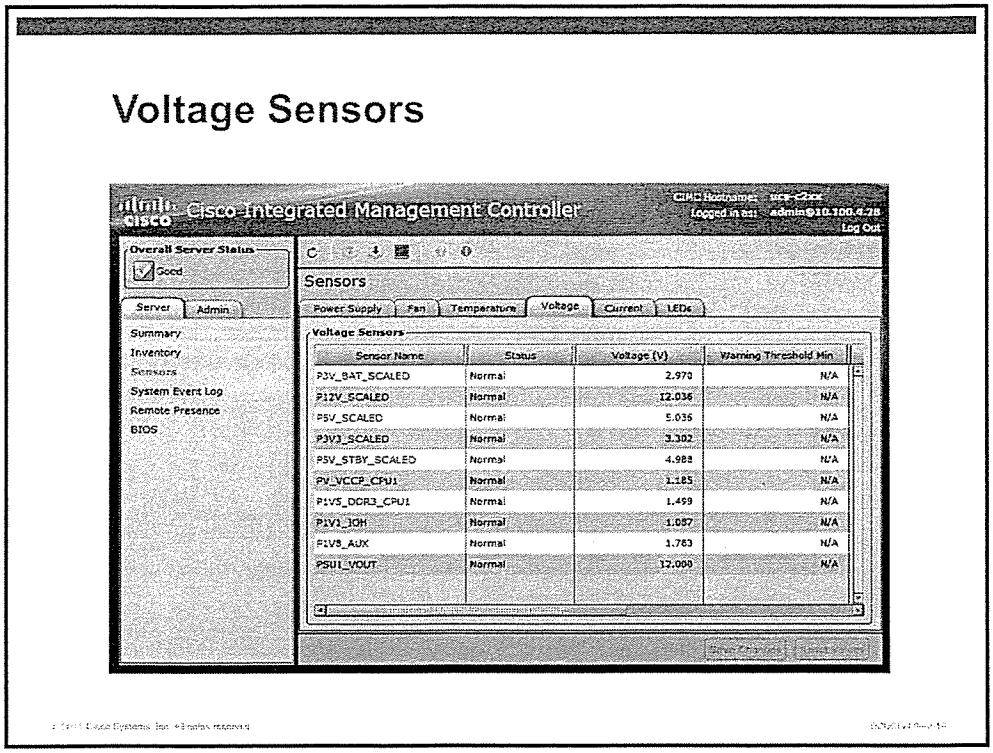
Fan speed is a good general metric of the thermal characteristics of a particular installation. In a controlled environment such as a data center, fan speed should vary little unless there is a failure of the HVAC system, an air inlet blockage, or fan failure. There are factory thresholds that are set for minimum RPM of chassis fans.

Temperature Sensors



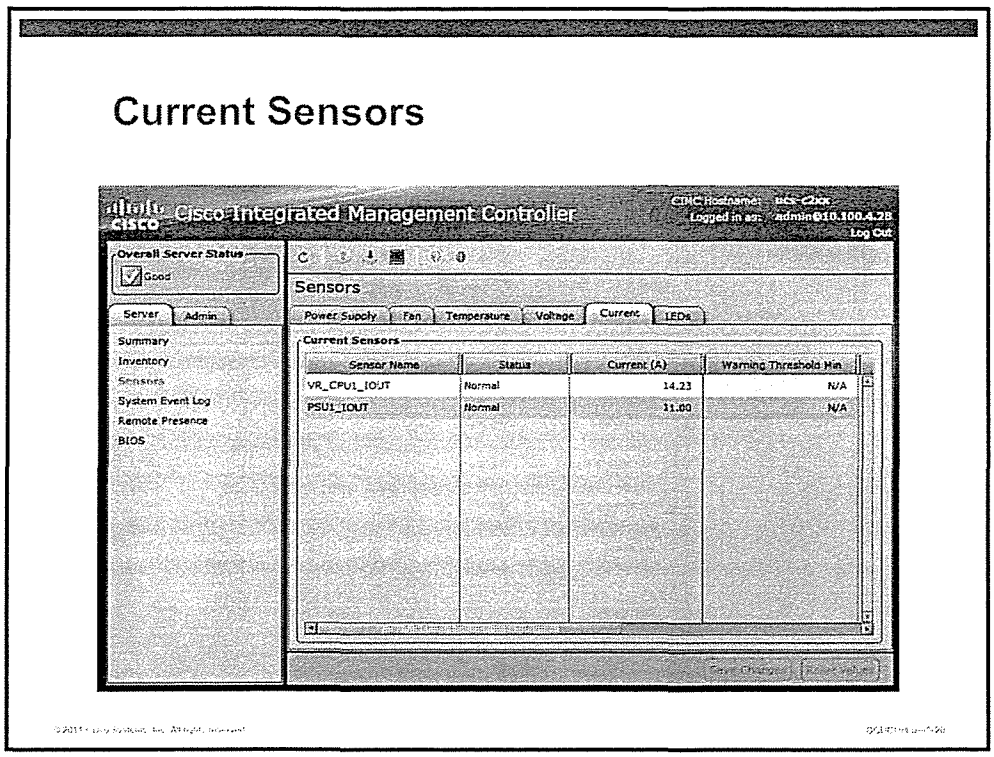
Temperature sensors are included to monitor the I/O hub, DIMM memory channels, power supplies, and ambient chassis temperature. The factory defaults for warning and critical thresholds should be compared against policies in place for equipment in your data center.

Voltage Sensors



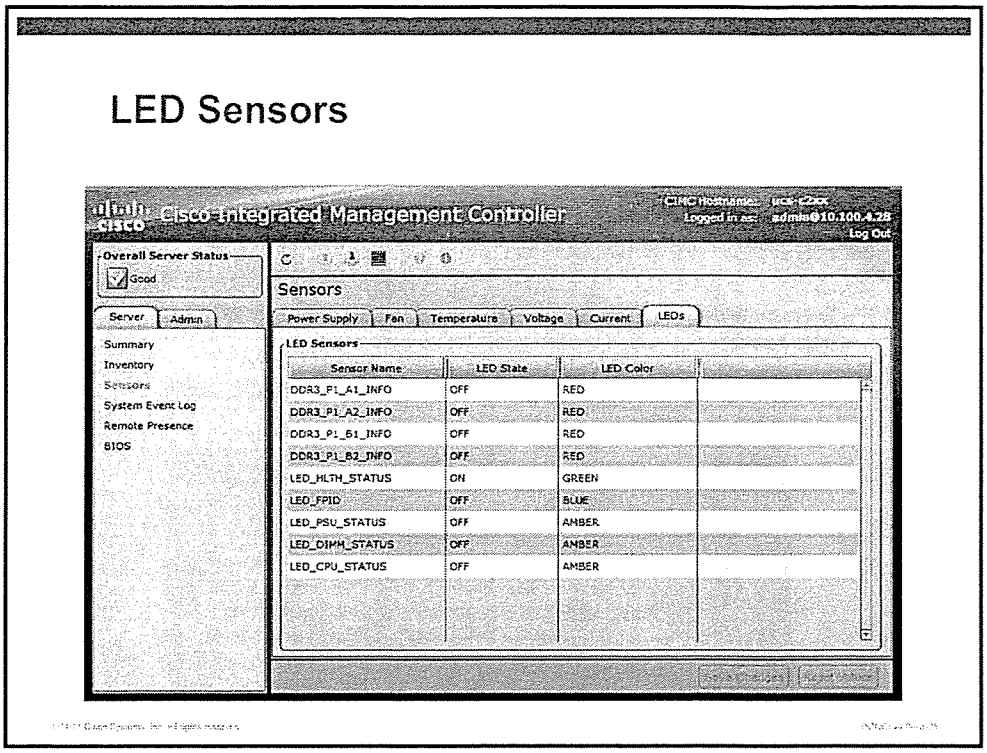
Voltage sensors monitor all DC voltage sources, including power supplies and NVRAM battery. There are factory voltage thresholds for warnings and critical conditions. Both over- and under-voltage conditions can affect the stability and reliability of a server.

Current Sensors



Current sensors monitor all DC voltage sources, including power supplies and NVRAM battery. There are factory voltage thresholds for warnings and critical conditions. Both over- and under-current conditions can affect the stability and reliability of a server.

LED Sensors

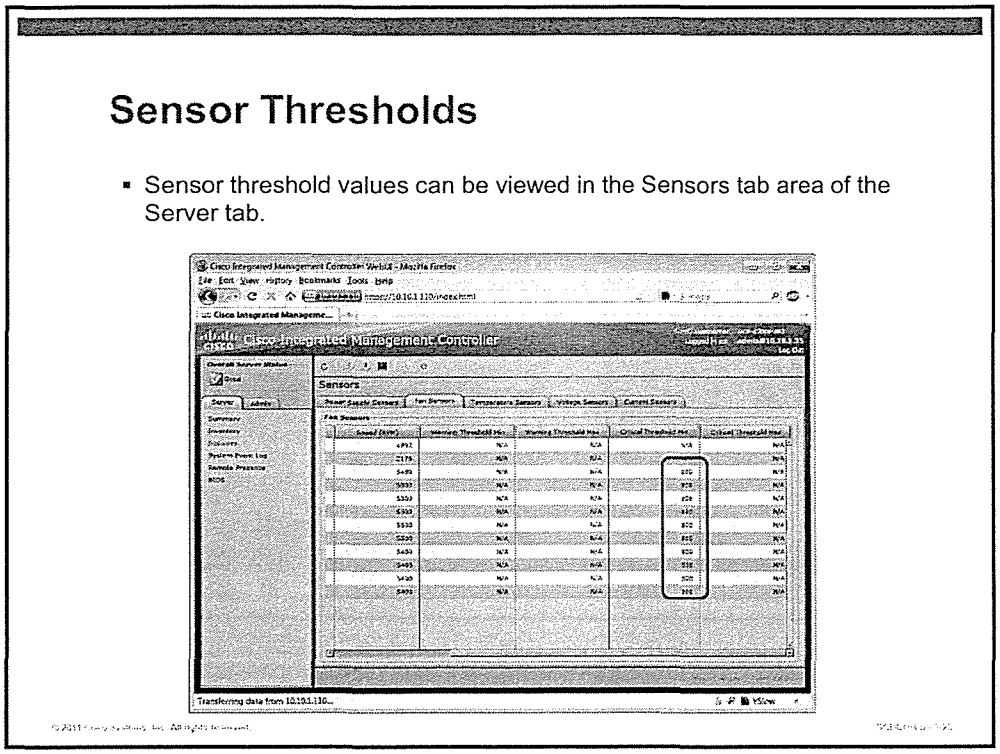


LED sensors allow for remote monitoring of the C-Series chassis LED state.

Sensor Thresholds, Alerts, and Actions

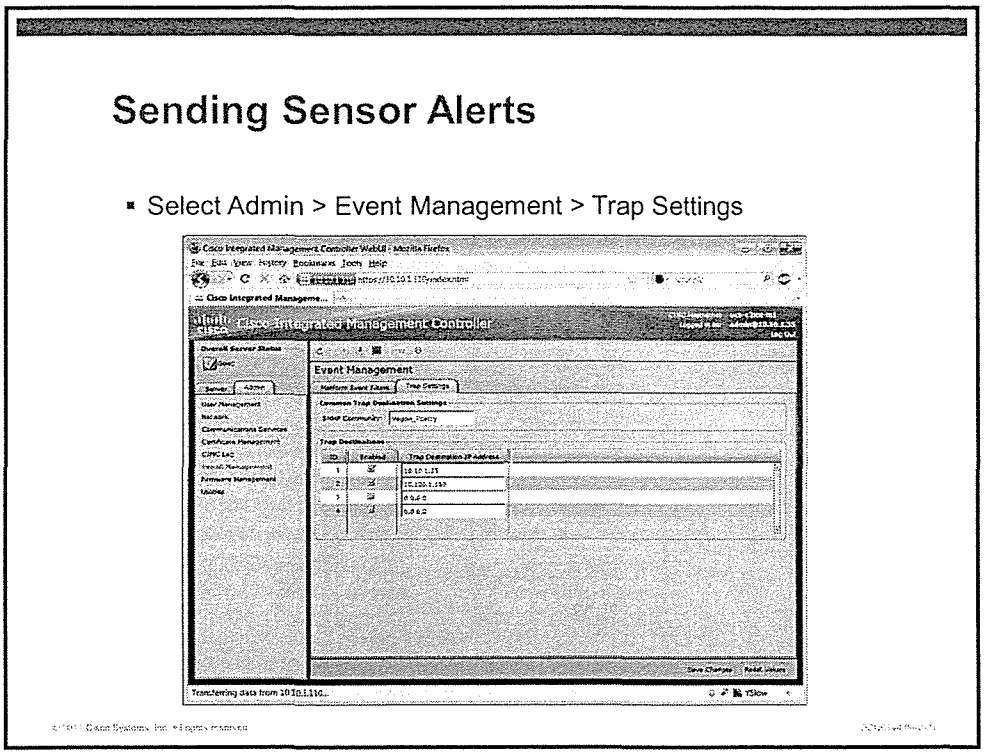
This topic describes sensor thresholds, alerts, and actions that are associated with those alerts.

Sensor Thresholds



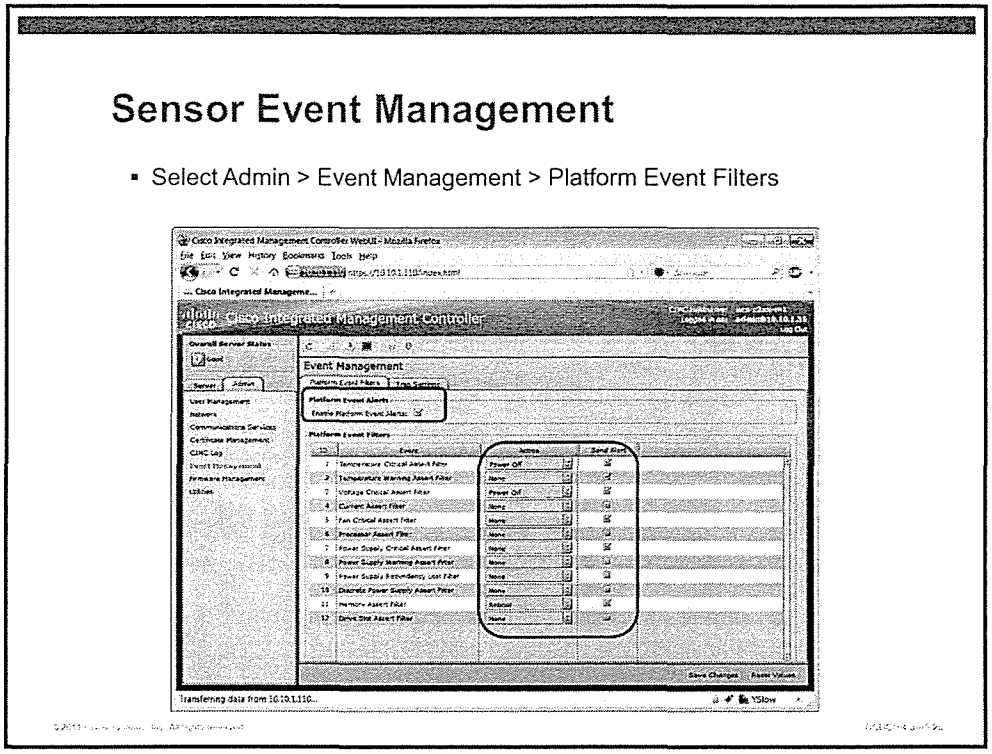
The thresholds for warning and critical conditions can be viewed in the content window of any sensor category. Thresholds are fixed based on industry best practices. Future releases of C-Series BIOS and Cisco Integrated Management Controller firmware may allow user-settable thresholds. In the figure, you can see if any chassis fan falls below 800 RPMs, which is considered a critical severity event.

Sending Sensor Alerts



C-Series servers send alerts via Community-based Simple Network Management Protocol version 2 (SNMPv2c) traps. You must configure an SNMP community string that matches the network management console acting as trap receiver. Up to four trap receiver destinations can be configured for redundancy and event correlation.

Sensor Event Management



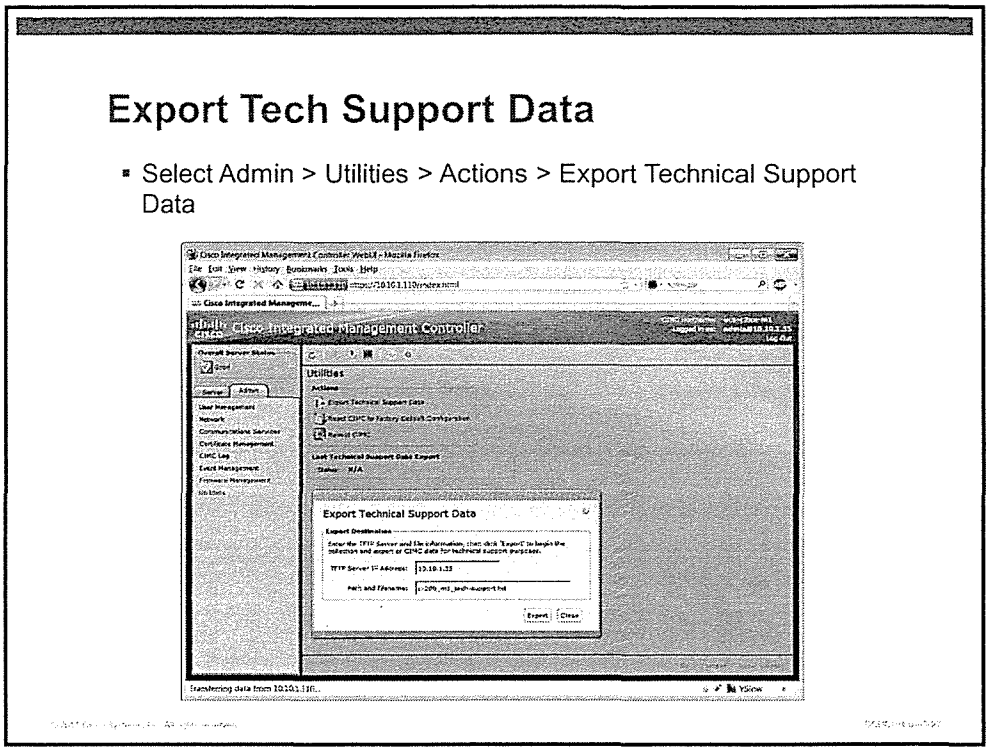
To send SNMP traps, you must globally enable alerting by checking the **Enable Platform Event Alerts** box. You then need to select which event classes are of interest to the network monitoring team. There is also the choice of event actions upon exceeding a particular threshold, which include None, Reboot, Power Cycle, and Power Off. When you have made your choices, be certain to click **Save Changes** in the lower-right portion of the window.

Reboot, Power Cycle, and Power Off only affect the operating system or hypervisor running on the C-Series server. Cisco Integrated Management Controller remains online.

Cisco IMC Logs and TFTP Export of Tech Support Data

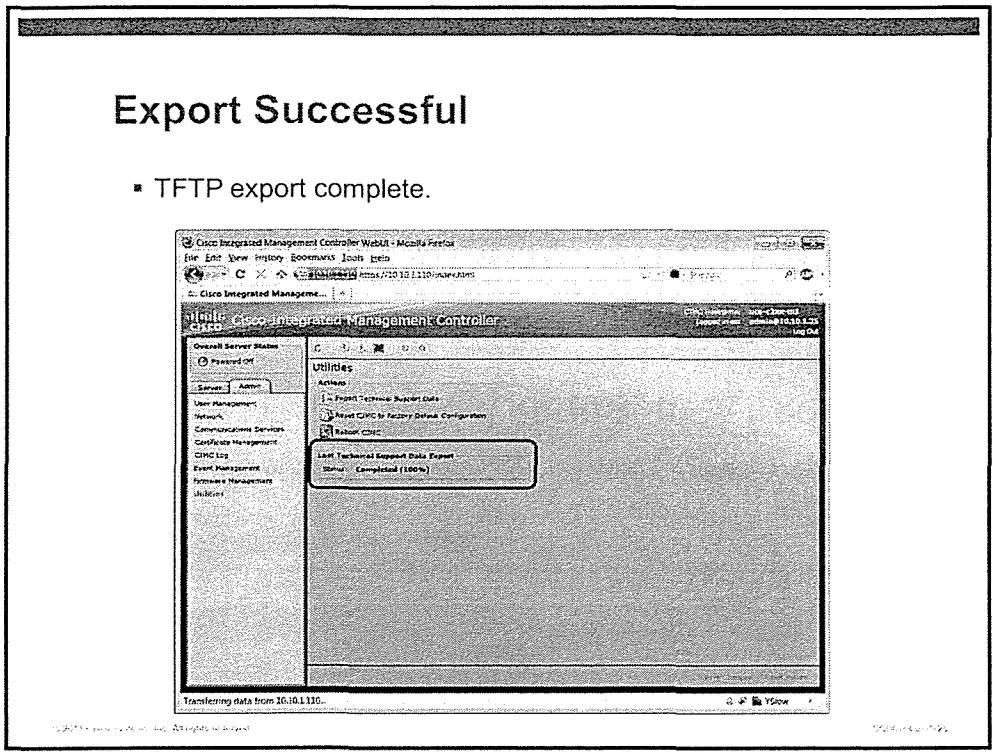
This topic describes how to collect and export critical technical support data. This topic also describes the System Event Log and Cisco Integrated Management Controller Log. You will also learn how to recover from administrative lockout and how to clear complementary metal-oxide semiconductor (CMOS).

Export Tech Support Data



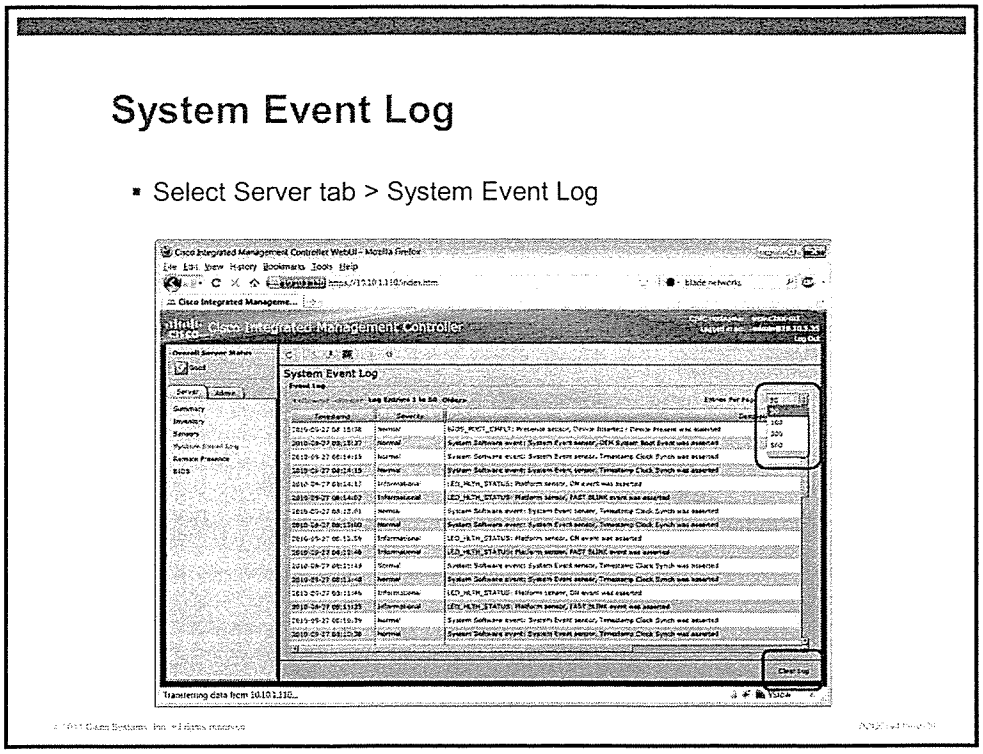
If you are actively troubleshooting a tech support issue with Cisco Technical Assistance Center (TAC), you need to know how to collect and export critical tech support data. Cisco Integrated Management Controller includes an easy-to-use collection system that exports your system support data to a TFTP server. Cisco Integrated Management Controller will update a progress indicator while it is collecting and sending data to the TFTP server. The resulting file is machine-readable by Cisco TAC.

Export Successful



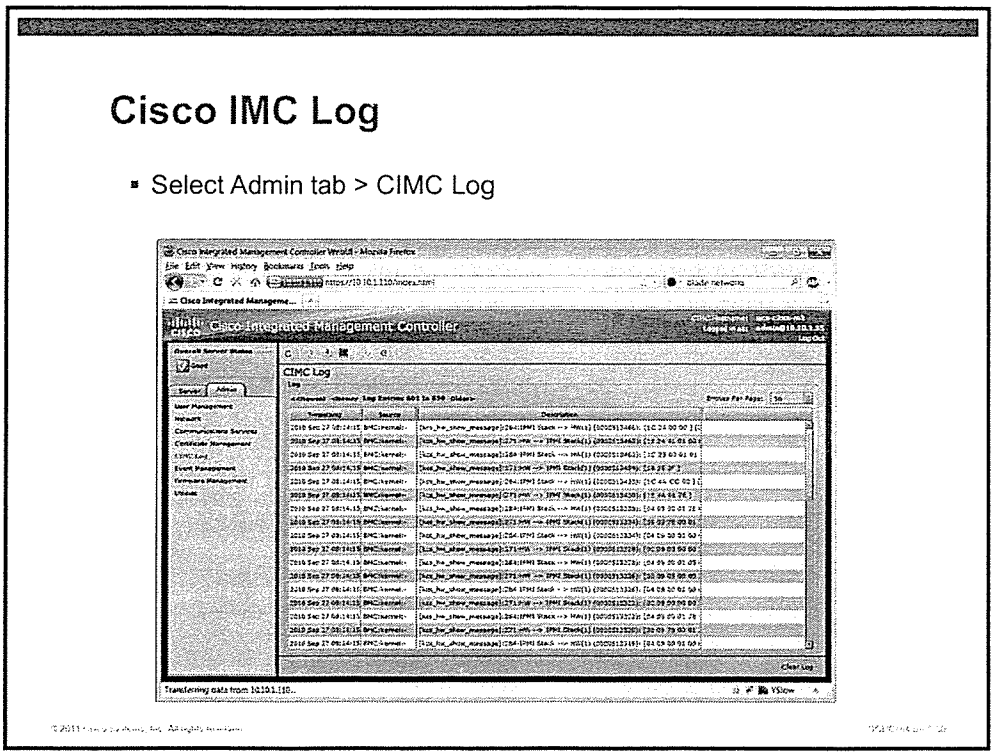
The status of Last Technical Support Data Export should indicate 100 percent.

System Event Log



The System Event Log (SEL) collects information about host hardware operation. The timestamp for log entries is based on the time and date that is set in the server BIOS. There are six severity levels: Unknown, Informational, Normal, Warning, Critical, and Non-Recoverable. You can select how many log entries to display per page and the SEL can be cleared by clicking **Clear Log** in the lower-right corner of the Cisco Integrated Management Controller SEL page.

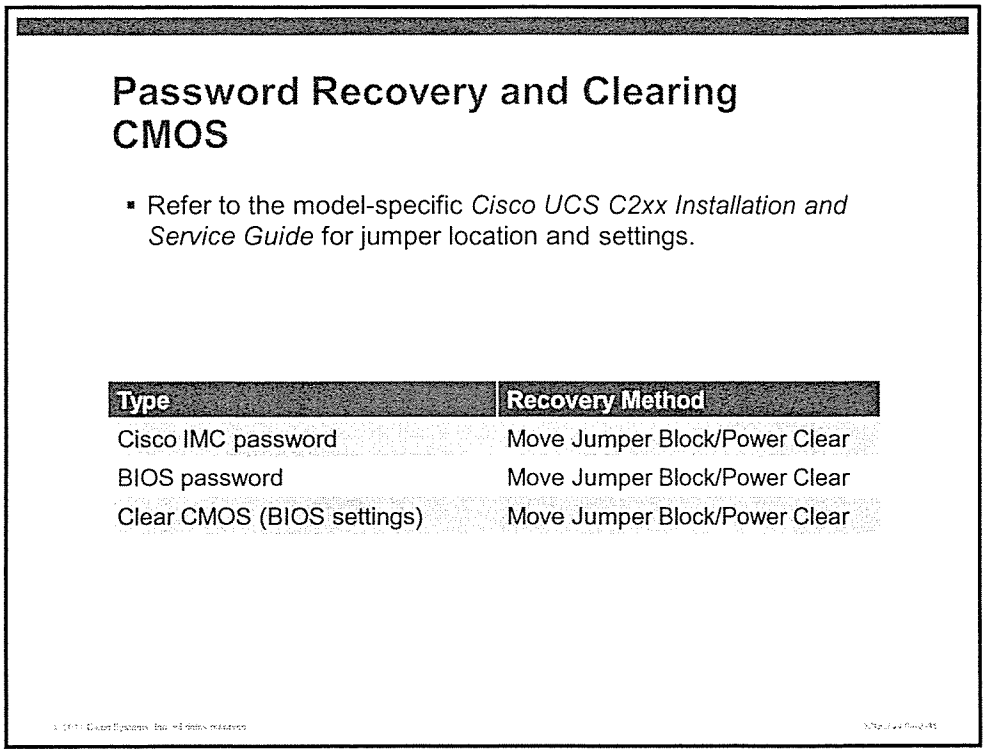
Cisco Integrated Management Controller Log



The Cisco Integrated Management Controller log collects information only about management processor operations and events and is maintained separately from the SEL. The timestamp for log entries is based on the time and date that is set in the server BIOS. If the server is running in standby mode, Cisco Integrated Management Controller does not have access to the real-time clock (RTC) on the motherboard. The timestamp will begin with January 1, 1970 at midnight (00:00). When the server is powered on, the Cisco Integrated Management Controller will begin to use the RTC setting for timestamps.

You can select how many log entries to display per page and the Cisco Integrated Management Controller log can be cleared by clicking **Clear Log** in the lower-right corner of the page.

Password Recovery and Clearing CMOS



The Cisco Integrated Management Controller admin password is critical to managing C-Series servers. If the password is forgotten or maliciously changed, you will be locked out of Cisco Integrated Management Controller GUI and CLI functions. To clear the Cisco Integrated Management Controller password, you must power off the server, remove power cords, and open the cover of the server. Refer to the model-specific *Cisco UCS C2xx Installation and Service Guide* for jumper location and procedure.

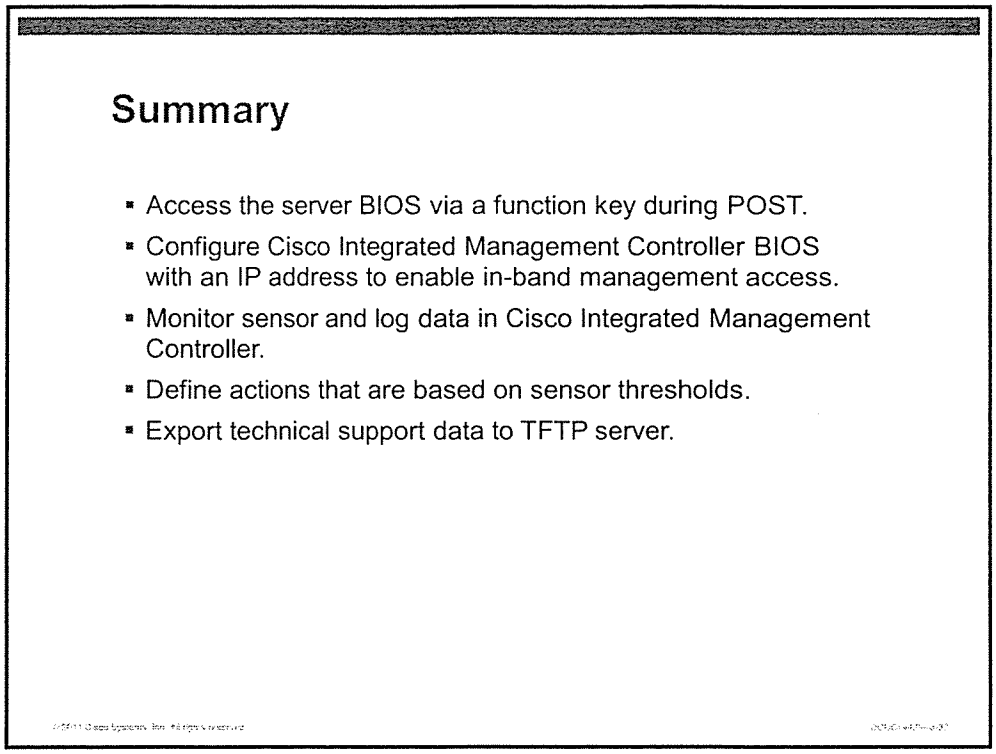
The BIOS password protects against unauthorized changes to BIOS settings. If the password is lost, it can be recovered by moving a jumper and power clearing the system, identical to the procedure for clearing the Cisco Integrated Management Controller admin password.

In certain instances, a setting that is made in BIOS setup is incompatible with the server hardware and system instability or lockup can occur. The BIOS CMOS can be initialized by powering off the system, unplugging the power cords, and moving a jumper.

Note It is important to move the affected jumper back to its factory position. Otherwise, the affected password or BIOS settings will be cleared at every power cycle.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 2

Provisioning Server Hardware with Cisco IMC

Overview

In this lesson, you will learn how to use the Cisco Integrated Management Controller (IMC) to prepare C-Series hardware for server operating system installation and remote management.

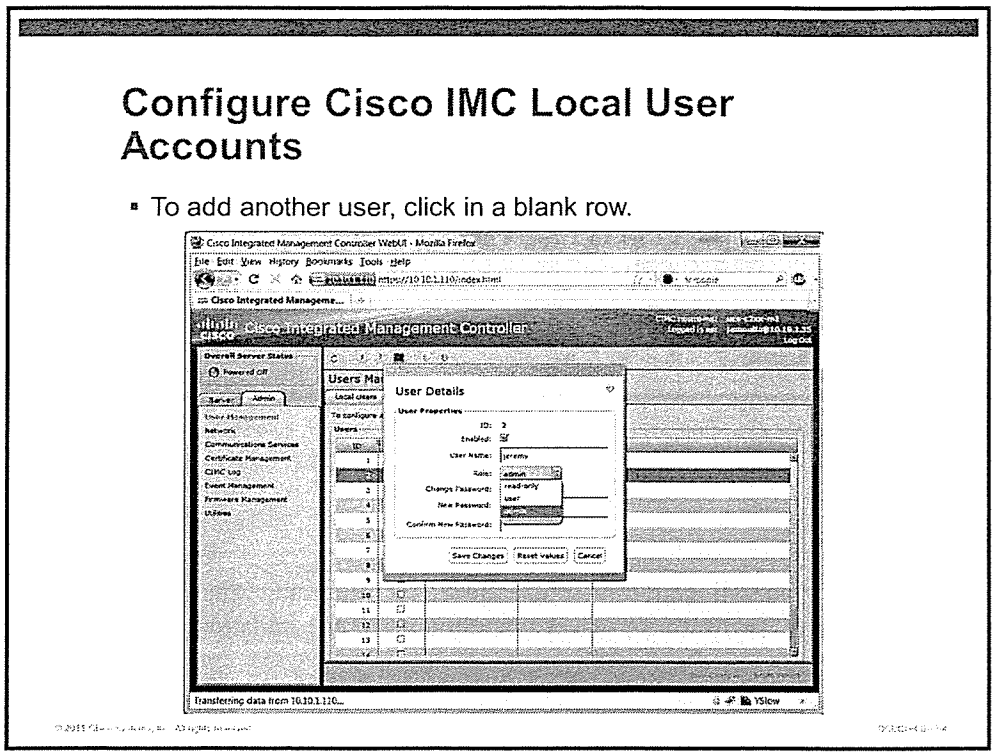
Objectives

Upon completing this lesson, you will be able to configure Cisco Integrated Management Controller to prepare for the installation of an operating system or hypervisor. This ability includes being able to meet these objectives:

- Configure local user accounts to restrict access to Cisco Integrated Management Controller
- Launch and use the KVM console
- Configure virtual media to install operating system software
- Locate and download operating system-specific utilities and drivers on Cisco.com
- Configure IPMI
- Configure SoL

Configure Cisco IMC Local User Accounts

Access to Cisco Integrated Management Controller is controlled by a local username and password database. In this topic, you will learn how to create users, set authorization permissions, change passwords, and disable local users for security reasons.

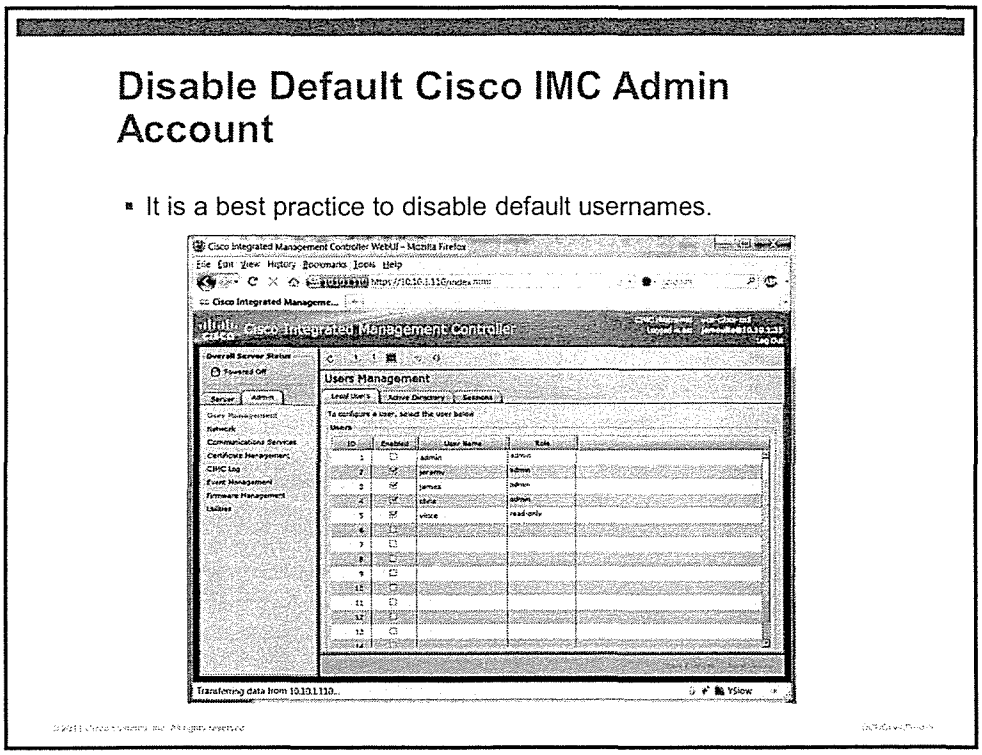


As soon as you configure the Cisco Integrated Management Controller BIOS with IP address information, you can access Cisco Integrated Management Controller with the default user "admin" and the default password "password." You can add 14 additional users for a total of 15 local users.

To add a new user, click in a blank user row and a dialog will prompt you for enabled state, username, role, and password. Roles are mapped to users to assign the appropriate level of access.

Role	Privileges
Read-Only	Read-only access to all areas of the Cisco Integrated Management Controller user interface, which is an appropriate role for an IT auditor.
User	View all information. Manage the power control options such as Power On, Power Cycle, and Power Off. Launch the keyboard, video, mouse (KVM) console and virtual media. Clear all logs. Toggle the locator LED.
Admin	Users with the admin role can perform all actions available through the GUI, command-line interface (CLI), and Intelligent Platform Management Interface (IPMI).

Disable Default Cisco IMC Admin Account

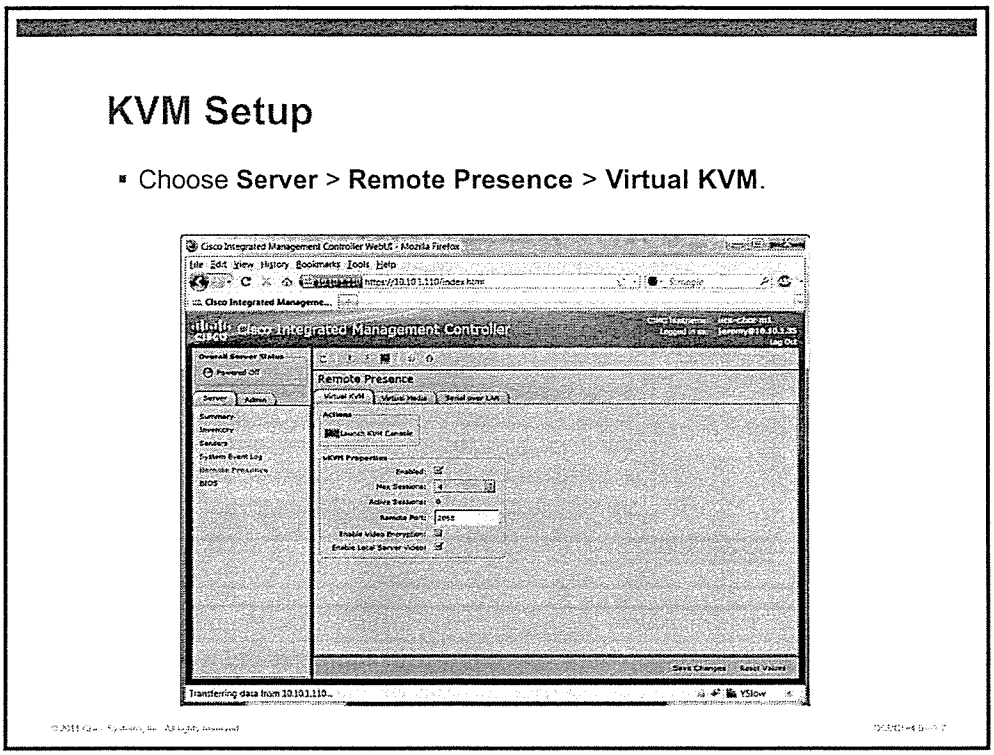


Because default usernames and passwords are documented and well-known, it is considered best practice to rename, delete, or disable built-in user accounts. Cisco Integrated Management Controller does not allow for the admin account to be deleted or renamed, but it can be disabled. Although the admin password can be changed, knowledge of the username itself makes the interface more vulnerable to dictionary or brute-force attacks.

Click the admin user and uncheck the **Enabled** box and click **Save Changes** in the dialog box. There must be at least one user that is enabled with admin role.

Launch and Use the KVM Console

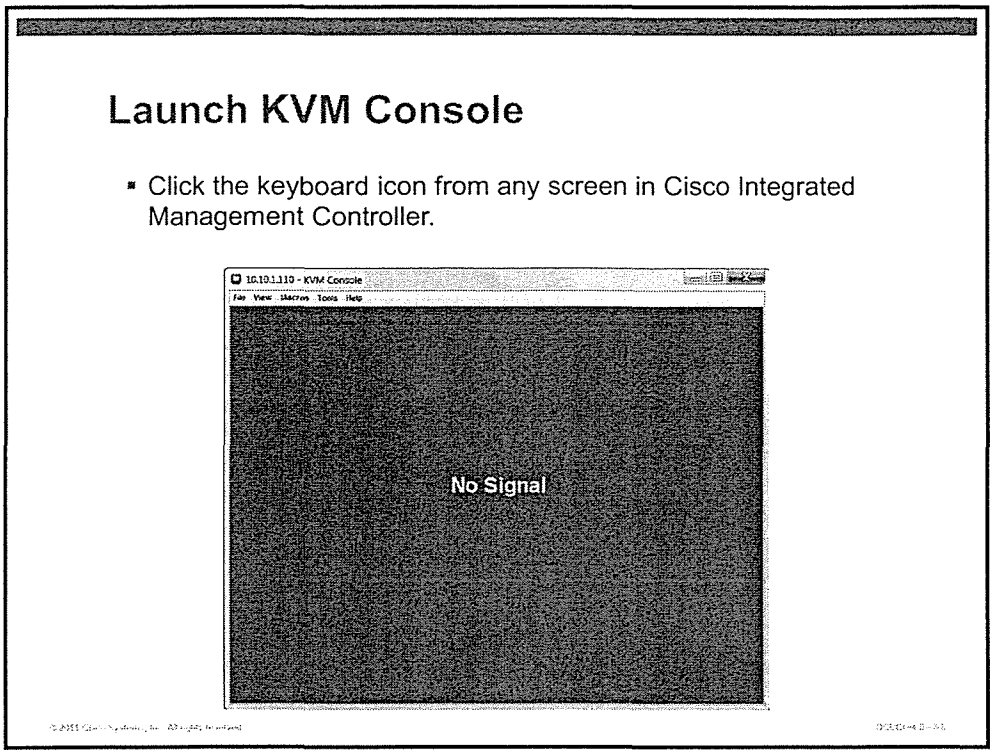
This topic discusses how to configure the keyboard, video, mouse (KVM) console to facilitate remote access to the physical server console. The KVM console can be accessed from every screen in Cisco Integrated Management Controller.



Although protocols such as Secure Shell (SSH), X-Windows, and Microsoft Remote Desktop allow access to the operating system CLI or desktop, they cease to function if the server is rebooted. Certain operations, such as changing BIOS settings, can only be performed if you are at the server console. The KVM console allows remote access to the physical console of the C-Series server, even if the operating system or hypervisor is not running.

Name	Description
Enabled check box	Globally enable or disable KVM console.
Max Sessions field	Maximum concurrent KVM connections. A number between 1 and 4.
Active Sessions field	This indicates the number of current KVM sessions.
Remote Port field	The TCP port over which the KVM session communicates.
Enable Video Encryption check box	If checked, all video transmissions will be encrypted.
Enable Local Server Video check box	If checked, video will also be displayed on any monitor that is connected to the server from the rear panel or front panel dongle.

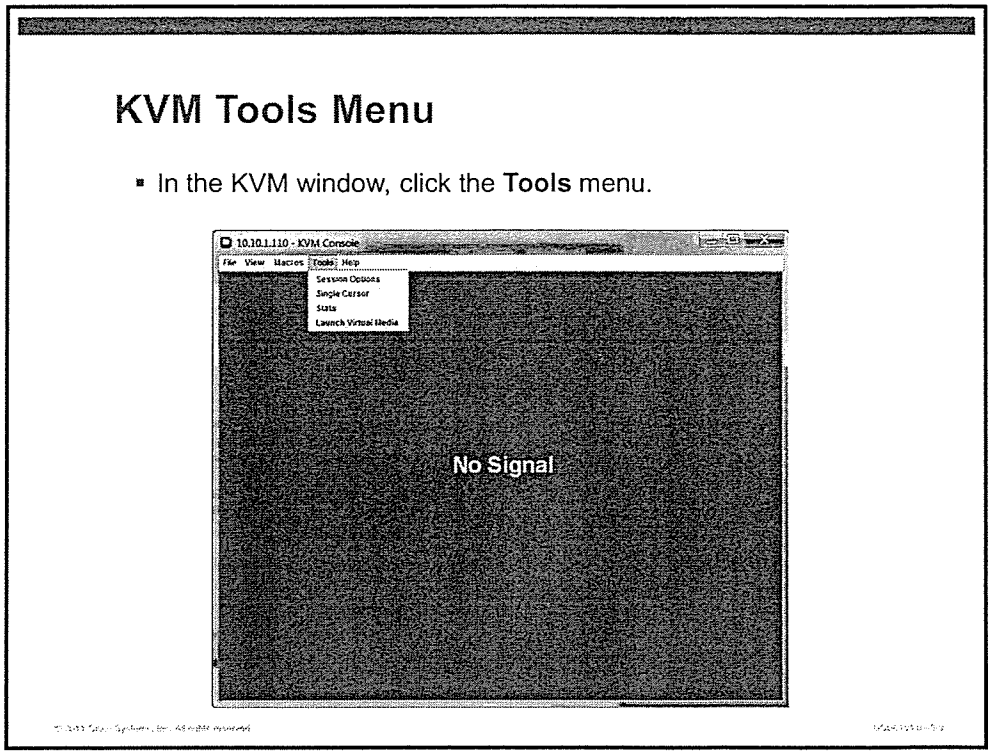
Launch KVM Console



The KVM console can be launched from any window in Cisco Integrated Management Controller by clicking the small keyboard icon at the top of each content pane. If the server is powered down, the console will have a green background with the words "No Signal" in yellow text.

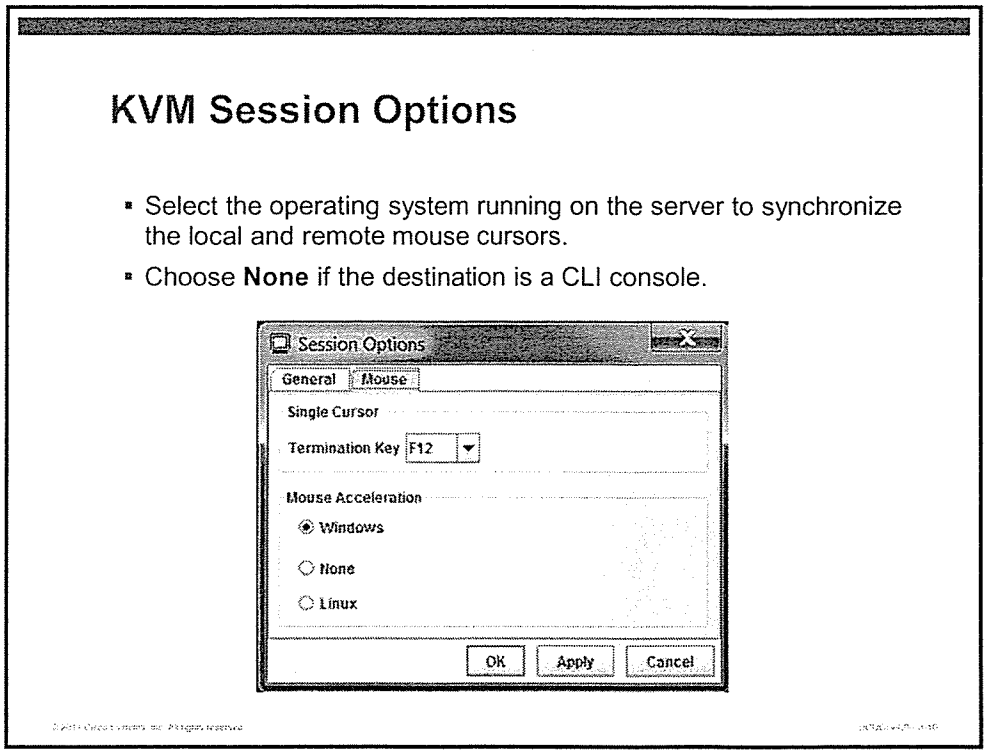
After you apply power to the server, you can observe the boot process and operations as if you were physically connected to the console.

KVM Tools Menu



The KVM Tools menu provides access to Session Options, Single Cursor mode, network statistics, and the Virtual Media launcher. If mouse tracking lags, single cursor mode locks together the local and remote mouse cursors. While in single cursor mode, you cannot move the mouse cursor outside the KVM console borders. To exit single cursor mode, press **F12**.

KVM Session Options

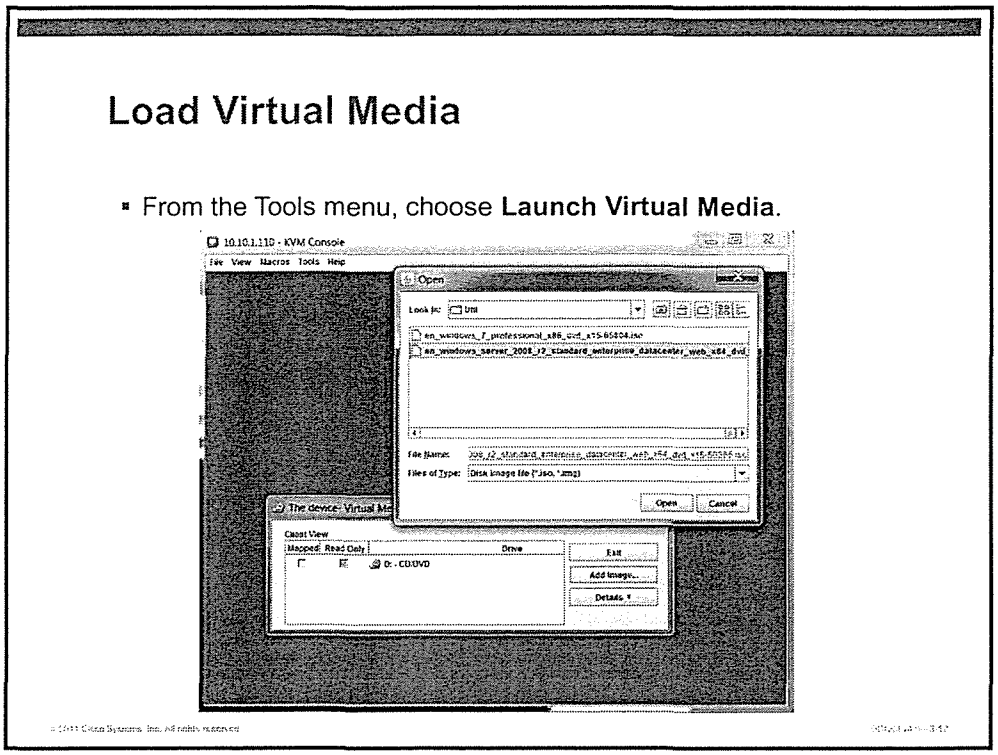


The Session Options dialog allows you to configure the mouse acceleration mode for the local and remote cursors. If you are running Linux and mouse acceleration is set to Windows (or vice versa), there will be noticeable space on the screen between the local and remote cursors. The local cursor is usually white and the remote is always black.

If the F12 key is needed for another function, you can assign another function key to exit single cursor mode.

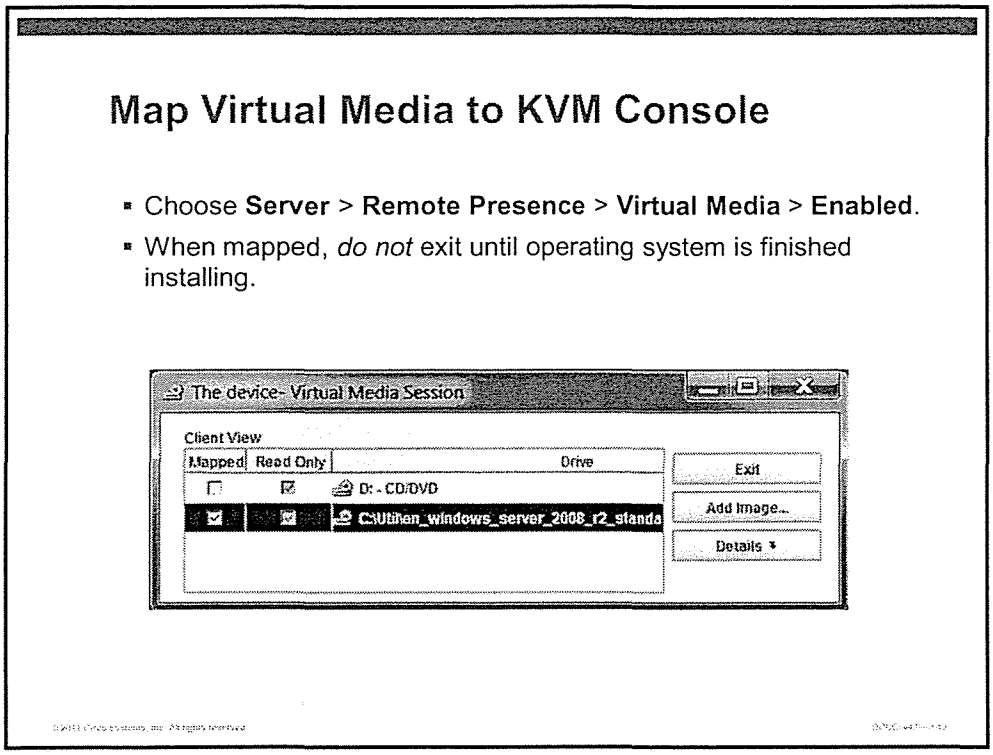
Configure Virtual Media

This topic shows how to configure virtual media to allow remote installation of operating systems, device drivers, utilities, and applications.



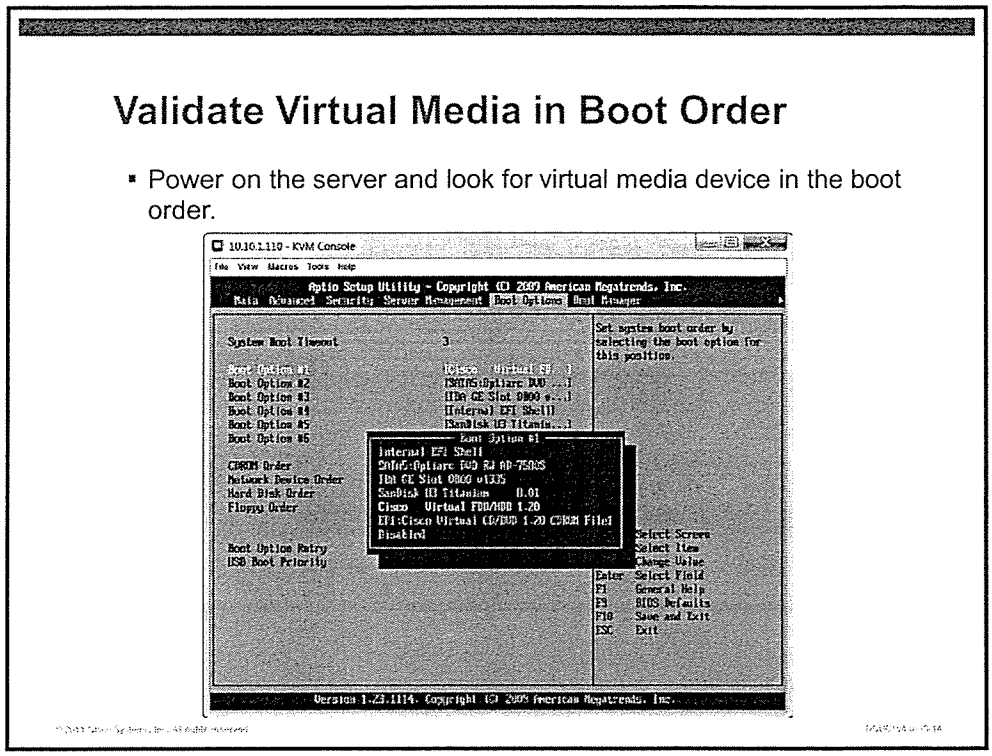
From the Tools menu on the KVM console, select **Launch Virtual Media**. You can select from physical drives that are connected to the machine where the KVM console was launched, such as CD/DVD drive, floppy drive, or USB key.

Map Virtual Media to KVM Console



You can also mount a virtual media drive based on an ISO or IMG image. IMG is to floppy disks as ISO images are to CD/DVD discs. After you have selected physical or virtual media, click the check box under the Mapped column. It is very important *not* to click **Exit** until you have successfully finished loading the operating system on the server. After **Exit** is pressed, all device mappings are cleared. If this occurs during operating system install, the process will stop.

Validate Virtual Media in Boot Order

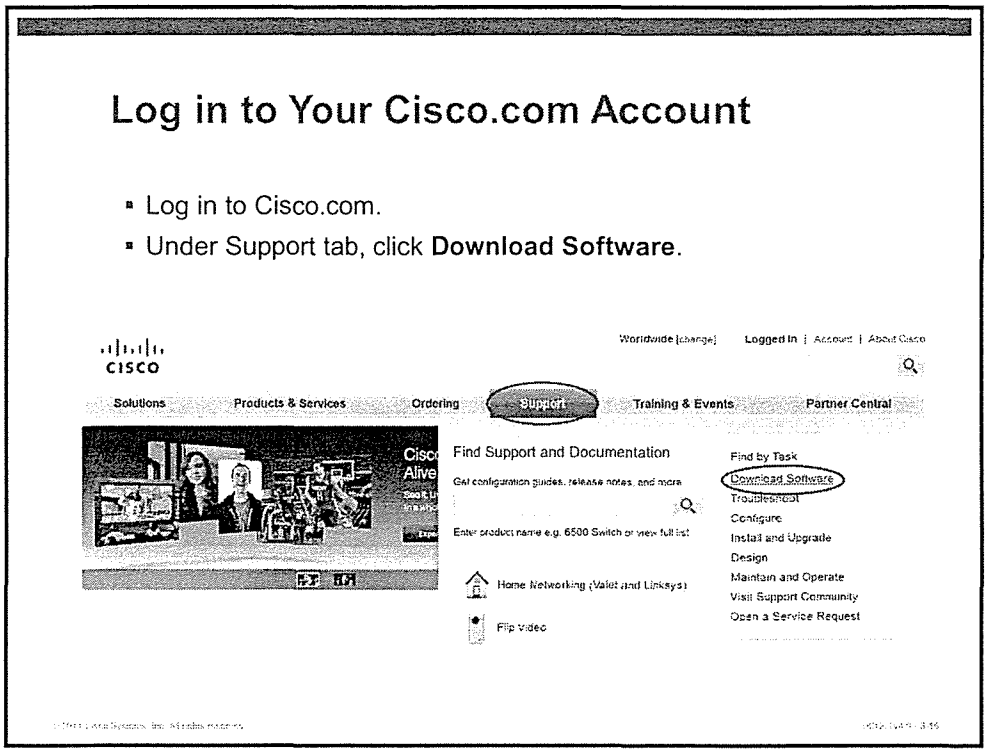


There are two ways to validate that the mapped virtual media is recognized by the server. You can either enter the BIOS setup and look for Cisco Virtual FDD/HDD in the BIOS Boot Options, or press **F6** during power-on self-test (POST) to select the virtual media as the boot device.

When the virtual media is unmapped, it will no longer appear in the boot order.

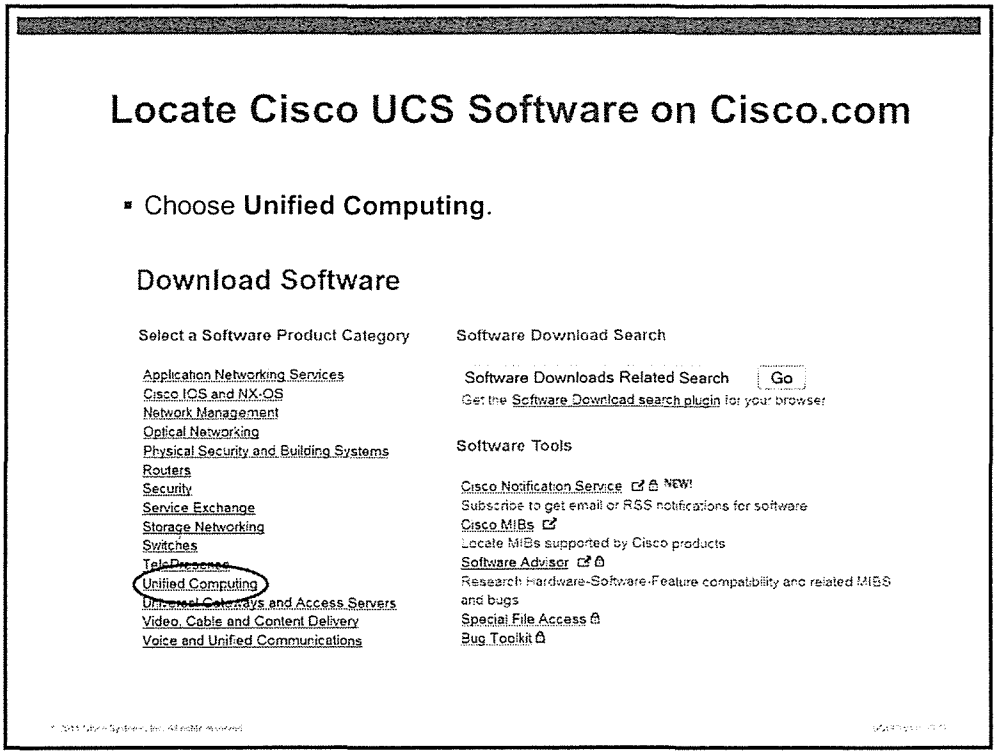
Locate and Download Operating System-Specific Drivers and Utilities from Cisco.com

Although drivers and utilities are included on a CD at the factory, updated software must be downloaded from Cisco.com. This topic discusses how to locate and download operating system-specific drivers and utilities from Cisco.com.



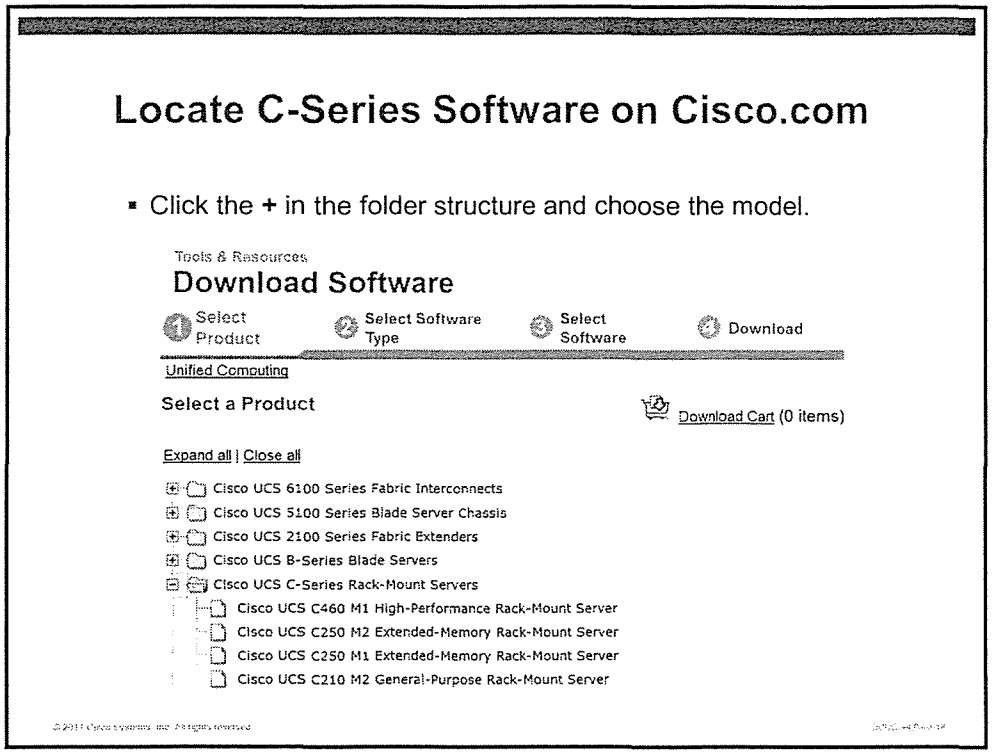
To access Cisco Unified Computing System (UCS) C-Series drivers and utilities, log in to your Cisco.com account, hover your mouse over the Support link, and select **Download Software**.

Locate Cisco UCS Software on Cisco.com



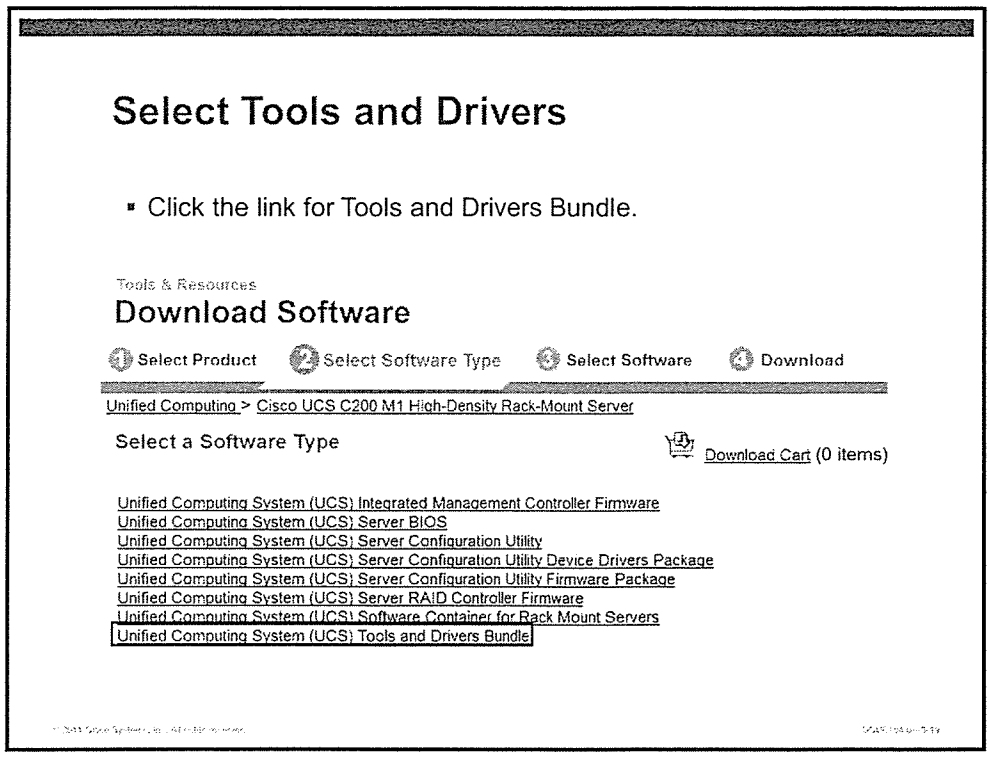
Locate and click the link to **Unified Computing.**

Locate C-Series Software on Cisco.com



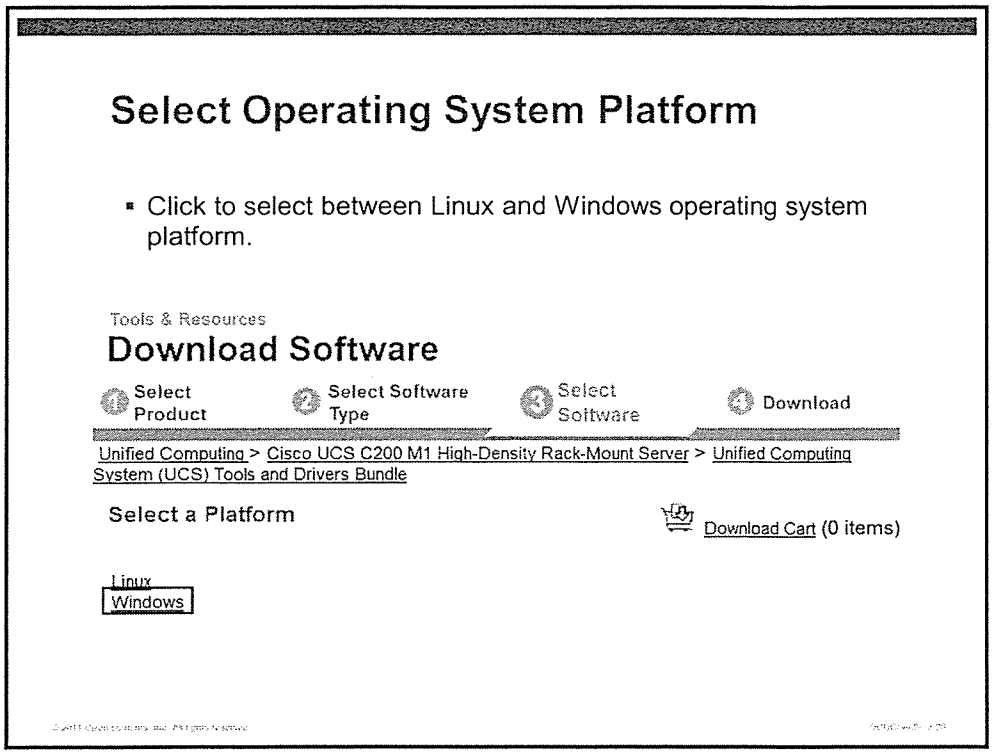
Click the + sign in the Unified Computing dialog and select the model for which you want to download device drivers and utility software.

Select Tools and Drivers



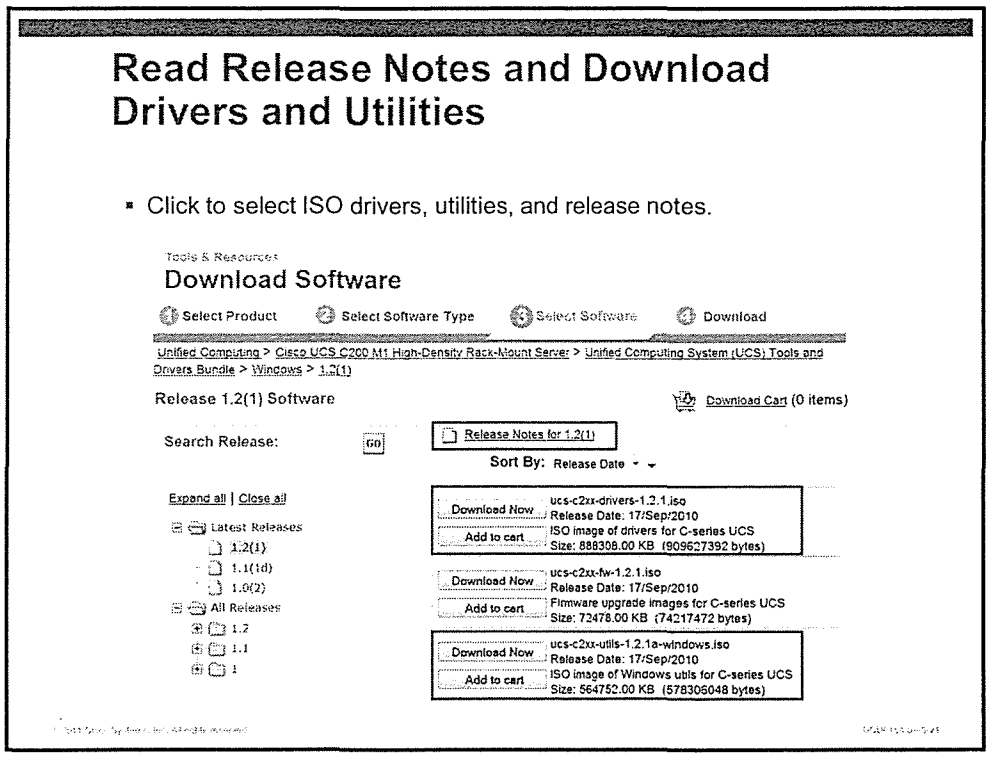
Click the link for **Unified Computing System (UCS) Tools and Drivers Bundle.**

Select Operating System Platform



Select the operating system for which you require drivers and utility software.

Read Release Notes and Download Drivers and Utilities

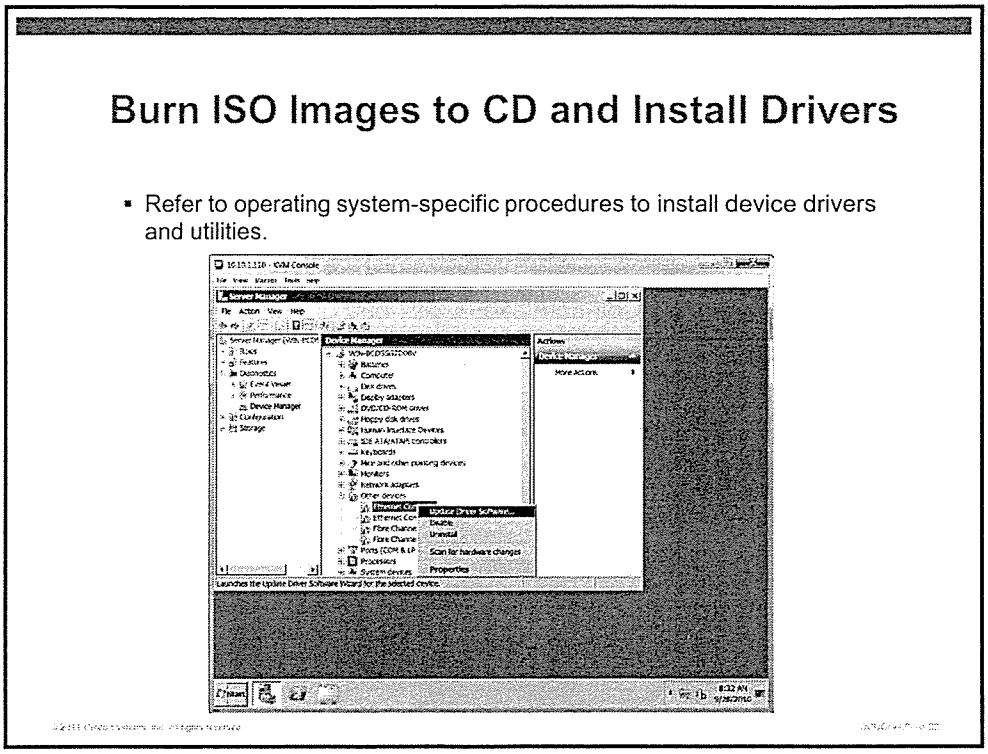


Before installing utility software or device drivers, it is important to read the release notes. There may be firmware dependencies that need to be met for proper operation with the new drivers. The release notes also contain a list of open caveats. If there is an unresolved hardware or software issue that would negatively impact your production solution, the new software should not be installed.

There are two ISO packages that you will need to download:

- The first is a model-specific and operating system-specific package of device drivers. This includes updates for the Intel motherboard chipset, Ethernet Fibre Channel, and video drivers. The operating system or hypervisor will run in a degraded state until necessary device drivers are installed.
- The second package includes operating system-specific utilities for managing Ethernet network cards and Fibre Channel host bus adapters (HBAs).

Burn ISO Images to CD and Install Drivers



The device drivers and utility software packages are in the form of ISO CD-ROM images and must be burned to a disc before use. Free burning software for Windows and Linux is widely available.

Windows: ImgBurn http://www.imgburn.com

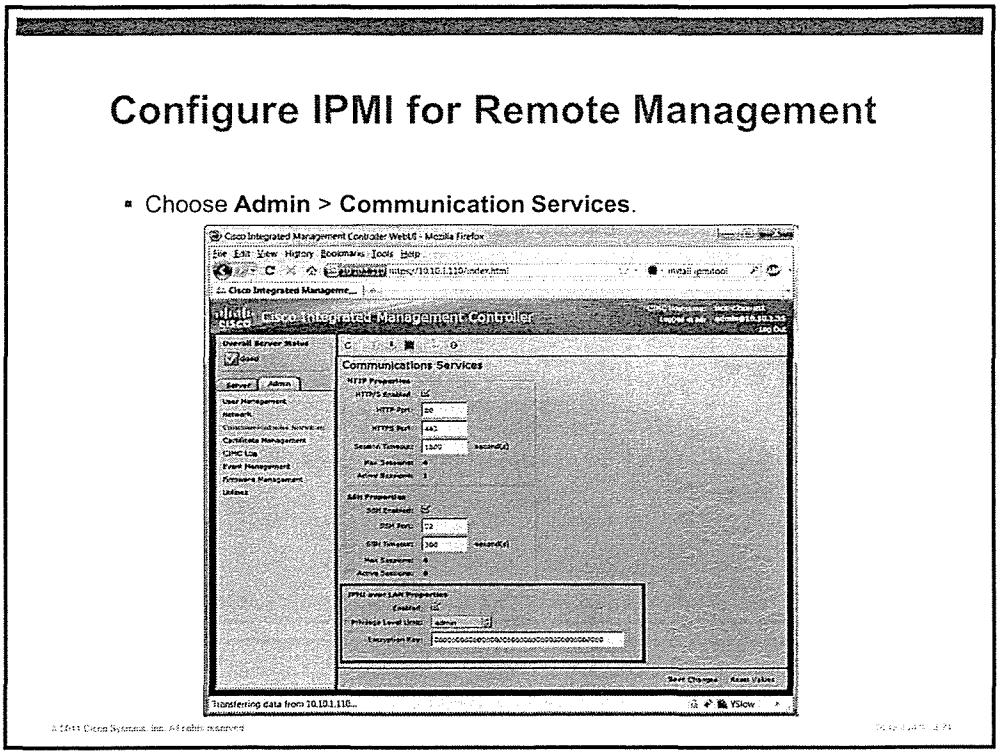
Linux: X-CD-Roast http://www.xcdroast.org

After the drivers and utilities are successfully burned to disc, insert the disc in the DVD/CD-ROM drive of the server. Follow the operating system procedures to install device drivers and utility software.

Alternatively, you can map virtual media to the ISO files and they can be mounted by the operating system as a regular DVD/CD-ROM drive. This method works best when the machine hosting the ISO images is on a LAN with the C-Series server. Although virtual media will operate over a WAN link, installation may be very slow.

Configure IPMI for Remote Management

This topic describes configuring Intelligent Platform Management Interface (IPMI) for remote management.

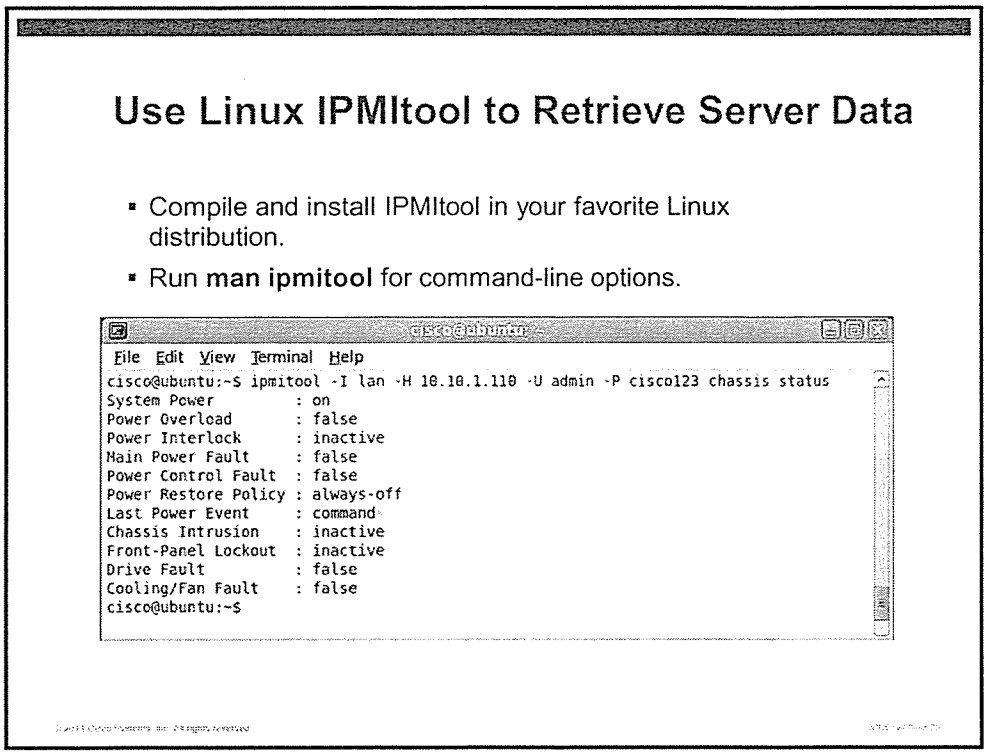


IPMI is a remote management and monitoring protocol that was developed by Intel and a multivendor consortium (http://www.intel.com/design/servers/ipmi/spec.htm).

IPMI controls are accessed via the Communications Services item in the Admin tab. IPMI is enabled by default as an administrator privilege. Any user with the admin role can remotely access IPMI data with their Cisco Integrated Management Controller credentials. Because the default encryption setting allows usernames and passwords to be passed in cleartext, it is critical that an encryption string is configured and matched in any IPMI monitoring tool.

Name	Description
Enabled check box	Globally enable or disable IPMI.
Privilege Level Limit field	Select between Read-Only, User, or Admin.
Encryption Key field	This hex field is used to specify a manual encryption key for IPMI data. The default is no encryption.

Use Linux IPMItool to Retrieve Server Data



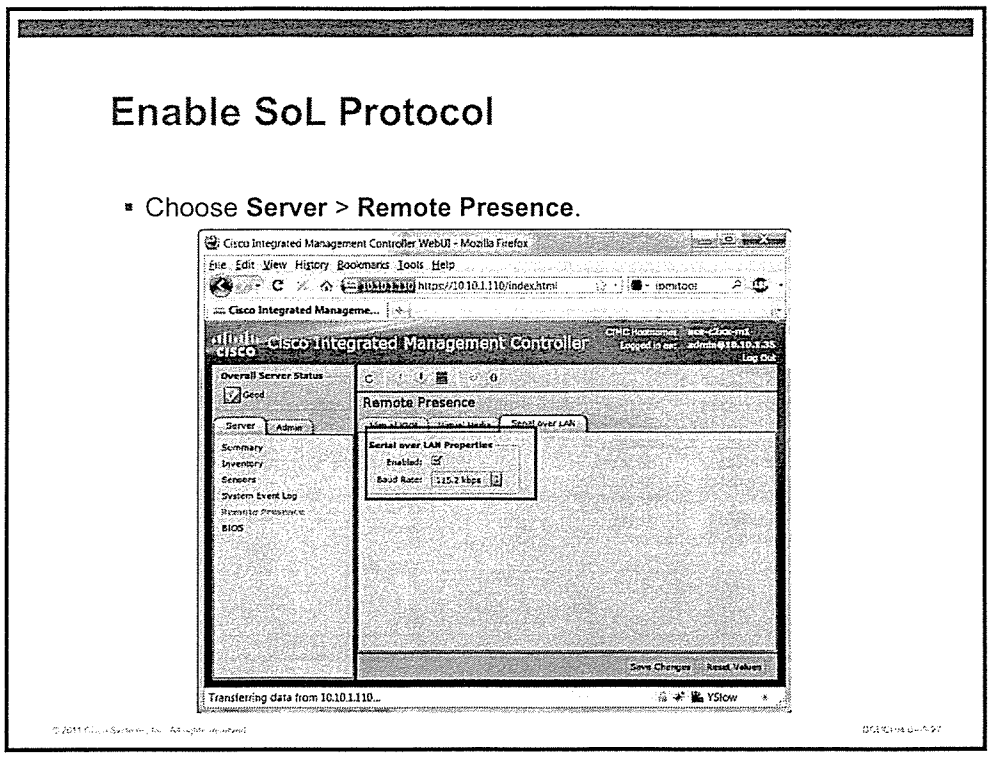
Although the Cisco Integrated Management Controller GUI and CLI offer the same information available via IPMI, you may want to create scripted queries to servers with specifically formatted output. To achieve this flexibility, you can use the Linux-only IPMItool.

Refer to the IPMItool manpage for complete command syntax.

The IPMItool home page on Sourceforge houses the latest builds and source code (http://ipmitool.sourceforge.net).

Configure SoL Protocol

This topic discusses how to configure Serial over LAN (SoL) Protocol.

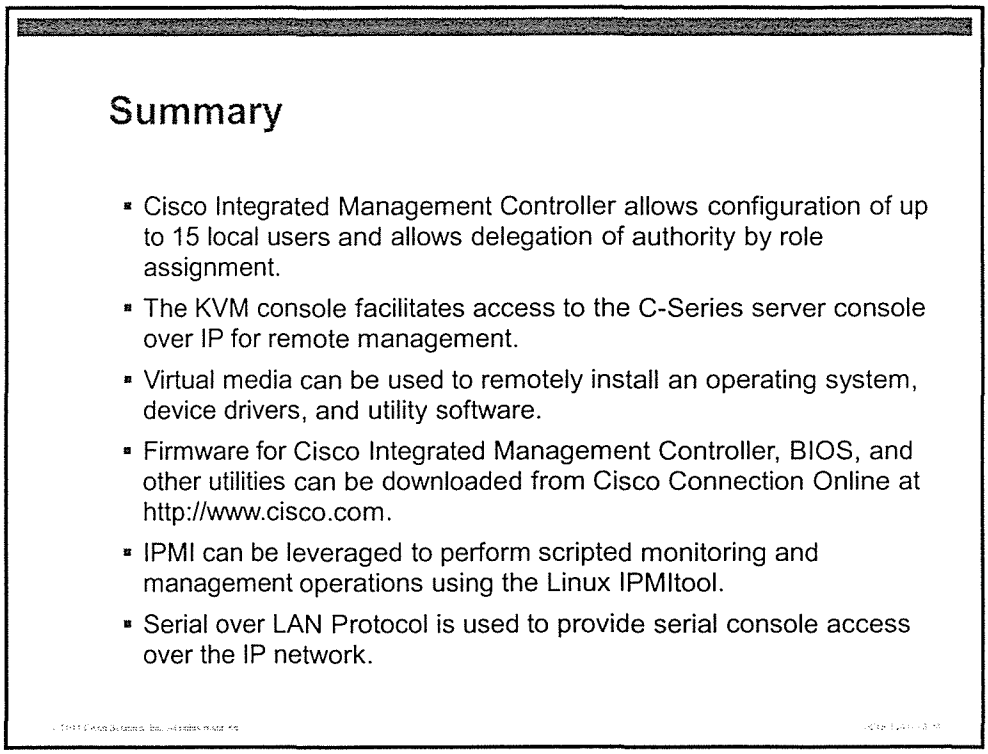


Serial over LAN (SoL) can be used to connect to the physical serial console of server operating systems that allow console access. SoL operates over User Datagram Protocol (UDP) port 623.

Note	SoL also requires enabling Console Redirection in the server BIOS. When Console Redirection is enabled, POST messages are only forwarded to the SoL console. The choice to enable SoL should be considered carefully.

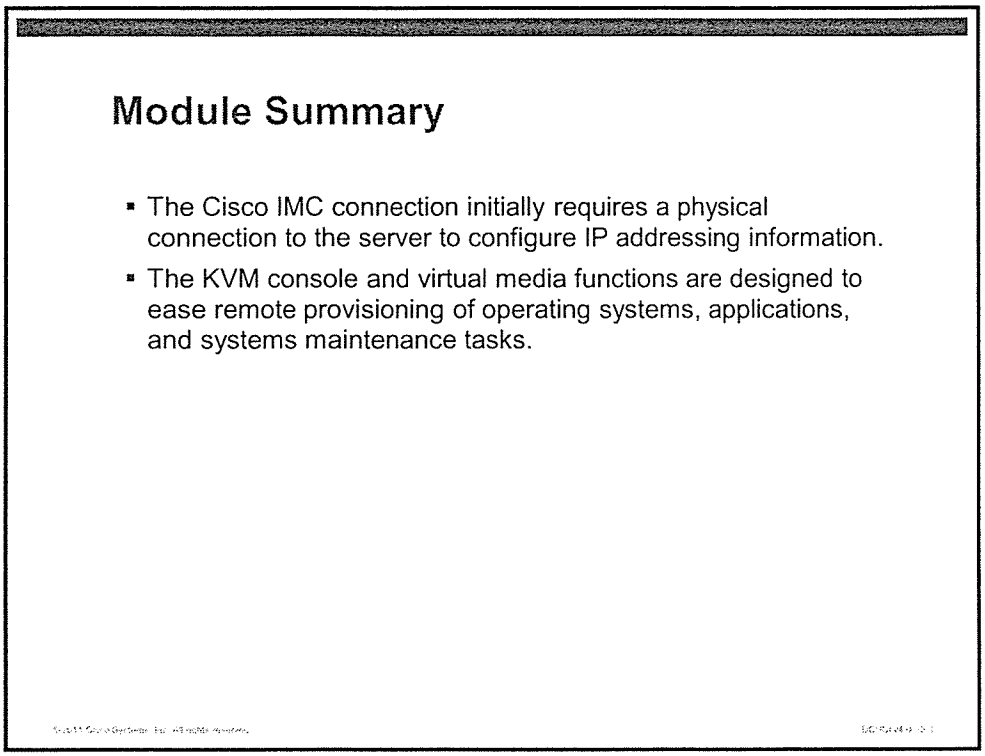
Summary

This topic summarizes the key points that were discussed in this lesson.



Module Summary

This topic summarizes the key points that were discussed in this module.



The Cisco Integrated Management interface is designed to allow seamless provisioning of server hardware and allow for Remote Monitoring and maintenance. The keyboard, video, mouse (KVM) console and virtual media are used to support remote access software provisioning of operating systems, device drivers, and applications.

To facilitate lights-out management, maintenance, Remote Monitoring, and server hardware provisioning, Cisco created Cisco Integrated Management Controller as a central console that can be accessed via web browser or Secure Shell (SSH) command-line interface (CLI).

Unlike the server BIOS, which is only accessible at the time of power-on self-test (POST), Cisco Integrated Management Controller runs on a dedicated "server within the server," with its own CPU, RAM, and flash memory complex. Because it is not tied to the operating system running on the C-Series host, it operates autonomously. However, Cisco Integrated Management Controller can control what server hardware resources are available to the host operating system.

This module illustrates the use of the Cisco Integrated Management Controller to provision Cisco Unified Computing System C-Series rack servers for Remote Monitoring, management, and initial operating system load.

References

For additional information, refer to these resources:

- Cisco, Inc. *Managing Local User Accounts* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.1.2/Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_2_chapter7.html

- Cisco, Inc. *Managing Remote Presence* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.1.2/Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_2_chapter6.html#concept_AC4EC4E9FA3F4536A26BAD49734F23D0
- Cisco, Inc. *Configuring Virtual Media* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.1.2/Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_2_chapter6.html#task_99CD607A55D6405BBCD4BB72AC93B5E2

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) Which two choices are valid for performing initial management configuration of a Cisco C-Series server? (Choose two.) (Source: "Configuring Cisco IGC")

A) Cisco Integrated Management Controller KVM console
B) virtual media
C) rear panel dongle
D) PS/2 keyboard and monitor
E) front panel dongle
F) USB keyboard and monitor

Q2) Which function key is used to access the Cisco Integrated Management Controller configuration BIOS at POST? (Source: "Configuring Cisco IMC")

A) F1
B) F2
C) F5
D) F6
E) F8
F) F12

Q3) Which three choices are valid Cisco Integrated Management Controller Sensor tabs? (Choose three.) (Source: "Configuring Cisco IMC")

A) fan sensors
B) chassis intrusion sensors
C) voltage sensors
D) chassis ground fault sensors
E) current sensors
F) air flow sensors

Q4) What is the effect of Quiet Mode? (Source: "Configuring Cisco IMC")

A) Chassis fan speed is throttled to 2500 RPM until fan sensors come online.
B) It suppresses output of BIOS POST messages.
C) Power supply fan speed is throttled to 4500 RPM until fan sensors come online.
D) It suppresses output of video signal until BIOS tests memory.

Q5) Which method is used to resolve administrative lockout? (Source: "Configuring Cisco IMC")

A) From Cisco Integrated Management Controller console, choose Admin tab > **Unlock.**
B) From BIOS, choose **Advanced Options > Unlock.**
C) Call the Cisco Technical Assistance Center.
D) Open the C-Series case and move the appropriate jumper.
E) Connect a keyboard and monitor and hold down F7 while powering on the server.

Q6) How many local user accounts can be created and renamed by the Cisco Integrated Management Controller administrator? (Source: "Provisioning Server Hardware with Cisco IMC")

A) 5

B) 14
C) 15
D) 20

Q7) Which three operating system mouse acceleration modes can be configured in the Cisco Integrated Management Controller KVM console? (Choose three.) (Source: "Provisioning Server Hardware with Cisco IMC")

A) Windows
B) VMware ESX
C) Suse
D) Red Hat
E) Linux
F) None

Q8) What is a best practice to secure the local Cisco Integrated Management Controller admin account? (Source: "Provisioning Server Hardware with Cisco IMC")

A) It is a well-known user account and should be deleted.
B) Use a strong password with mixed case, numbers, special characters, and at least nine characters.
C) The Cisco Integrated Management Controller is out-of-band, so this is not an issue.
D) Configure the local admin account to use RSA SecurID token.
E) Disable the admin account.

Q9) For which two operating systems can you download device driver and utility software from Cisco.com? (Choose two.) (Source: "Provisioning Server Hardware with Cisco IMC")

A) Red Hat
B) VMware vSphere
C) Windows
D) Suse
E) Linux
F) Ubuntu

Q10) What is the maximum number of simultaneous KVM console connections to a single Cisco UCS C-Series server? (Source: "Provisioning Server Hardware with Cisco IMC")

A) unlimited
B) 2
C) 4
D) C-200 and C-210 allow 5, C-250 allows 10, C-460 allows 20
E) C-200 and C-210 allow 4, C-250 allows 10, C-460 allows 25
F) C-200 and C-210 allow 4, C-250 allows 10, C-460 allows 50

Module Self-Check Answer Key

Q1) E, F

Q2) B

Q3) A, C, E

Q4) B

Q5) D

Q6) B

Q7) A, E, F

Q8) E

Q9) C, E

Q10) D

Module 4

Cisco UCS B-Series Hardware and Management

Overview

Before undertaking the installation of an advanced data center computing system, it is important to have a solid understanding of the hardware components and their installation requirements. This module describes installation and configuration of the Cisco Unified Computing System (UCS) B-Series rack servers.

Module Objectives

Upon completing this module, you will be able to assemble Cisco UCS B-Series components. You will have the skills to select field-installable hardware options, observe ESD precautions to safely install Cisco UCS B-Series blade server hardware, and perform initial startup configuration. You will understand how to meet licensing requirements, how component fault tolerance operates, and how to use the fault management system to troubleshoot hardware misconfigurations that may occur during initial startup.

This ability includes being able to meet these objectives:

- Managing Cisco Unified Computing System B-Series hardware
- Assembling B-Series architecture and features
- Installing Cisco UCS B-Series hardware

Lesson 1

Describing Cisco UCS B-Series Hardware Components

Overview

To promote good planning and avoid implementation delays and interruption to operation, you must understand general licensing requirements and system fault-tolerance features. Power planning, for example, is often an overlooked issue, such as when an installation is stopped because the wrong power supply cables were ordered. Implementation engineers are the second line of auditing a project plan to mitigate invalid or inaccurate configurations.

Objectives

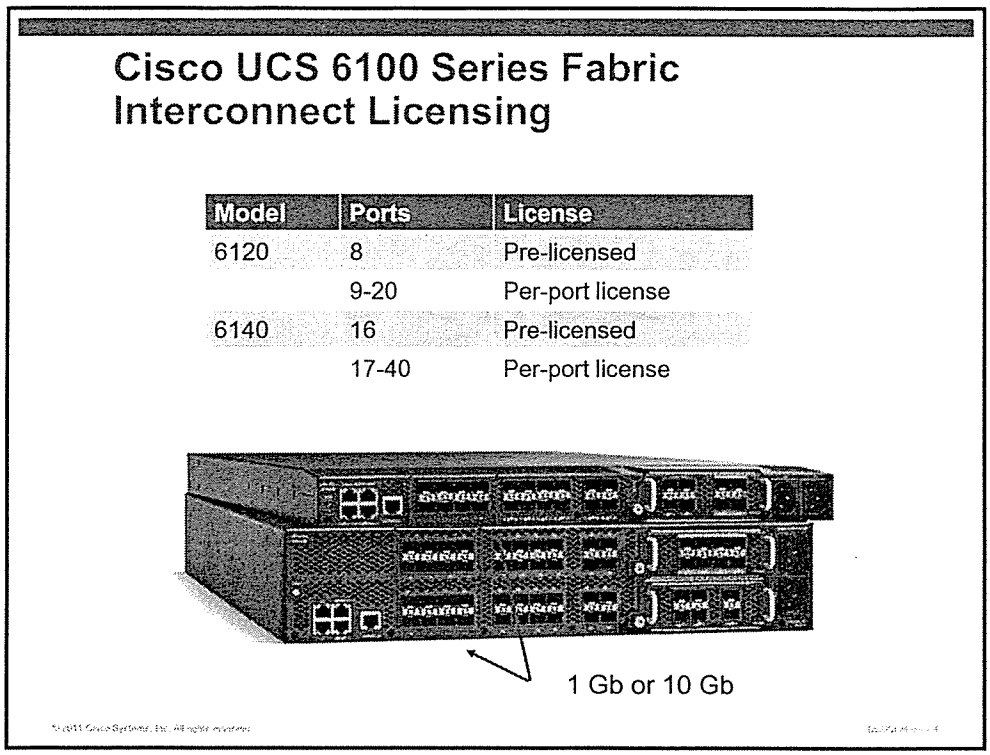
Upon completing this lesson, you will be able to define the high-level requirements of a Cisco UCS B-Series installation. This ability includes being able to meet these objectives:

- List the Cisco UCS 6100 Series Fabric Interconnect licensing requirements
- Differentiate between the three fault-tolerant configurations of the Cisco UCS B-Series power supplies
- Describe hardware redundancy components for data and management planes

Cisco UCS 6100 Series Fabric Interconnect Licensing Requirements

This topic discusses the fabric interconnect licensing requirements.

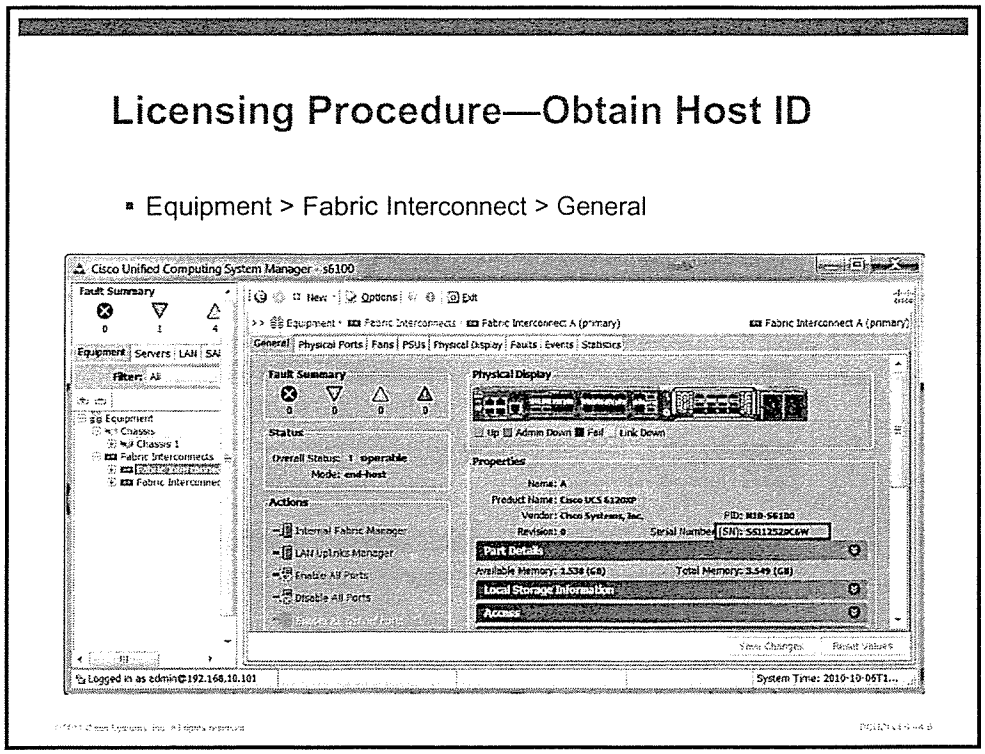
Locate B-Series Firmware on Cisco.com



The Cisco 6100 Series Fabric Interconnects require per-port licensing for fixed 10-GE ports. Eight ports on a 6120 and 16 ports on a 6140 are prelicensed. Customers can use any 8 or 16 ports before licensing is required. Ports do not need to be contiguous. Customers that require more than the number of prelicensed ports can purchase per-port activation licenses from Cisco.

Note	The purchase price of generic expansion modules (GEMs) includes all requisite licensing.

Licensing Procedure—Obtain Host ID



The first step in purchasing port licenses is to obtain the host ID that is associated with each fabric interconnect in the cluster. From the Equipment tab in Cisco UCS Manager, select the fabric interconnect. The host ID is in the serial number field. The host ID is burned into the fabric interconnect hardware and uniquely identifies that unit.

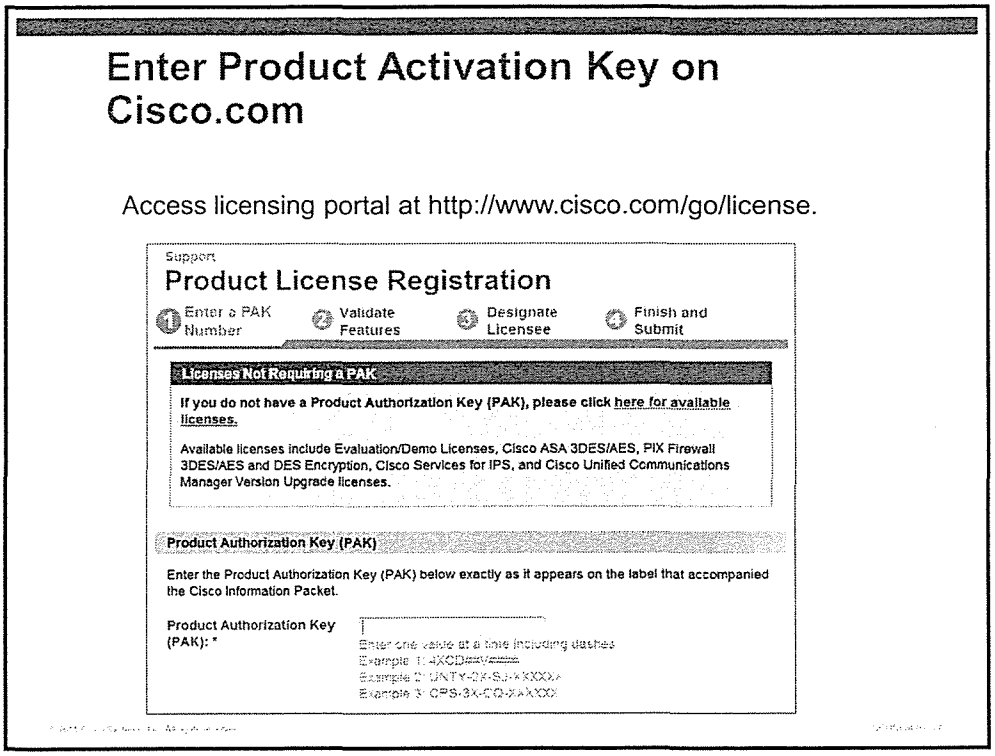
If you attempt to use an unlicensed port, a 120-day grace period counter begins. If you have not obtained a port license before expiration of the grace period, the port will become nonfunctional.

The host ID can also be obtained from a command-line interface (CLI) session to the fabric interconnect. Connect to the NX-OS shell and issue the **show license host-id** command. The host ID is burned into the fabric interconnect hardware and uniquely identifies that unit.

```
s6100-A# connect nxos
s6100-A(nxos)# show license host-id
License hostid: VDH=SSI12520C6W
```

Note	You must purchase a matching number of port licenses for each fabric interconnect in the cluster.

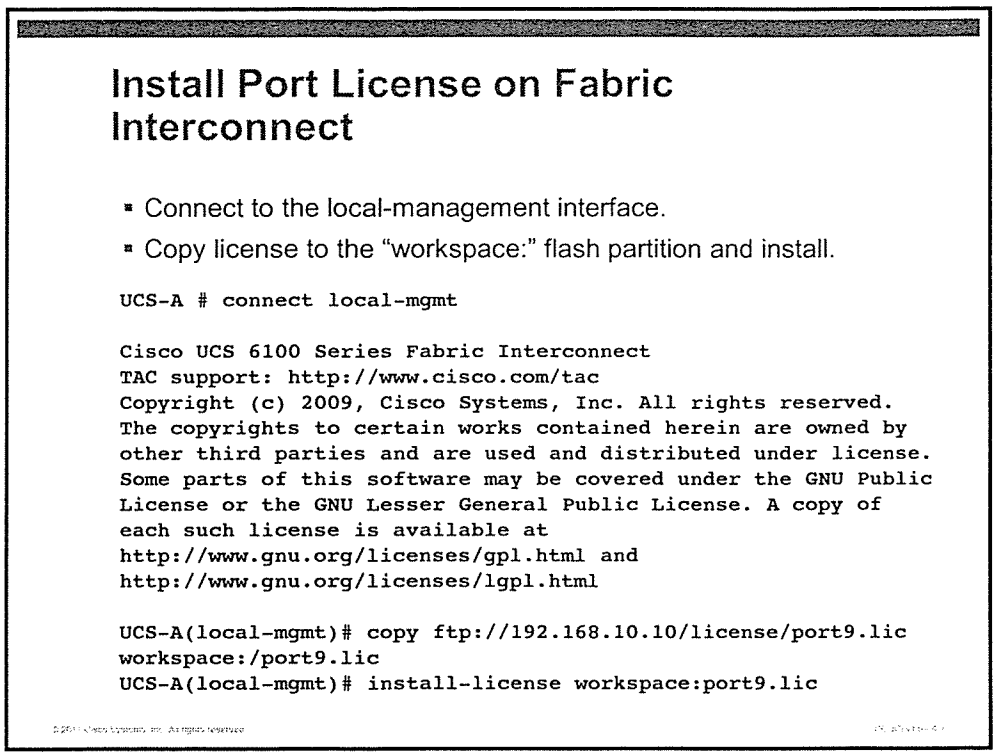
Enter Product Activation Key on Cisco.com



Purchase a license pack from Cisco for each fabric interconnect. You will receive a document with a Product Authorization Key (PAK) for each device that you are licensing. Access the licensing portal at Cisco by browsing to: http://www.cisco.com/go/license.

After the PAK is validated, a license file will be emailed to you for each PAK submitted.

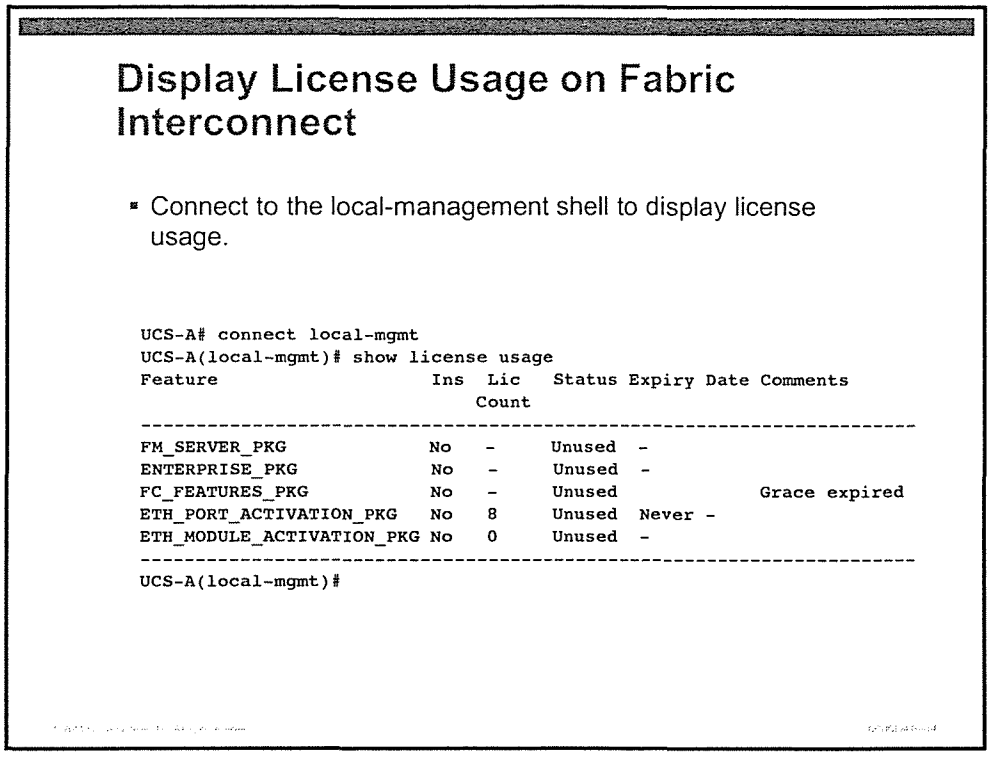
Install Port License on Fabric Interconnect



License files can only be installed from the CLI. Use Secure Shell (SSH) to enter the fabric interconnect and connect to the local-management shell. The license file must be copied to "workspace: <flash partition>." "Workspace:" is an area of persistent storage accessible to administrators. Any files that are copied into this location will remain until manually deleted.

An archive copy of any license files should be kept in a secure location. If a fabric interconnect has to be exchanged due to hardware failure, the replacement unit has a different host ID and the old license file will fail validation. To obtain a license for the replacement hardware, send an email to licensing@cisco.com. Be sure to include the host ID of the failed unit and the replacement. Requests are processed within 24 hours.

Display License Usage on Fabric Interconnect

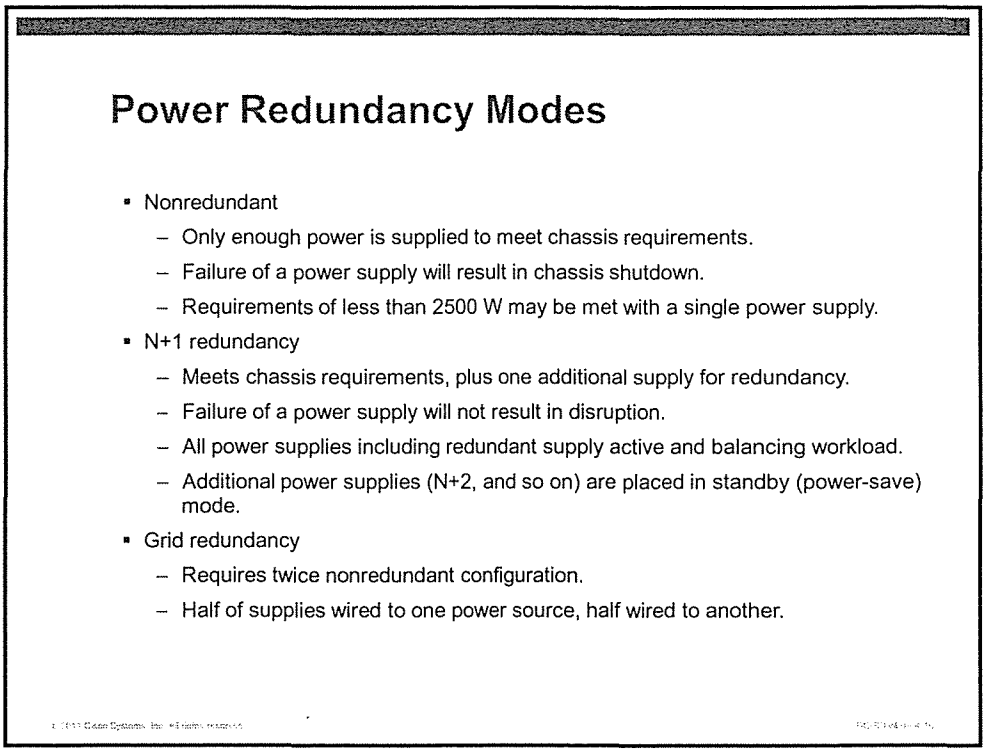


Fabric interconnect license usage can only be accessed from the Cisco UCS Manager CLI. Connect to the fabric interconnect with SSH and issue the **show license usage** command. This command can be issued by connecting to either the local-management shell or NX-OS shell.

Differentiate Between Fault-Tolerant Configurations of the Cisco UCS B-Series Power Supplies

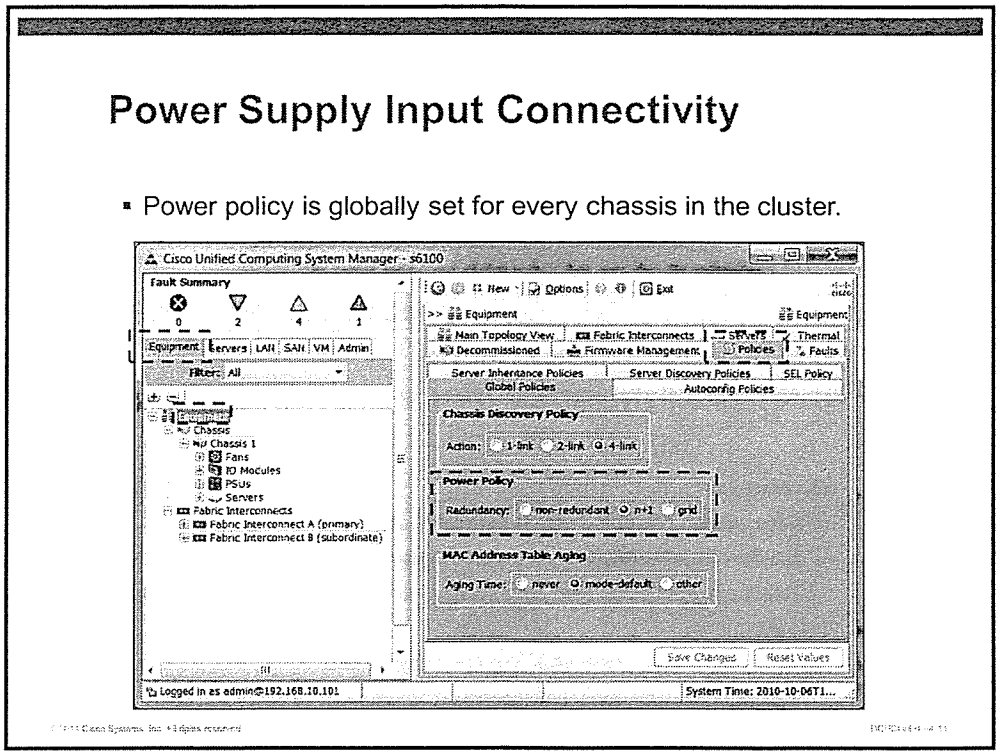
Cisco UCS B-Series server chassis support three modes of fault tolerance to suit your organization policy.

Power Redundancy Modes



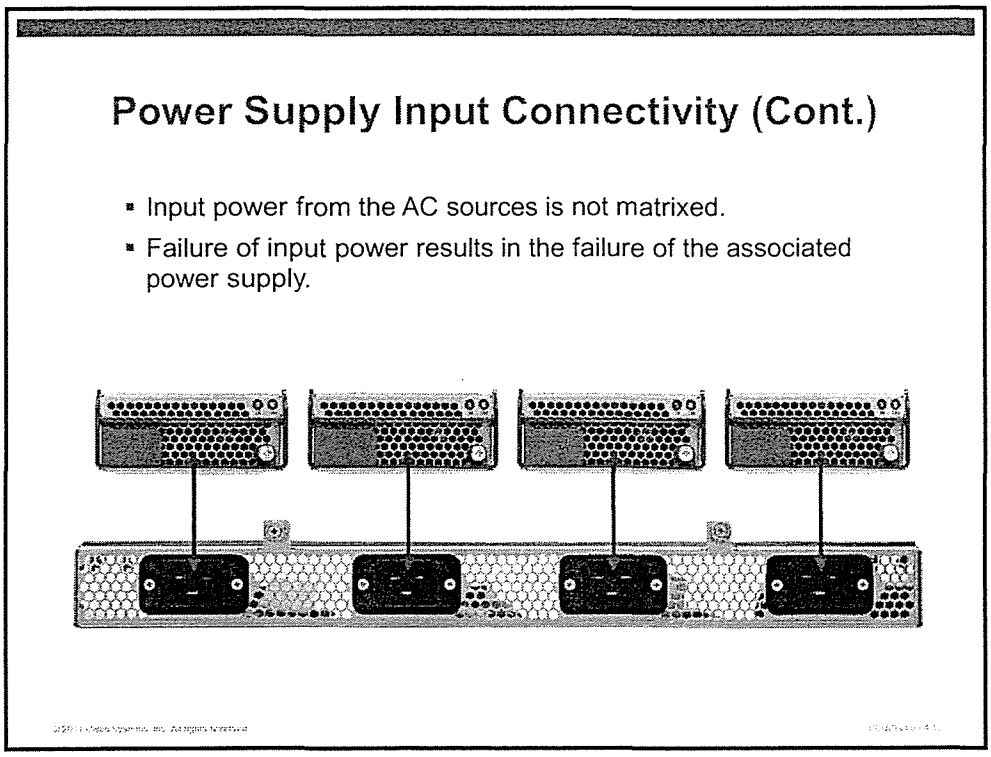
Redundancy Mode	Description
Nonredundant	All installed power supplies are turned on and the load is evenly balanced. If power supply failure results in inadequate power, the chassis will fail.
n+1	In this mode, install the number of power supplies to satisfy nonredundancy, plus at least one additional power supply for redundancy. All power supplies are turned on and equally share the power load for the chassis. If any additional power supplies are installed beyond the n+1 requirement, Cisco UCS Manager sets them to a "power-save" standby state. If the power supply state drops below the n+1 threshold, a standby power supply is activated to maintain power policy.
Grid (n+n)	Two power sources are employed. Power output is split between pairs. Power supplies 1 and 2 form one pair, and power supplies 3 and 4 are the second pair. In this mode, it is recommended that each pair is supplied from an independent power source. A typical configuration might be the use of two power utilities with separate cable routes to the data center. If a source fails (causing a power loss to one or two power supplies), the surviving power supplies on the other circuit continue to provide power to the chassis.

Configuring Chassis Power Policy



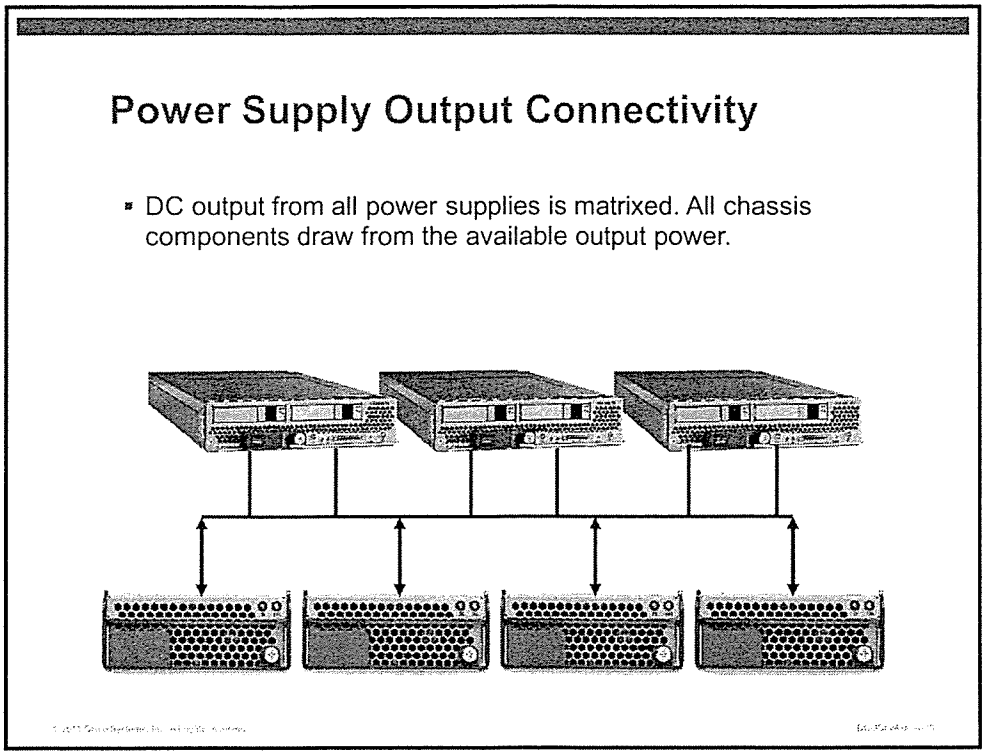
The power supply redundancy mode is a global, clusterwide setting. All Cisco UCS 5108 chassis that are connected to the fabric interconnects will inherit this policy during chassis discovery. Failure to install enough power supplies to meet the requirements of the power policy can result in an inoperable chassis.

Power Supply Input Connectivity



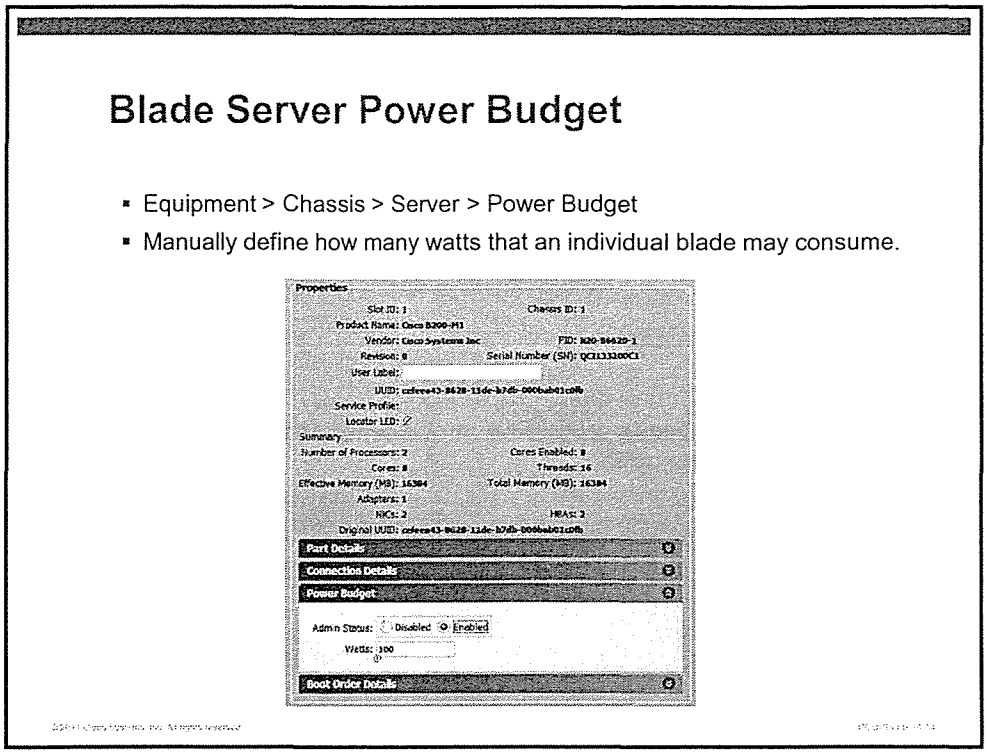
Power from each AC input is connected directly to the power supply in that chassis position. If the power cord is unplugged or loses its source, the associated power supply will power down.

Power Supply Output Connectivity



The combined DC output of all power supplies is matrixed. All components have equal access to the pool unless a power budget policy is configured on a blade server. If a power supply fails, the pool is reduced by 2500 W.

Blade Server Power Budget



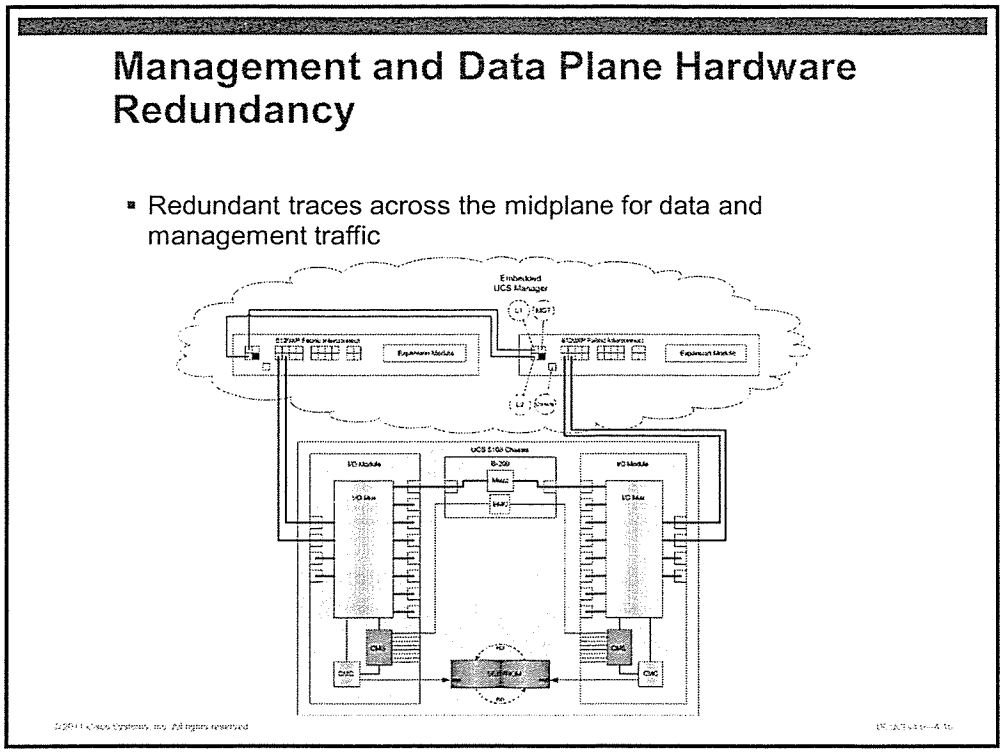
Beginning with Cisco UCS Manager version 1.2, administrators have the ability to place an upper limit on blade power consumption. If left in the default disabled state, the blade can draw the maximum that is allowed for its type.

Field	Description
Admin Status	Enabled or disabled. Disabled by default. B200 default power budget is 550 W, B250 is 1100 W.
Watts	Values must be between 100 and 1100 W.
Status	The status of the power budget being applied to the server.

Hardware Redundancy Components for Data and Management Planes

This topic describes the components of hardware redundancy components for data and management planes.

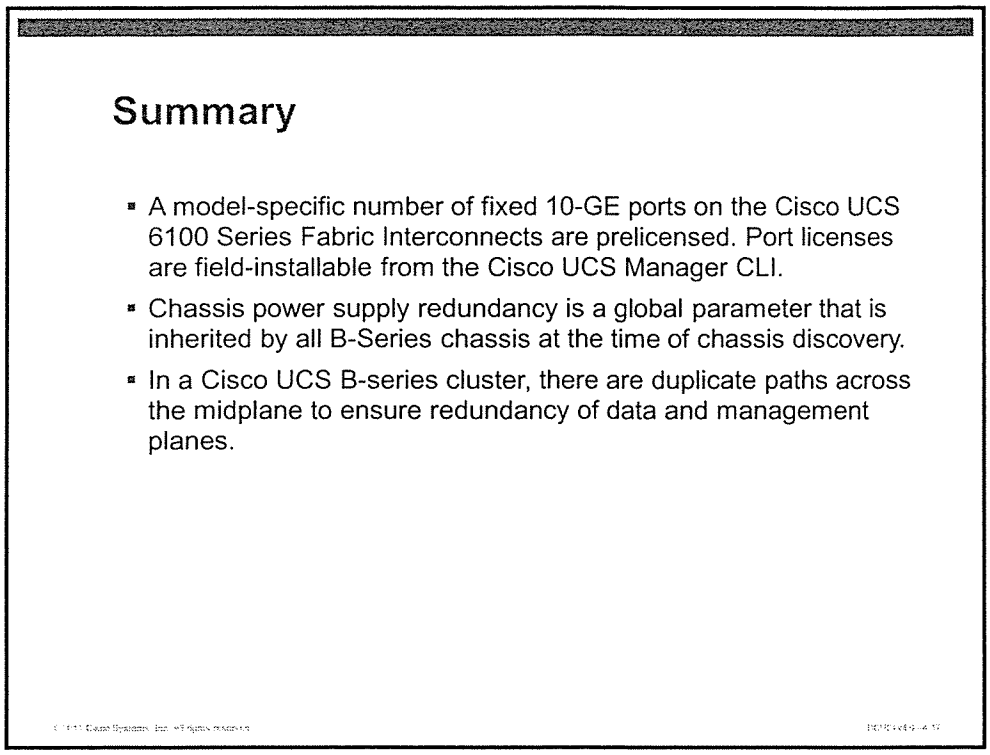
Management and Data Plane Redundancy



With redundant I/O modules (IOMs) and redundant links between IOMs and the fabric interconnects, the only single point of failure is the midplane.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 2

Assembling B-Series Architecture and Features

Overview

High availability is a critical requirement when designing a data center computing system. A thoughtful design is built with redundant components and as few single points of failure as possible.

To operate Cisco UCS in high availability mode, a management and data plane cluster is formed with two fabric interconnects, redundant 2100 Series I/O modules, and redundant links from the fabric interconnect to blade server chassis and the Layer 3 aggregation layer.

When environmental, power, component, or connectivity failures occur, Cisco UCS Manager has tools available from the GUI and command-line interface (CLI) to acknowledge, clear, and archive fault data.

Objectives

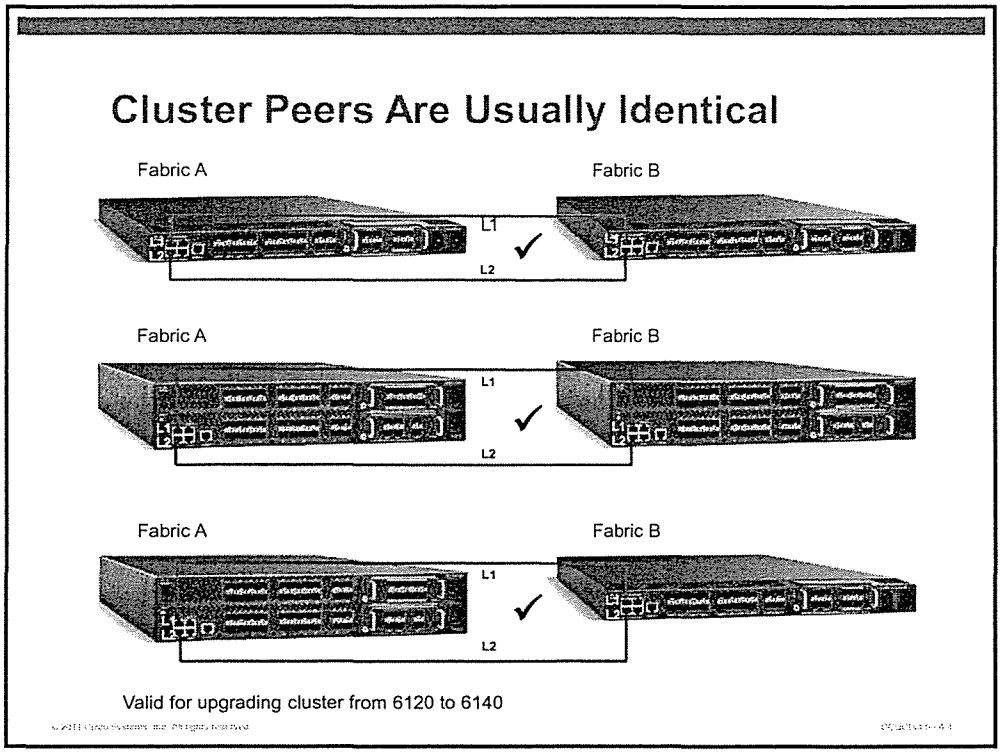
Upon completing this lesson, you will be able to define the high-level requirements of a Cisco UCS B-Series installation. This ability includes being able to meet these objectives:

- Describe high availability cluster requirements and processes of the Cisco UCS 6100 Series Fabric Interconnect
- Describe fault detection and correction using Cisco UCS Manager and the CLI

Cisco UCS 6100 Series Fabric Interconnect Cluster Requirement

This topic discusses the fabric interconnect requirements to form a high availability cluster for management and data planes.

Cluster Peers Must Be Identical

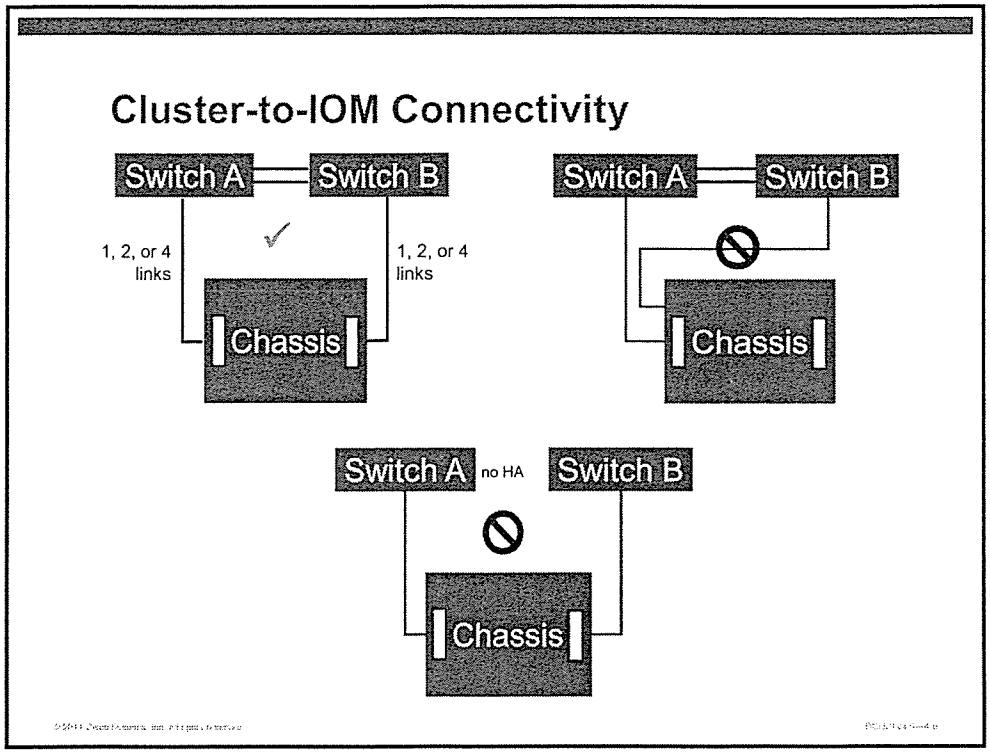


Before you configure a cluster relationship between two Cisco UCS fabric interconnects, there are two important requirements:

- Cluster peers are generally the same model. A 6120 would only peer with a 6140 to upgrade the cluster to a pair of 6140s.
- Each peer requires identical licensing. If fabric A has an installed port license for additional ports, fabric B must be licensed for the same number of ports.

For the cluster to complete negotiations, both peers need to be connected via the cluster links. One connection from port L1 to L1 and one from L2 to L2 must be made with straight-through Category 6 Ethernet cables.

Cluster-to-IOM Connectivity



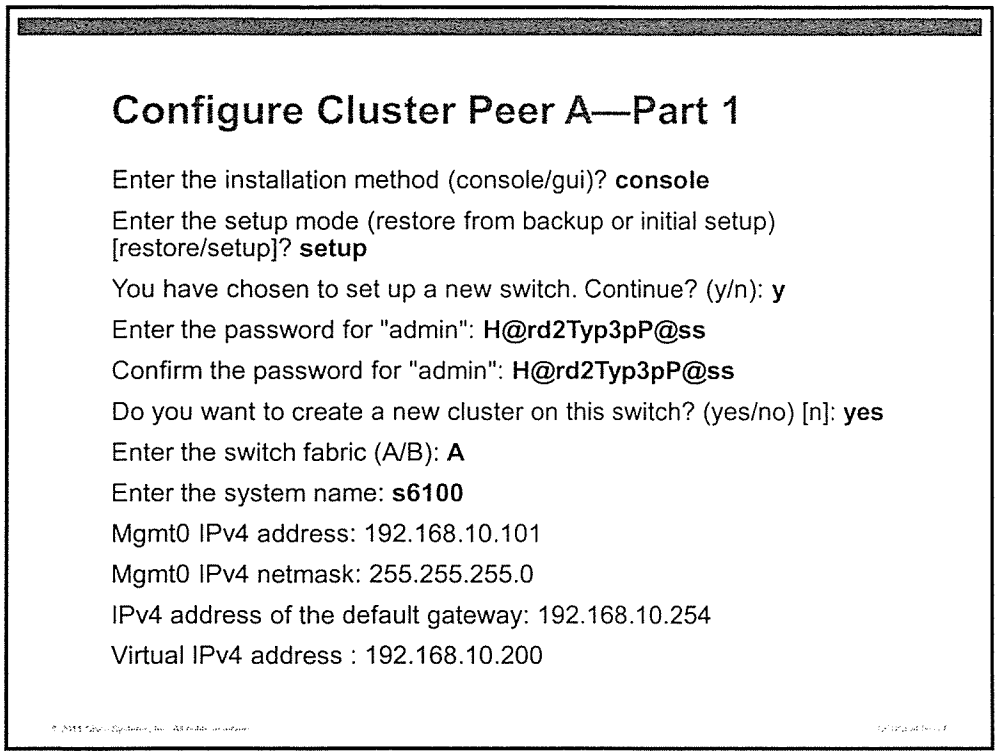
When an I/O module (IOM) of a new UCS 5108 chassis is connected to a fabric interconnect, chassis discovery begins an information exchange. IOM sends fabric ID and serial numbers for itself, and sends the process ID (PID), version identifier (VID), and serial number of the chassis. The fabric interconnect sends PID, VID, serial number, and cluster ID to the IOM. After the exchange completes without error, the cluster takes ownership of the chassis. No other cluster of fabric interconnects will accept registration of that chassis unless it is decommissioned from that cluster.

Data that is exchanged during discovery is used to validate the topology from the chassis to the cluster. In the upper-left corner of the figure, IOM A is connected to the fabric interconnect acting as fabric A. When IOM B is connected to fabric interconnect B, the PID, VID, serial number, fabric ID, and cluster ID is exchanged. Because the fabric ID matches, the fabric interconnect knows that this is not a connection attempt by IOM A to register to a second fabric (invalid topology).

In the upper-right corner of the figure, IOM A attempts to register with fabric interconnect B. When fabric interconnect B reads the fabric ID "A" from IOM A, it rejects the registration.

In the lower part of the illustration, IOM A registers with fabric interconnect A and exchanges IDs. When IOM B attempts to register with fabric interconnect B, the fabric interconnect detects an invalid cluster ID and rejects registration, because the two fabric interconnects have not formed a cluster.

Configure Cluster Peer A—Part 1



To begin the cluster configuration on a new fabric interconnect, connect to the serial console of the first member of the cluster (fabric A). Although there is a GUI Express Start option after fabric interconnect A is configured with an IP address, only the CLI method will be covered here.

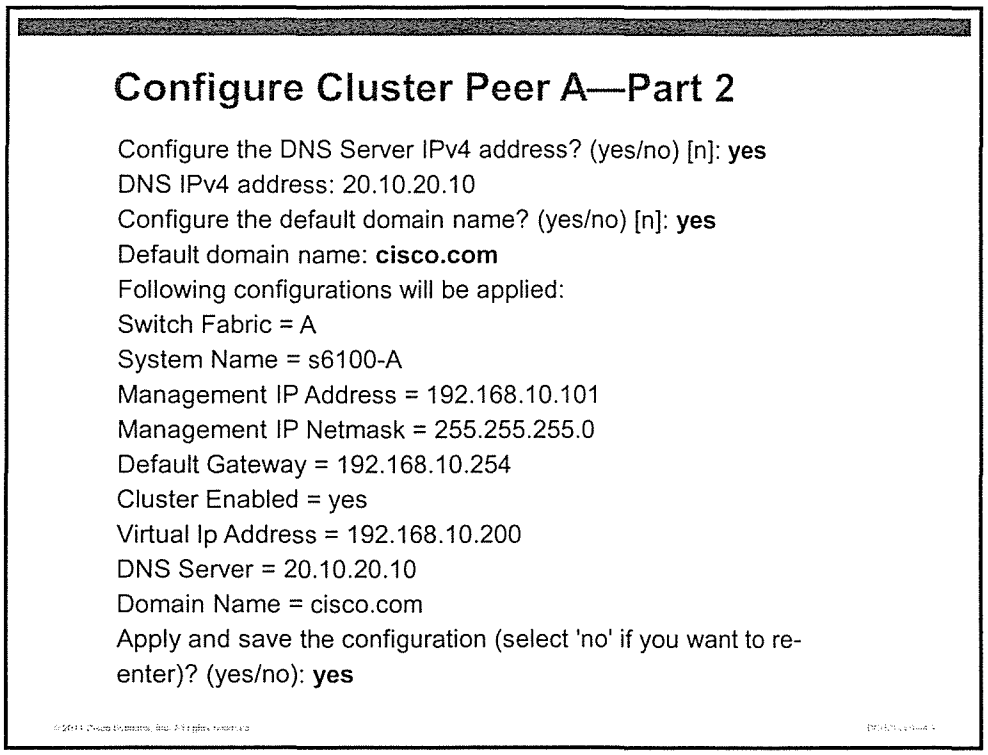
Like most Cisco devices with an RJ-45 serial console port, you can use a standard Cisco DB-9 to RJ-45 console cable. Configure your favorite terminal emulator for 9600 b/s, 8 data bits, 1 stop bit, and no parity (9600-8-1-none).

You will be prompted whether you would like to enter setup. Type "**Yes**" and press **Enter**.

All cluster configurations will be completed from the console, so select **Console**. Answer **Yes** to whether you want to create a cluster on the switch. If you decide initially to configure the fabric interconnect as standalone, it can be converted to cluster mode later.

The fabric selection for the first fabric interconnect is usually "A." After entering the hostname and IP information, you must select a virtual IP address. This is the address that you will use to connect to the active management node. While both nodes can be accessed from the CLI, only the active management node will permit a Cisco UCS Manager GUI connection.

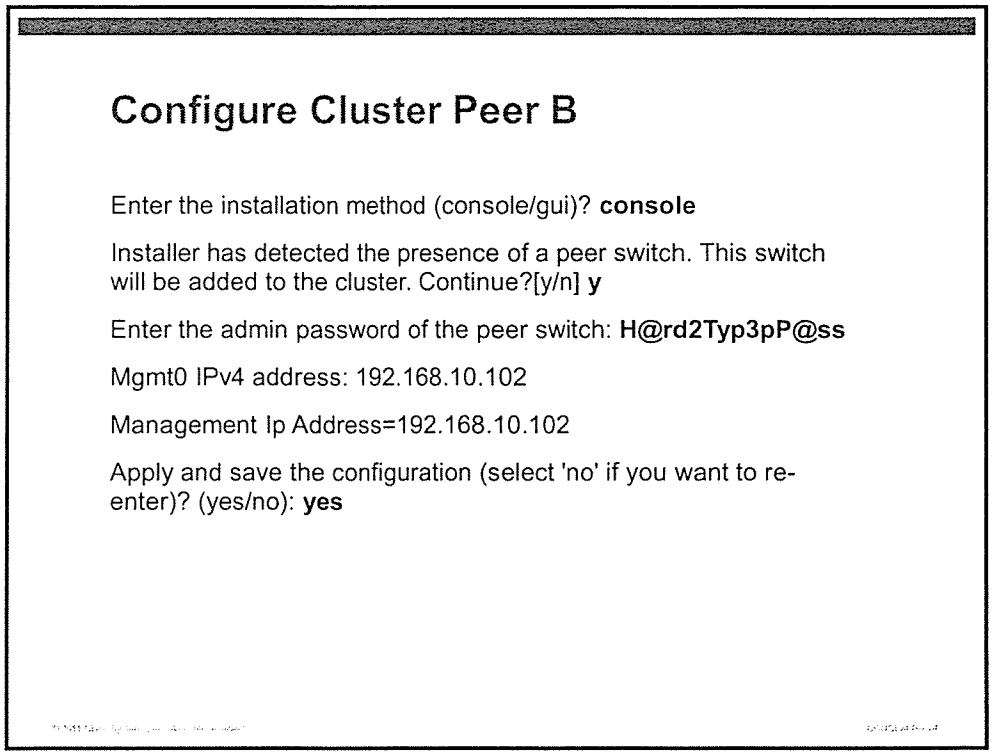
Configure Cluster Peer A—Part 2



The remainder of the dialog prompts for basic network connectivity options, including the Domain Name System (DNS) server and domain. The setup wizard then allows you to review your configuration and make corrections if necessary. When you answer "yes" to apply and save the configuration, the cluster services are configured and enabled on fabric interconnect A.

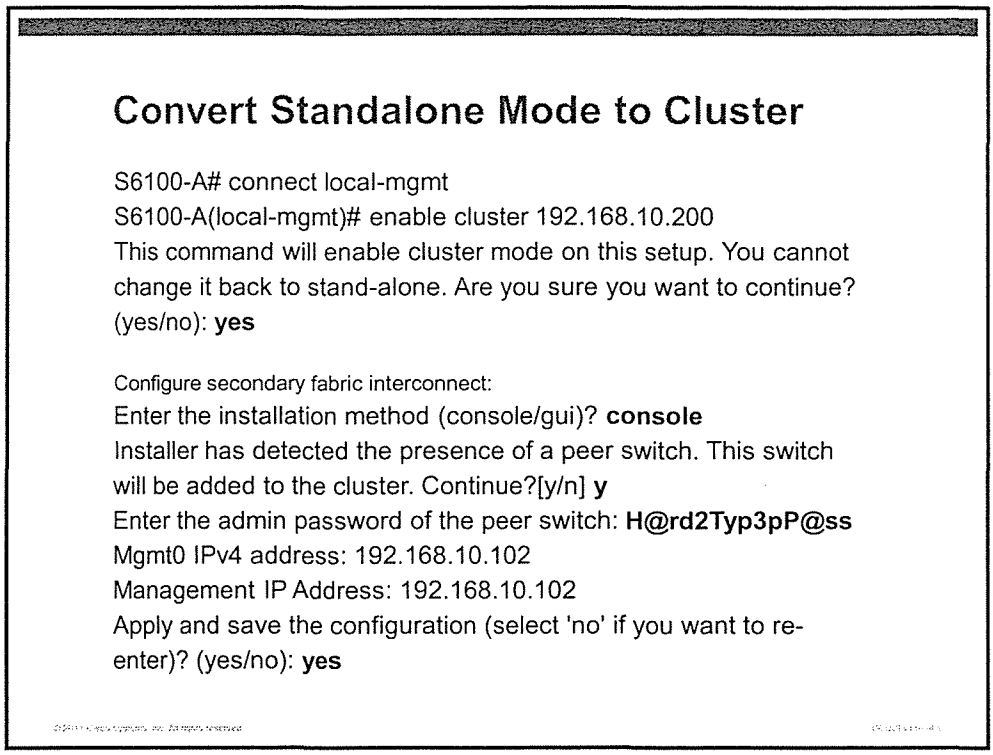
Note	The hostname and domain name need to be configured correctly to later enroll with a certificate authority (CA). The fully qualified domain name (FQDN) is part of the certificate signing request (CSR). Be certain that the FQDN is unique within your domain.

Configure Cluster Peer B



Assuming the Layer 1 and Layer 2 links are connected correctly, the second peer will detect the primary peer and ask to join the cluster. Enter the admin password and enter "**yes**" after reviewing the configuration. The primary peer will perform an initial synchronization from active to subordinate node. This includes all elements of the Cisco UCS Manager configuration database and images in the firmware store.

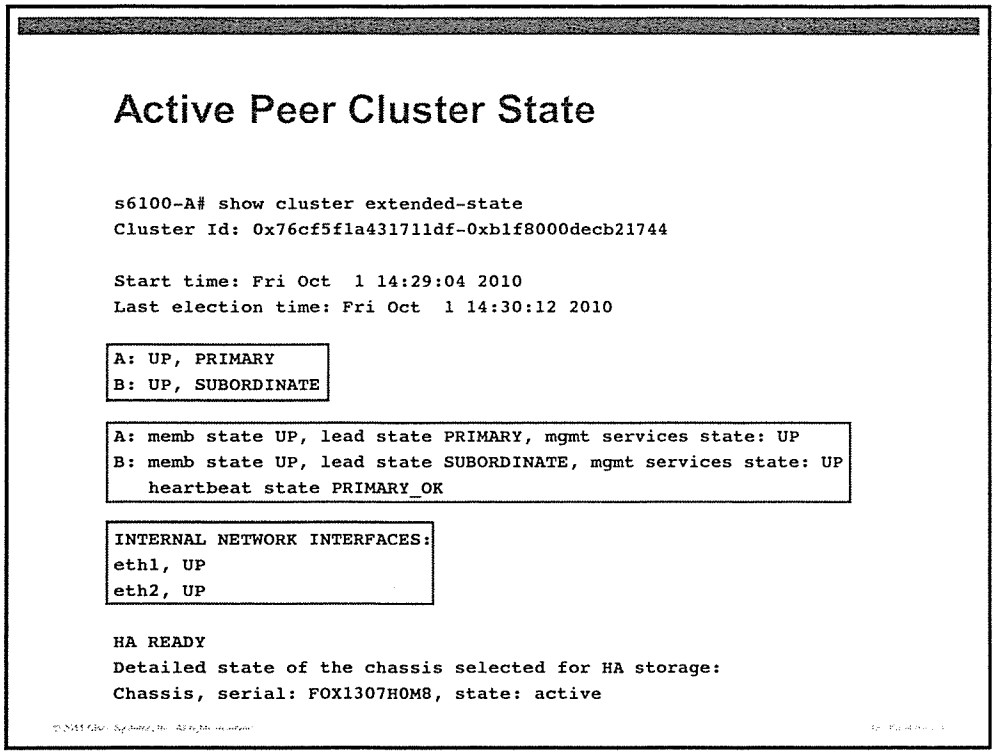
Convert Standalone Mode to Cluster



One potential scenario that might trigger the need to convert from standalone mode into a cluster is a proof-of-concept lab. Based on your budget to evaluate Cisco UCS, a redundant fabric interconnect might not be an option. After the evaluation is approved for conversion to production use, a secondary fabric interconnect is essential for production data center operation. The command **enable cluster 192.168.10.200** creates a new cluster on the fabric interconnect and defines 192.168.10.200 as the virtual IP address for the cluster.

To complete the cluster, connect Layer 1 to Layer 1 and Layer 2 to Layer 2 to enable cluster peer communication, and then add the secondary peer, as in the previous example.

Active Peer Cluster State

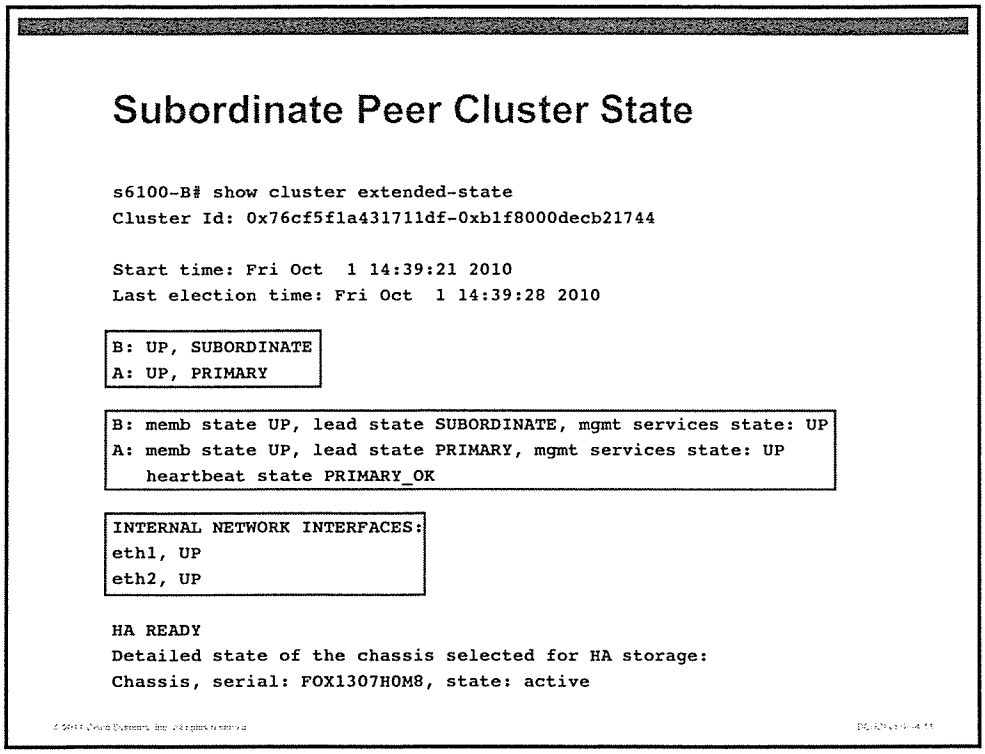


The **show cluster extended-state** command includes information that administrators need to validate cluster configuration and troubleshoot cluster operation. The output on this screen indicates that this fabric interconnect is the primary management node. The first fabric interconnect in a cluster is always assigned as fabric A.

All configuration is performed on the active management node. Before the active node commits a configuration transaction to the data management engine (DME), it first replicates the transaction to the subordinate node. After the subordinate acknowledges that its DME committed the transaction, the primary node commits the transaction.

On the active management node, the management plane and data planes are both active.

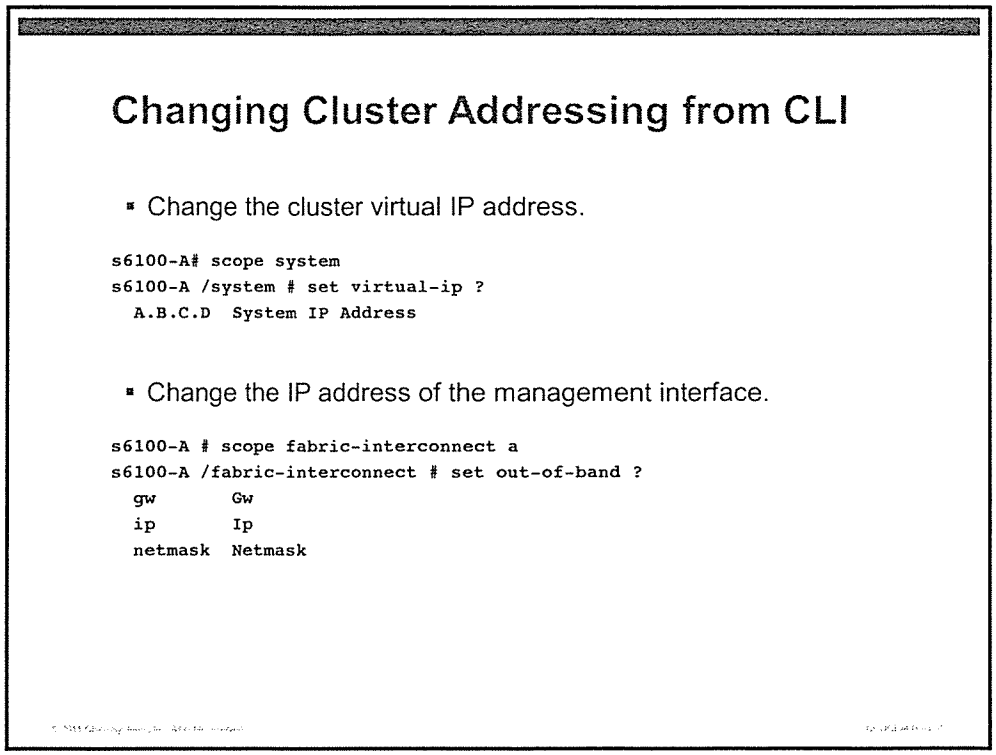
Subordinate Peer Cluster State



The subordinate node is not in a passive "standby" mode. The DME is active and accepts data that is synchronized from the active management node. Therefore, a distinction is made that it is *subordinate active*. If the active management node fails, the subordinate will wait a predetermined time and then declare the peer dead. At that time, the subordinate becomes the active management node.

Even when in subordinate mode for the management plane, the data plane is active and forwarding.

Changing Cluster Addressing from CLI



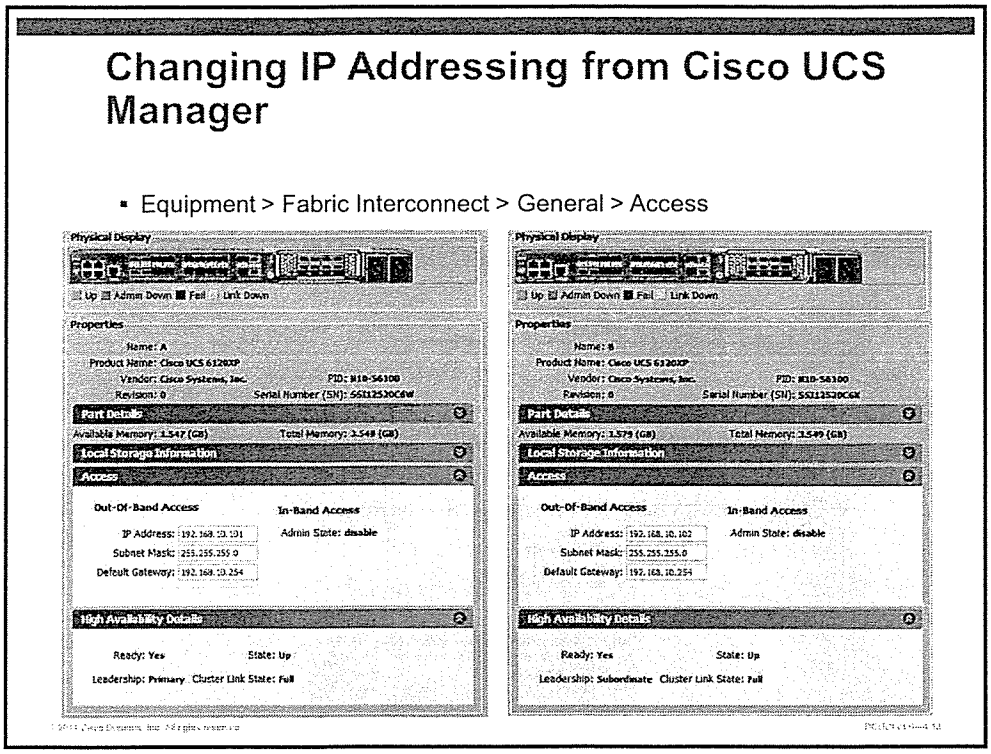
The ability to modify the IP settings of the cluster from the serial console is very useful. For example, if you set the wrong subnet mask on one of the cluster peers during setup, the cluster will not synchronize and you may not be able to access the virtual IP address for management.

```
s6100-A # scope fabric-interconnect a
s6100-A /fabric-interconnect # set out-of-band ip 192.168.10.101
s6100-A /fabric-interconnect # set out-of-band netmask
255.255.255.0
s6100-A /fabric-interconnect # set out-of-band gw 192.168.10.254
```

The cluster virtual IP address can only be changed in the Cisco UCS CLI.

```
s6100-A# scope system
s6100-A /system # set virtual-ip 192.168.10.200
```

Changing IP Addressing from Cisco UCS Manager



The IP address of either fabric interconnect can also be changed from the Cisco UCS Manager GUI.

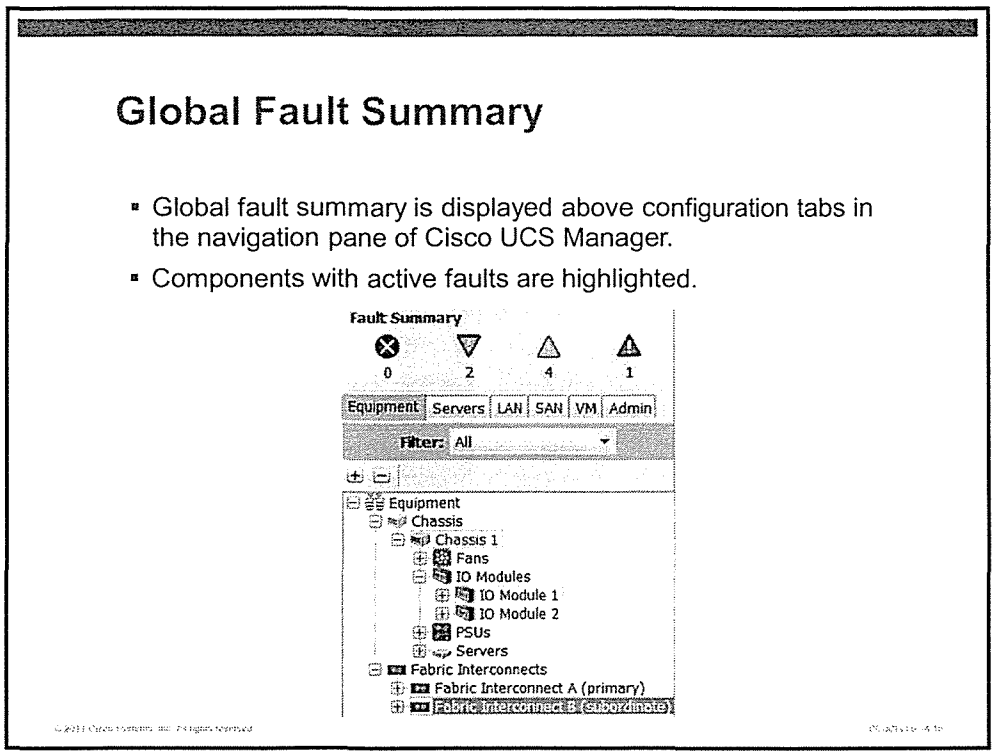
Note	If you change the IP address of the active management node and you used its explicit IP address instead of the virtual IP, you will lose your connection and need to log back in.

It is a best practice to always log in to the cluster virtual IP address.

Fault Detection and Correction Using Cisco UCS Manager and the CLI

This topic discusses the fault detection and correction facilities of Cisco UCS Manager, including local and remote logging.

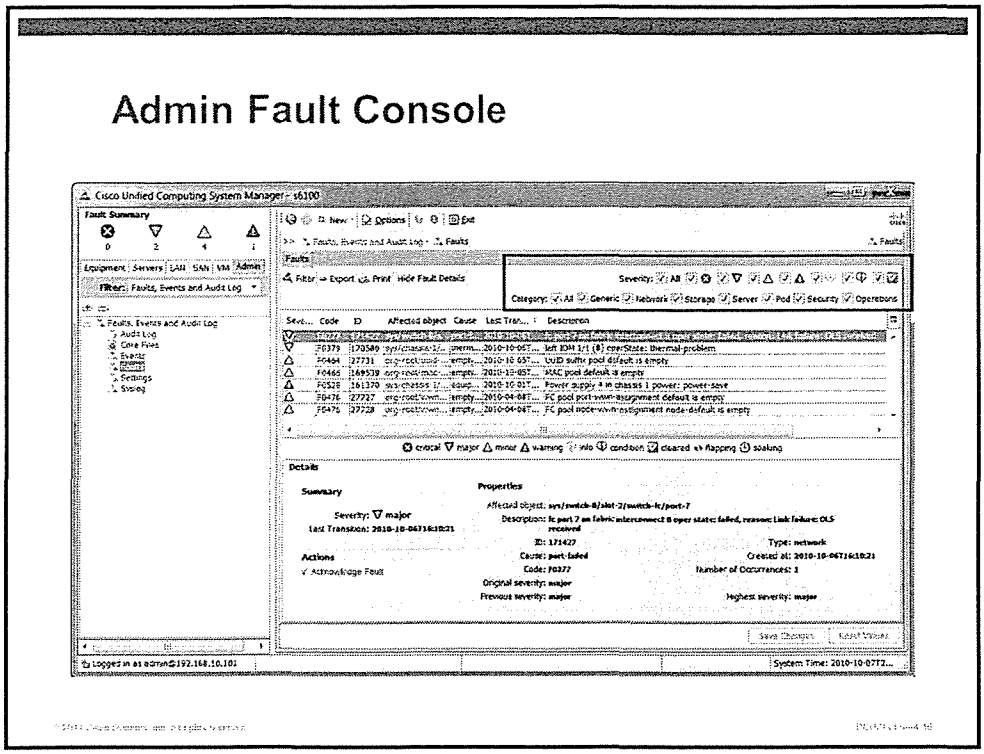
Global Fault Summary



Faults are categorized, in declining severity, as Critical, Major, Minor, and Warning. As you expand devices in the Equipment tab, devices with active faults have a rectangle around the device name. The color of the rectangle (red, orange, yellow, or green) indicates the level of the severity fault on the component.

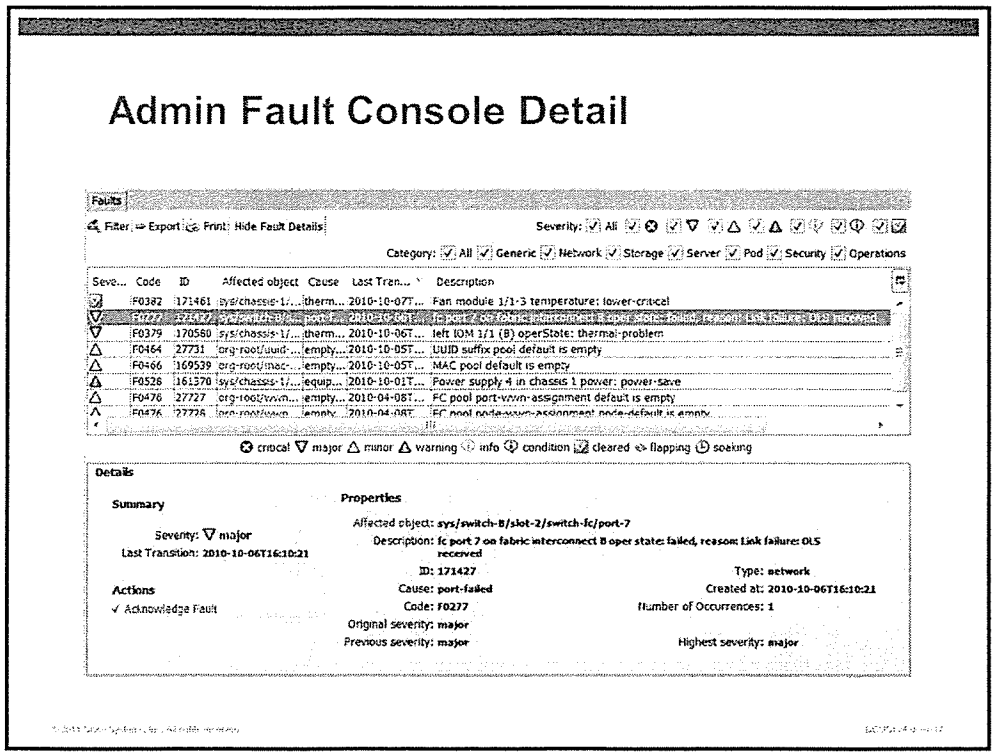
Clicking a fault icon in the fault summary will open the Admin tab to Faults, Events, and Audit Log.

Admin Fault Console



In the Admin tab under Faults, Events, and Audit Log, there is a Faults selection. By default, the console displays all fault severities and categories. The area that is highlighted in the illustration shows where you can filter the fault display to include only the criteria that is important to you. Filtering does not remove faults from the log, but only masks them.

Admin Fault Console Detail

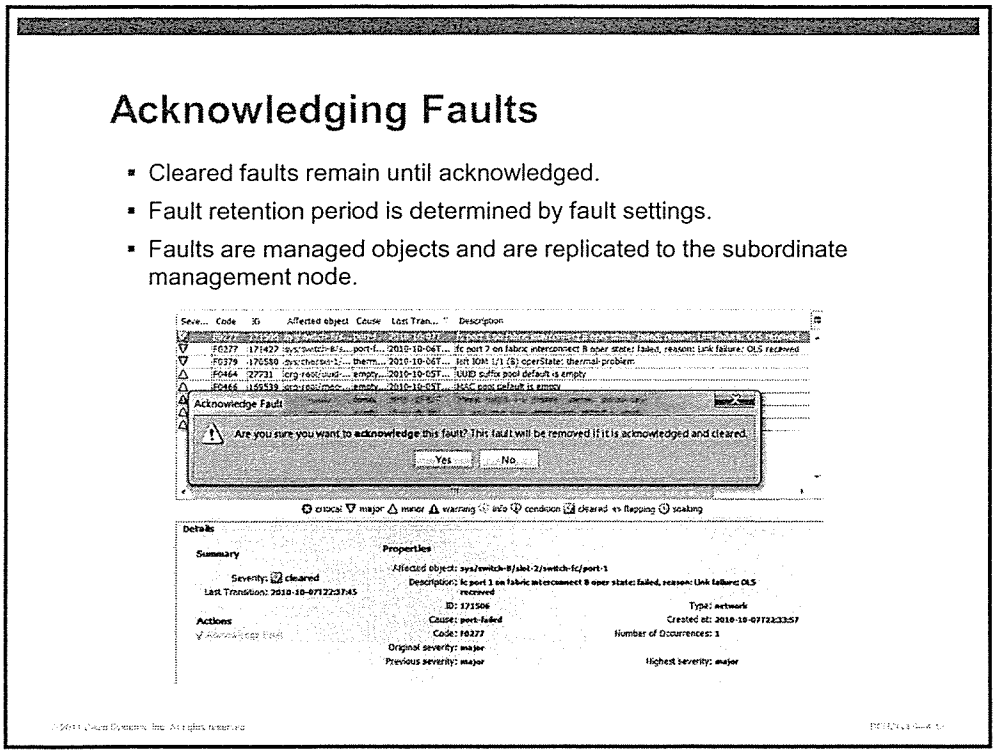


When you click an individual fault, the Details and Properties fields will populate with additional information about the fault. In this case, interface fc2/7 on fabric interconnect B is down. It received an offline sequence (OLS), indicating a loss of signal. Fc2/7 in the fabric interconnect expansion module is connected to fc1/9 on a Cisco MDS 9124.

Upon investigating the Fibre Channel switch, the cause of the fault is clear: the small form-factor pluggable (SFP) module was removed.

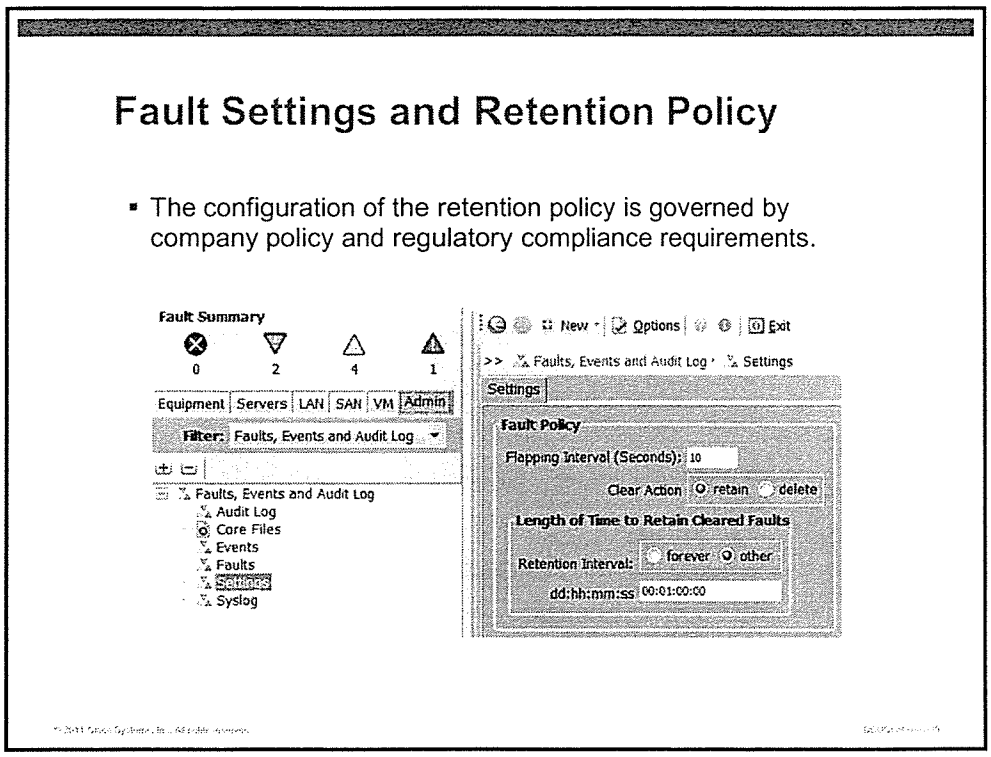
```
MDS9124-2# show interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper   Oper    Port
                  Mode   Trunk                          Mode   Speed   Channel
                         Mode                           (Gbps)
--------------------------------------------------------------------------------
fc1/1      12     auto   on      sfpAbsent       --     --             --
fc1/2      12     auto   on      sfpAbsent       --     --             --
fc1/3      12     auto   on      up              swl    F       4      --
fc1/4      12     auto   on      up              swl    F       4      --
fc1/5      12     auto   on      up              swl    F       4      --
fc1/6      12     auto   on      up              swl    F       4      --
fc1/7      12     auto   on      up              swl    F       4      --
fc1/8      12     auto   on      up              swl    F       4      --
fc1/9      12     auto   on      sfpAbsent       --     --             --
fc1/10     12     auto   on      up              swl    F       4      --
```

Acknowledging Faults



Interface fc2/1 went down and generated a major alarm. After the link transitioned back to operational state, the major alarm automatically cleared. Although the fault cleared, it will remain in the fault list for a time that is determined by the fault policy. The exception to this rule is if you explicitly acknowledge the fault. Acknowledging a cleared fault will cause the fault to be deleted, regardless of the fault policy.

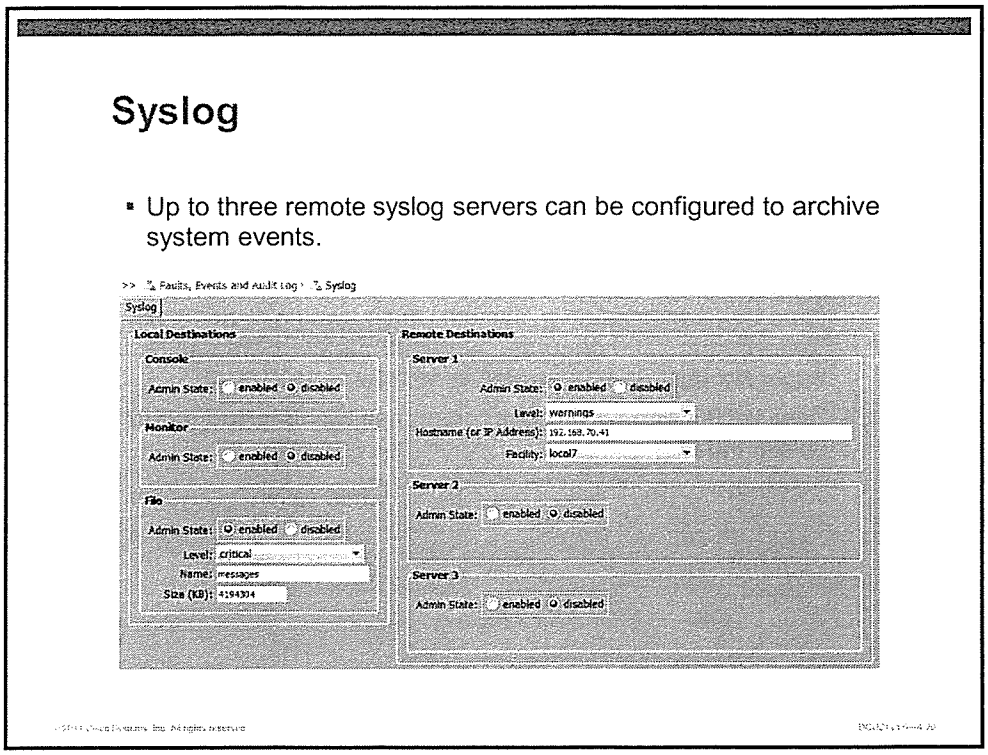
Fault Settings and Retention Policy



The fault policy determines the flapping interval and fault retention policy. The default flapping interval is 10 seconds. If a fault becomes active and clears more than once during the flapping interval, the fault is marked as flapping, which prevents excessive numbers of the same fault from being raised.

If the Clear Action is set to retain, you can set either a fixed amount of time or forever. If you set the retention time to 1 hour, all cleared faults will be retained for 60 minutes and then deleted. If the Retention Interval is set to forever, cleared faults will remain indefinitely unless explicitly acknowledged. When Clear Action is set to delete, cleared faults are immediately deleted.

Configuring Syslog

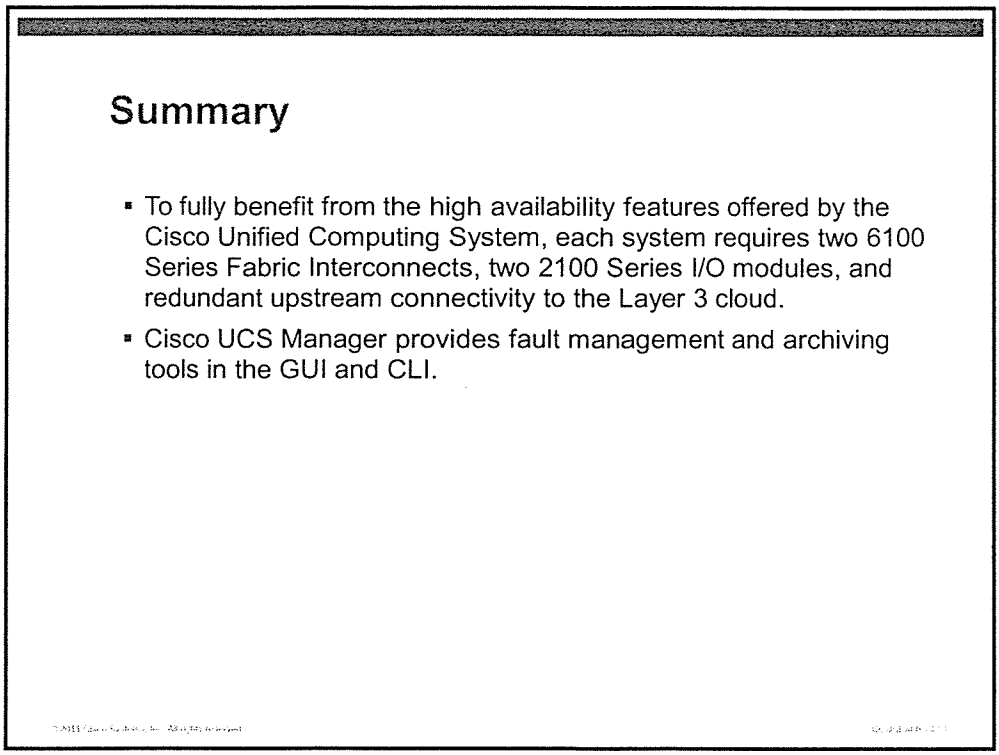


Fabric interconnects have a finite amount of storage for faults and logging data. Cisco UCS Manager allows you to configure up to three syslog servers as remote logging destinations. The log files on the syslog servers can be backed up and an archival copy can be stored to meet organizational and regulatory compliance policies.

Field	Description
Admin State	State can be enabled or disabled.
Level	This field controls the type of messages that are sent to the syslog server. If you set the level to Warnings (level 4), messages in levels 1–4 will be sent to the syslog server. Levels 5–7 will be suppressed. If you set the logging level to Debugging, all messages will be sent. Consult your logging policy to determine the correct level. The logging level applies to both fabric interconnects in a cluster. Alert Messages, Severity 1 Critical Messages, Severity 2 Error Messages, Severity 3 Warning Messages, Severity 4 Notification Messages, Severity 5 Informational Messages, Severity 6 Debugging Messages, Severity 7
Hostname	Enter the FQDN or IP address of the syslog server.
Facility	This can be set from local0 to local5. Some syslog servers use this label as the filename for log messages from a given host. Most modern syslog servers allow you to log to a file based on source IP address.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 3

Installing Cisco UCS B-Series Hardware

Overview

Only properly trained individuals should install Cisco UCS B-Series servers. Installation by trained individuals ensures the safety of installation personnel, reliable operation, and ease of maintenance. Failure to follow installation procedures can result in serious bodily injury or death.

Implementers need to establish that the site is prepared, power is provisioned, and all environmental requirements are met before installation can begin.

Objectives

Upon completing this lesson, you will be able to define the requirements of a Cisco UCS B-Series installation. This ability includes being able to meet these objectives:

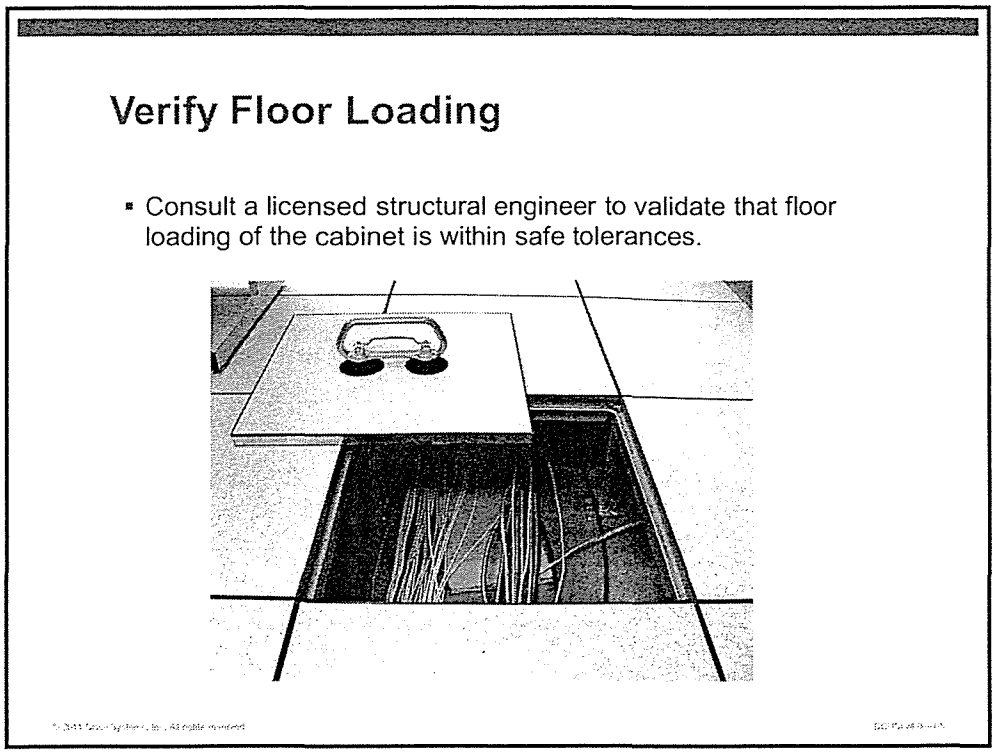
- Define the physical and environmental requirements for Cisco UCS B-Series servers, including dimensions, weight, and floor loading considerations
- List the steps for physical installation of rack-mount slides in the enclosure and on the Cisco UCS 5108 chassis
- List the steps for opening the cases of Cisco UCS B200, B230, B250, and B440 Blade Servers
- List the steps for installation and removal of CPU, RAM, and mezzanine cards in B-Series blades
- List the steps for physical installation and removal of local hard drives
- List the steps for installation of RAID BBU and RAID Key in B440 Blade Servers
- List the steps for physical installation of I/O modules and power supplies in the Cisco UCS 5108 chassis

- List the steps for physical installation and removal of fan units
- List the steps for physical installation of B200, B230, B250, and B440 Blade Servers
- List the steps for physical installation and removal of SFP+ copper Twinax and optical modules

Physical and Environmental Requirements for Cisco UCS B-Series Servers

This topic discusses critical planning and procedures necessary to safely install the Cisco UCS 5108 server chassis and components.

Verify Building Floor Loading



Floor loading refers to the measurement in pounds per square foot or kilopascals (kPa) per square meter of the foundational structure upon which the rack or cabinet is installed. Consult a licensed structural engineer to validate that the floor material can safely support the weight of your populated equipment cabinet.

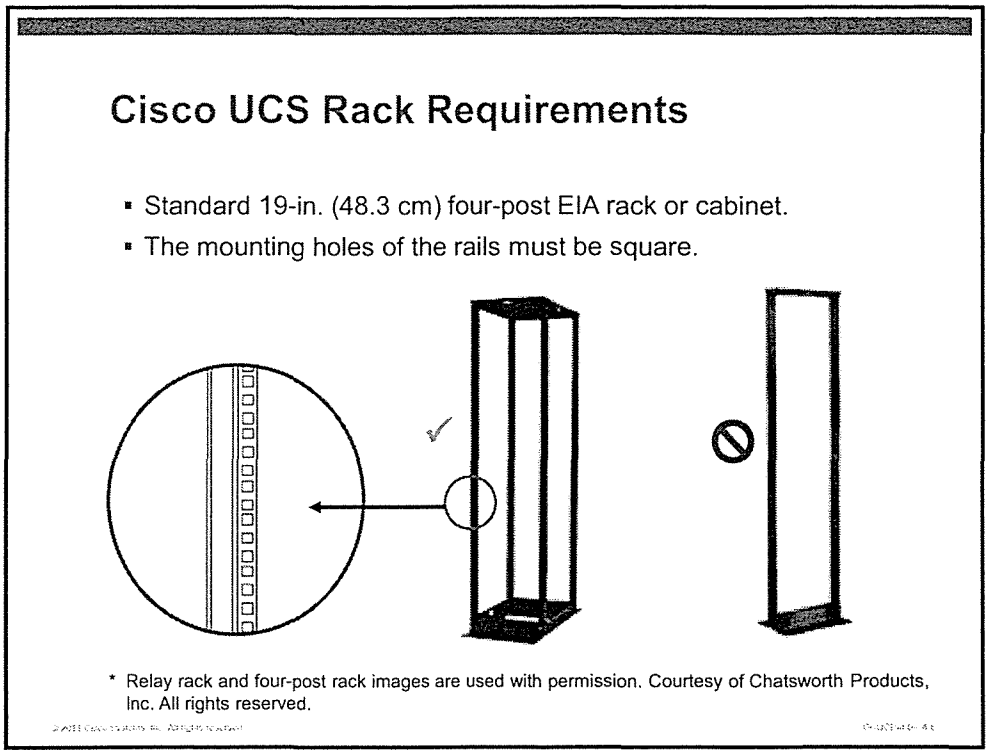
Physical Dimensions of UCS Server Chassis

Description	Specification
Height	10.5 in. (26.7 cm)
Width	17.5 in. (44.5 cm)
Depth	32 in. (81.2 cm)

Weight of Chassis Components

Description	Specification
Empty chassis	90 lb (40.83 kg)
2104XP Fabric Extender	2.5 lb (1.13 kg)
Fan module	1.8 lb (0.82 kg)
B200-M1 Blade Server	13.5 lb (6.12 kg)
Hard drive	0.8 lb (0.36 kg)
Weight	255 lb (115.66 kg) (maximum, fully populated)

Cisco UCS Rack Requirements

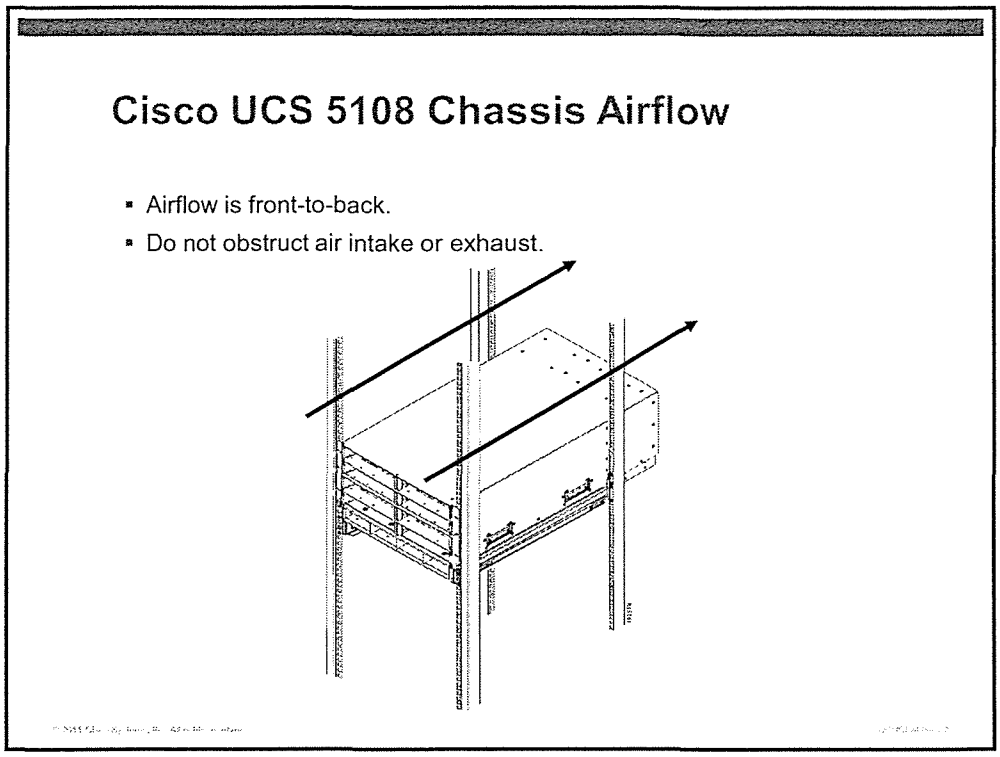


The Cisco UCS 5108 server chassis and 6100 Series Fabric Interconnects require a four-post EIA rack. Mounting rails must conform to English universal hole spacing per Section 1 of ANSI/EIA-310-D-1992.

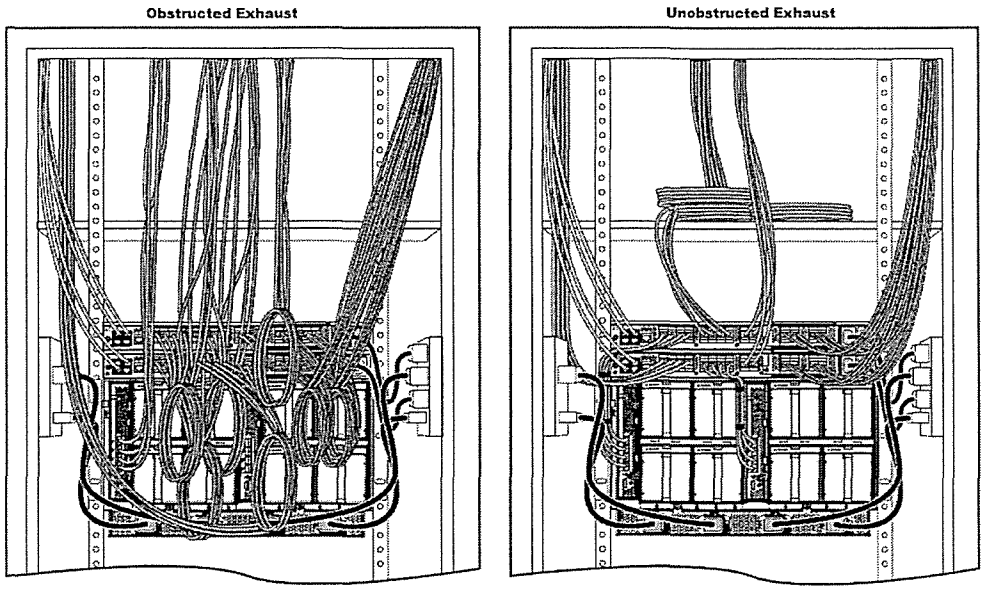
Do not attempt to install the 5108 chassis or Fabric Interconnect in a relay rack (two-post mount). The length and weight exceed the safe loading of a relay rack.

*Relay rack and four-post rack images are used with permission, courtesy of Chatsworth Products, Inc. All rights reserved.

Cisco UCS 5108 Chassis Airflow



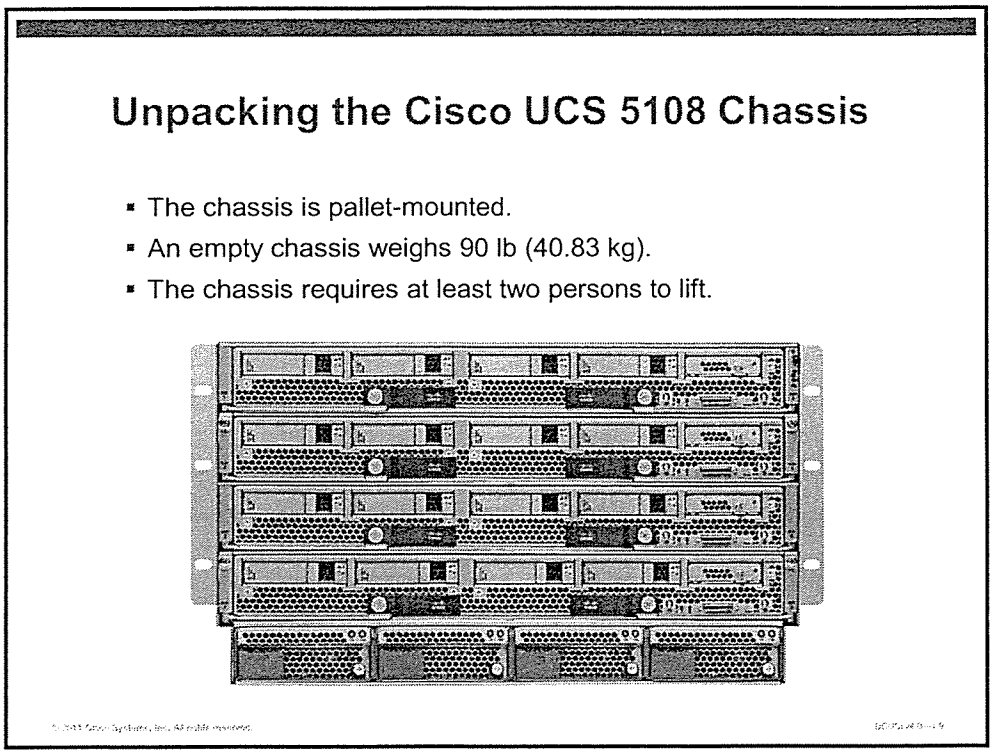
Ensure that the exhaust at the rear of the chassis is unobstructed for at least 24 in. (61 cm). This includes obstruction due to poor cable management. Route cables so that they do not impede fan exhaust. Exhaust obstructions can lead to unreliable operation and component failure.



Physical Installation of Rack-Mount Slides in the Enclosure and on the UCS 5108 Chassis

This topic discusses the steps to safely install the rack mount in an enclosure to support the Cisco UCS 5108 server chassis.

Unpacking the UCS 5108 Chassis



The Cisco UCS 5108 chassis is pallet-mounted. Follow this procedure to unpack the empty chassis:

Step 1 Before accepting receipt of the shipment, carefully inspect the box for damage. If there is evidence of rough handling, reject the shipment and work with your shipper to file a damaged-in-transit claim. Signs of rough handling include a broken pallet, smashed corners, or large holes.

Step 2 Move the pallet as close as possible to your data center staging area.

Step 3 Cut the straps that secure the outer cardboard shell.

Step 4 Lift the outer shell straight up and off.

Step 5 Remove accessory boxes and packing material.

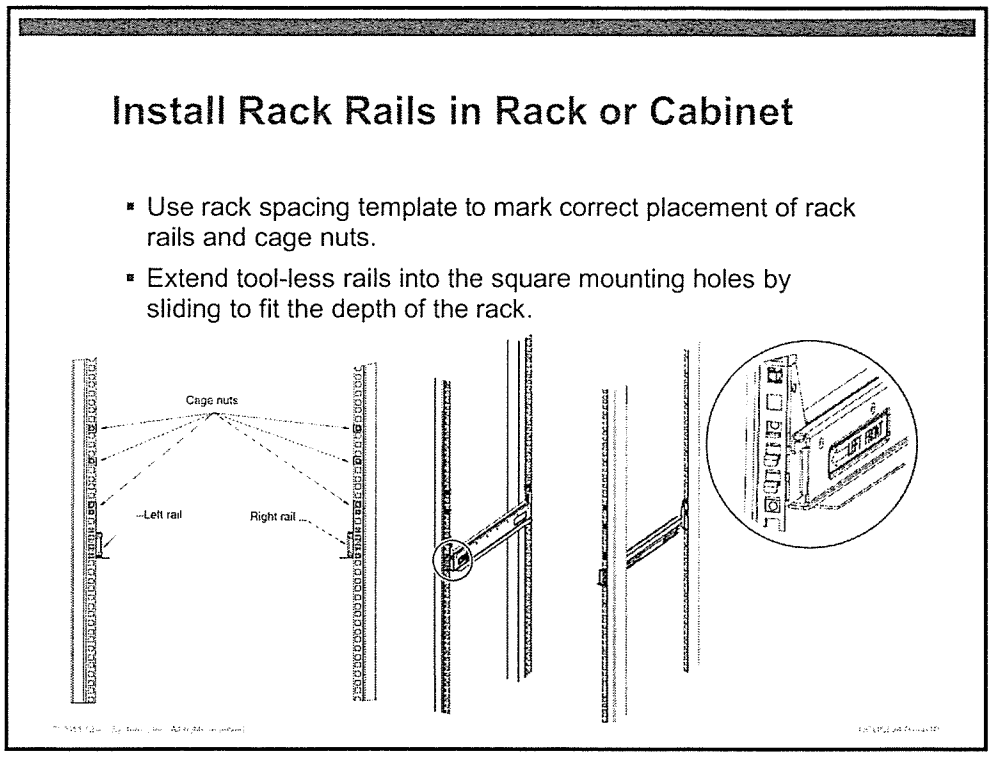
Step 6 Use at least two persons to lift the chassis out of the box.

Step 7 *Do not* use the handles on the side of the chassis to lift. They were designed for repositioning the chassis only.

Step 8 Remove power supplies from the bottom of the box.

Step 9 Retain all shipping materials in the event that you need to ship the unit.

Install Rack Rails in Rack or Cabinet



Follow this procedure to install the chassis rack rails:

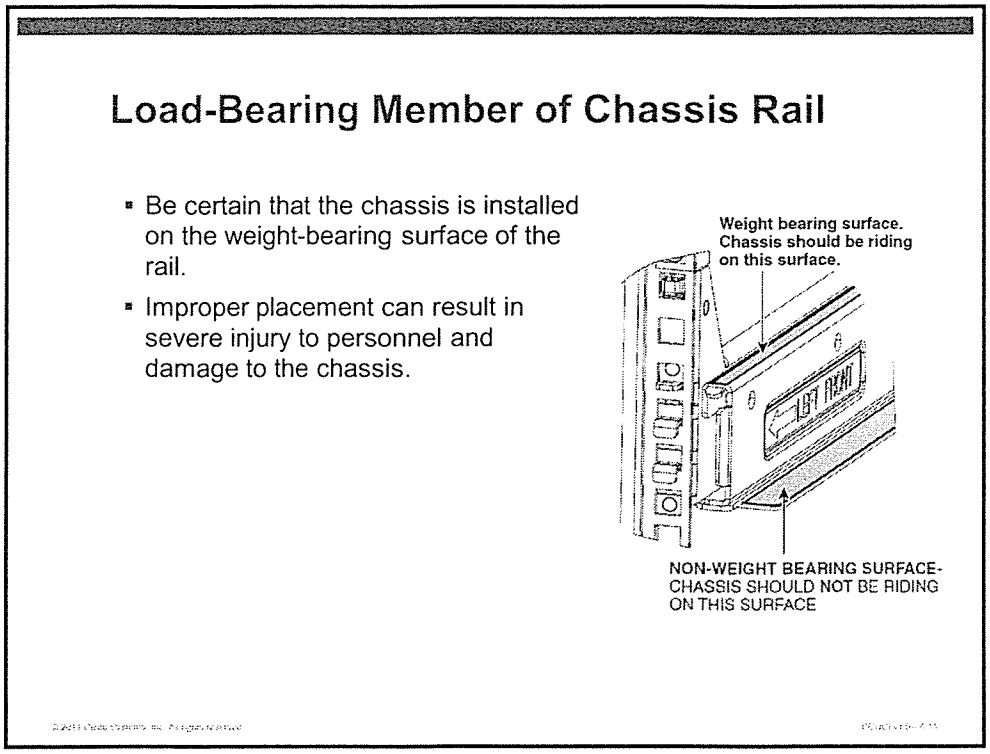
Step 1 Use the supplied paper template to mark the holes on all rails of the rack where the tool-less rails and cage nuts will be installed.

Step 2 Extend the tool-less rails and attach to the square mounting holes in the rack or cabinet. (Rack rails are clearly marked left and right.)

Step 3 Install cage nuts where indicated by the template.

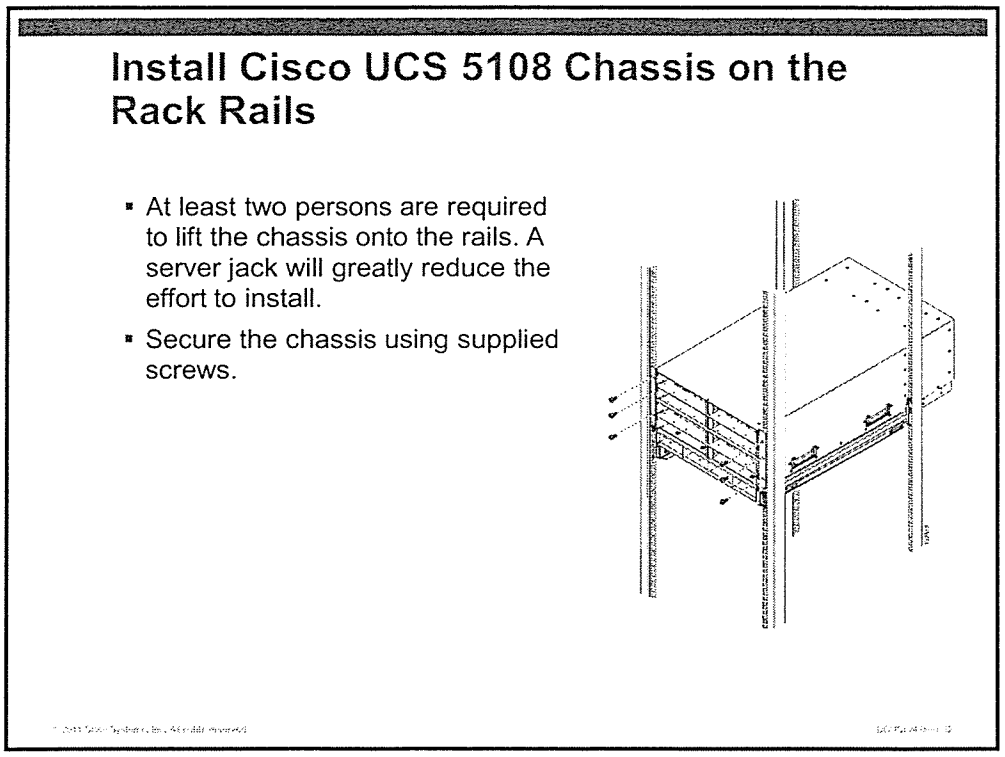
Step 4 Use a level to be sure that the rail is installed correctly.

Load-Bearing Member of Chassis Rail



Ensure that the chassis is mounted on the load-bearing portion of the rail. Serious injury and equipment damage can result from improper positioning.

Install Cisco UCS 5108 Chassis on the Rack Rails



Follow this procedure to install the Cisco UCS 5108 chassis into the rack or cabinet:

Step 1 If the rack or cabinet is on casters, employ the wheel brakes.

Step 2 Using at least two persons, slide the chassis onto the load-bearing portion of the rack rails.

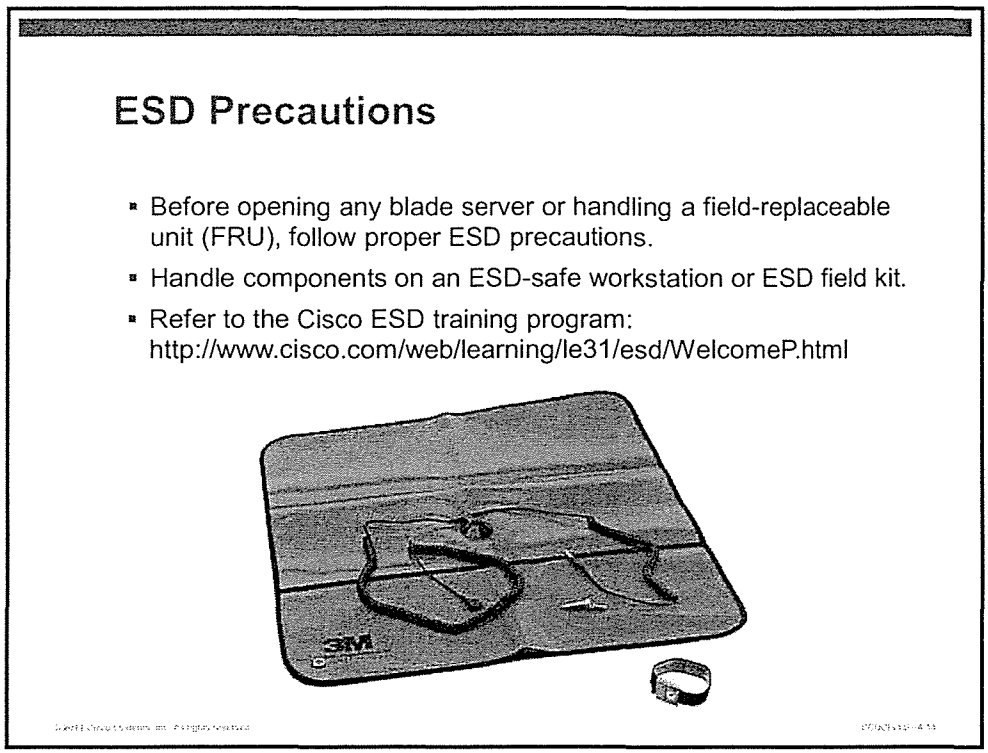
Step 3 Install the six 10-32 x 0.75-in. Phillips round washer head screws into the cage nuts.

Step 4 Torque the screws to no more than 20 ft-lb (27 Newton meters).

Opening the Cases of UCS B200, B230, B250, and B440 Blade Servers

This section discusses the ESD precautions and procedures to open B-Series server cases.

ESD Precautions



ESD from your skin, hair, or clothing can degrade or destroy components of the Cisco UCS B-Series blade servers and IOMs. When a nonconductor and conductor make and break contact, a charge is formed on the conductor. If you rub a plastic comb across wool fabric, enough static charge is formed to make your hair move when the comb gets close. If you touch a doorknob and can feel the shock, the power that was discharged into the doorknob was at least 3000 V. There are components in blade servers that can be damaged or rendered nonfunctional by less than 100 V.

Observe proper ESD precautions whenever you open a blade server. This includes wearing a grounded wrist strap and handling components on a static dissipative work surface. Your data center equipment staging area should have the proper grounded surfaces.

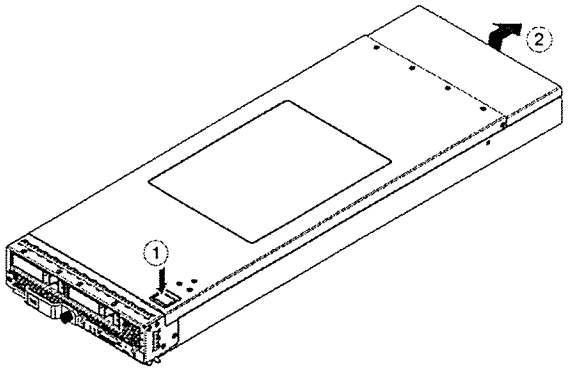
Follow these basic precautions:

- Only remove components from static-shielded bags on a static-safe work surface.
- Follow the site policy for ESD precautions by wearing a wrist strap (and heel strap if required).
- Roll up long-sleeved shirts.
- Tie-back long hair so it cannot make contact with the equipment.
- Remove any jewelry that could dangle on to the equipment.
- If wearing a necktie, tuck it into your shirt.

Opening the Cisco UCS B200 Blade Server

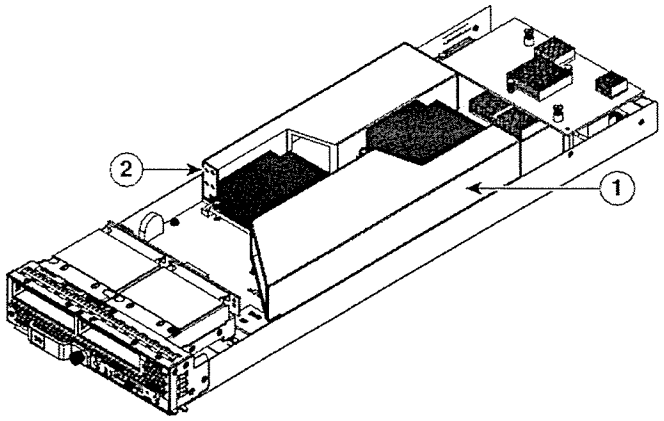
Opening the Cisco UCS B200 Blade Server

- Before opening the cover, place the server on an ESD-safe work surface and wear a grounded wrist strap.
- Push the button near the front of the case top and slide the cover toward the rear and up.

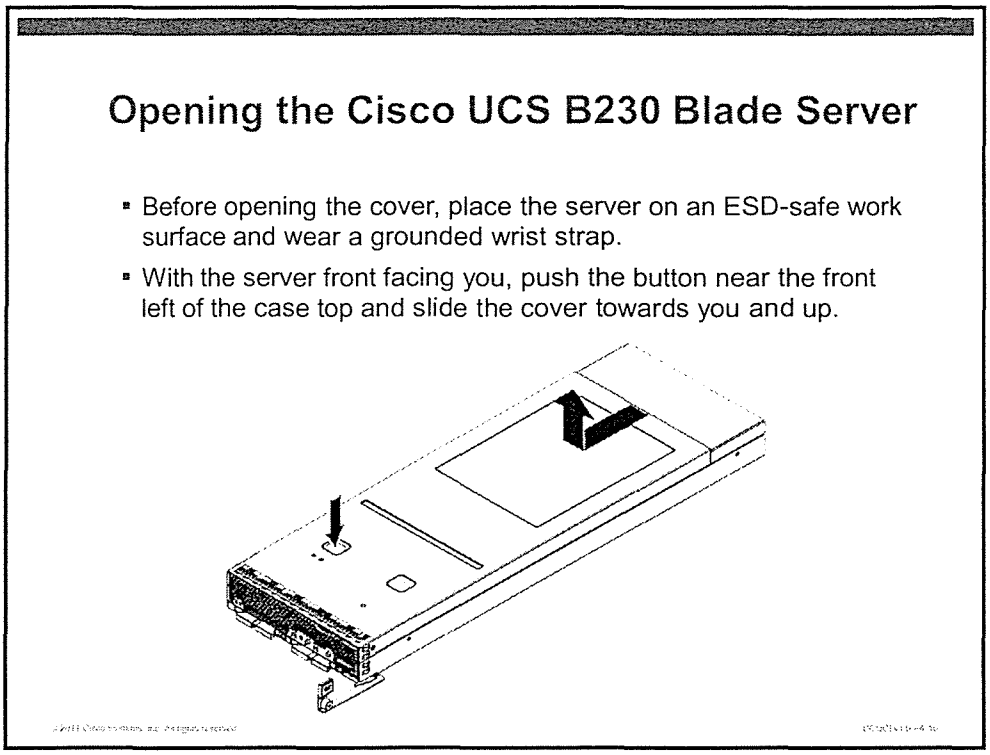


There are slight physical differences internally between the UCS B200 M1 and B200 M2 Blade Servers. The M2 model comes with two removable baffles that guide airflow over the DIMMs more efficiently. It is possible to purchase new baffles to retrofit B200 M1 blades. The baffles drop in with no tooling required.

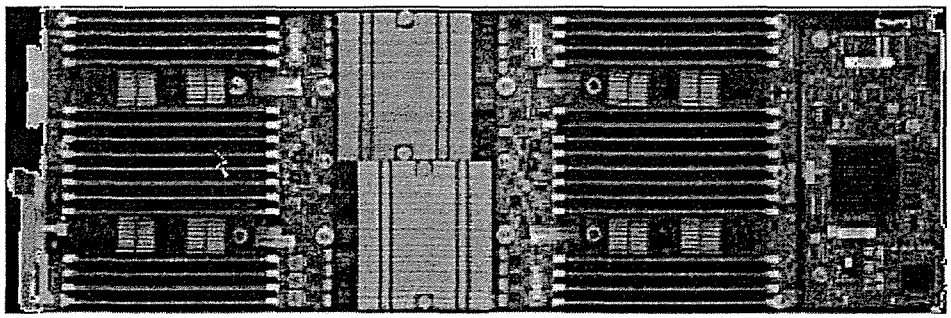
The baffles need to be lifted out to install or remove the CPU and DIMMs. Be certain to replace the baffles before closing the case.



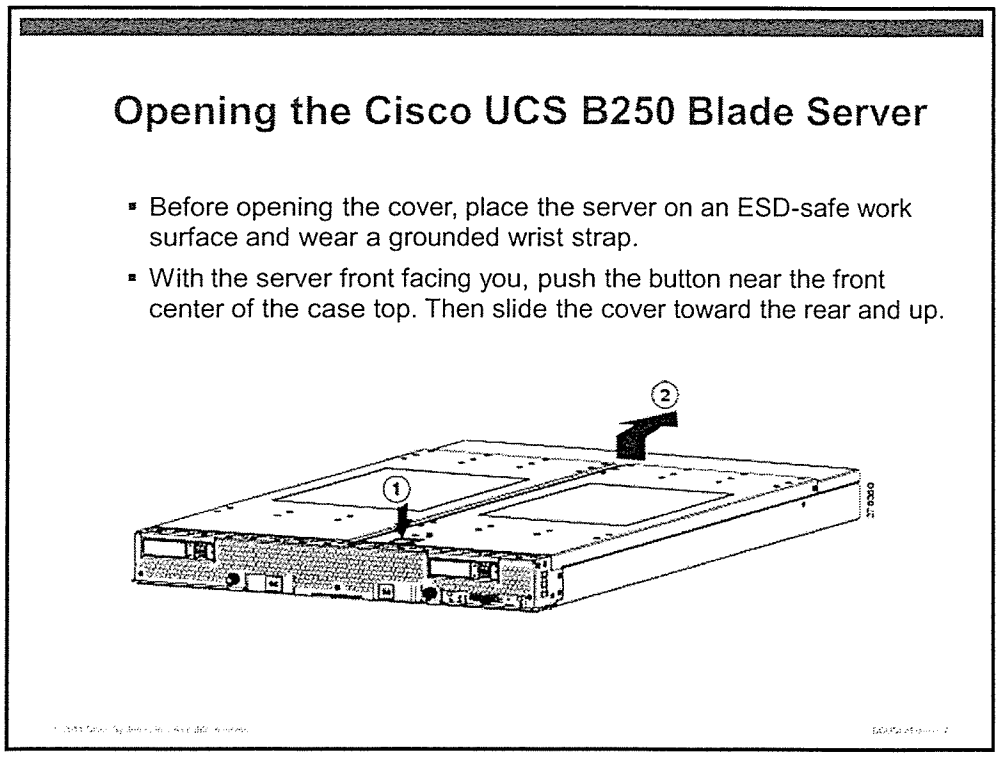
Opening the Cisco UCS B230 Blade Server



The Cisco UCS B230 Blade Server differs significantly from the B200 M1 and B200 M2 Blade Servers. Although it includes two CPU sockets, there are 32 DIMM slots. With the increased density of components on the motherboard, additional care should be taken when installing and removing field-replaceable units (FRUs).



Opening the Cisco UCS B250 Blade Server

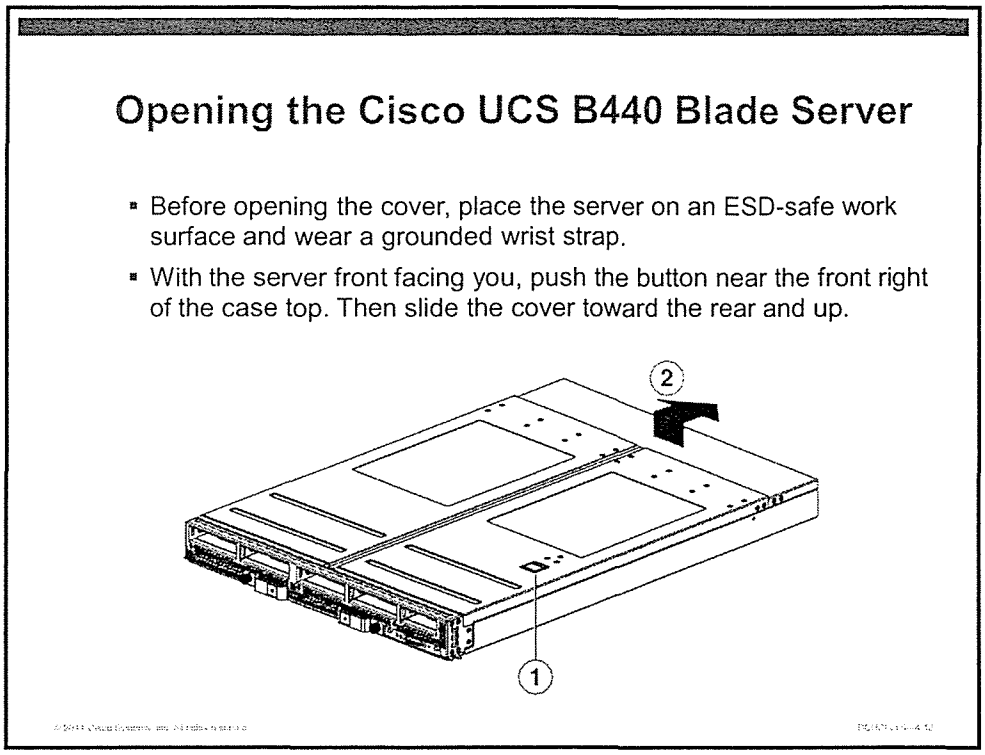


The Cisco UCS B250 M1 and B250 M2 Blade Servers differ in a few important areas, but procedures for installation of FRUs is identical.

Model	Capability
B250 M1	Intel Xeon 5500 Series CPU All RAM clocked at 1066 MHz
B250 M2	Intel Xeon 5600 Series CPU All RAM clocked at 1333 MHz and low-voltage DIMM support

Note With the UCS B250 Blade Server, the displayed VMware ESX and Linux operating system hard disk drive (HDD) boot device order is the reverse of the BIOS HDD boot order. To correct this discrepancy, review both of the disks and drive labels, as applicable, during installations of VMware ESX and Linux versions and choose the correct disk for installation.

Opening the Cisco UCS B440 Blade Server

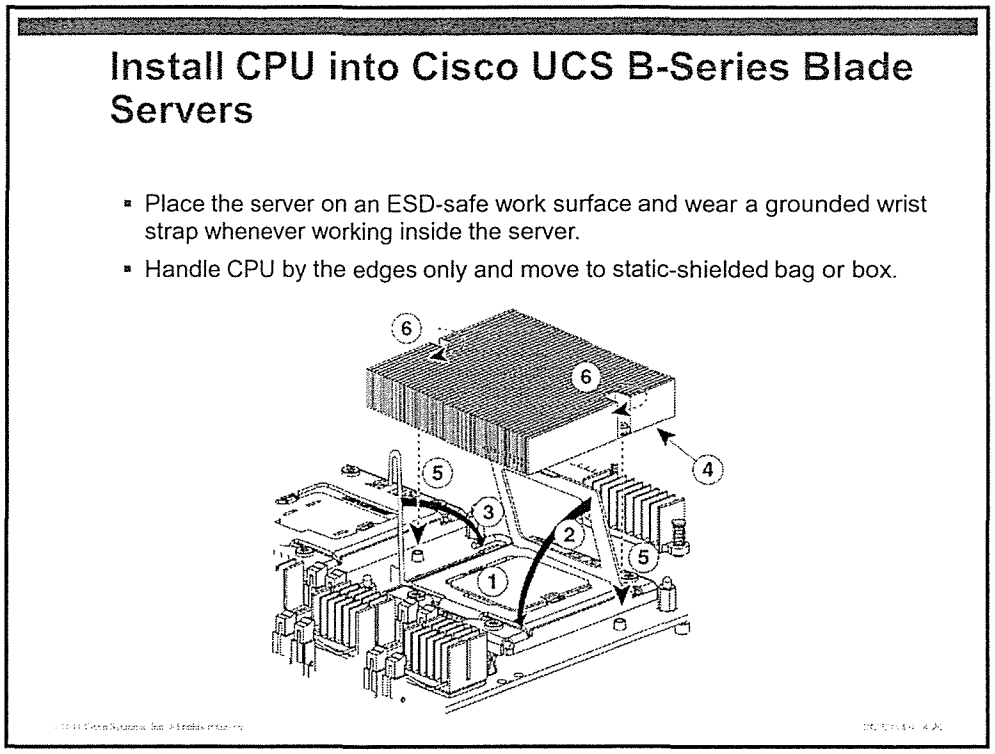


The Cisco UCS B440 Blade Server is the first four-socket CPU blade server. It offers support for two or four Intel Xeon 7500 series CPUs. This also includes eight DIMM slots per CPU, for a maximum capacity of 256 GB of RAM running at 1066 MHz.

Installation and Removal of CPU, RAM, and Mezzanine Cards in Cisco UCS B-Series Blade Servers

This topic discusses the steps that are required to install and remove CPU, RAM, and mezzanine cards in Cisco UCS B-Series blade servers.

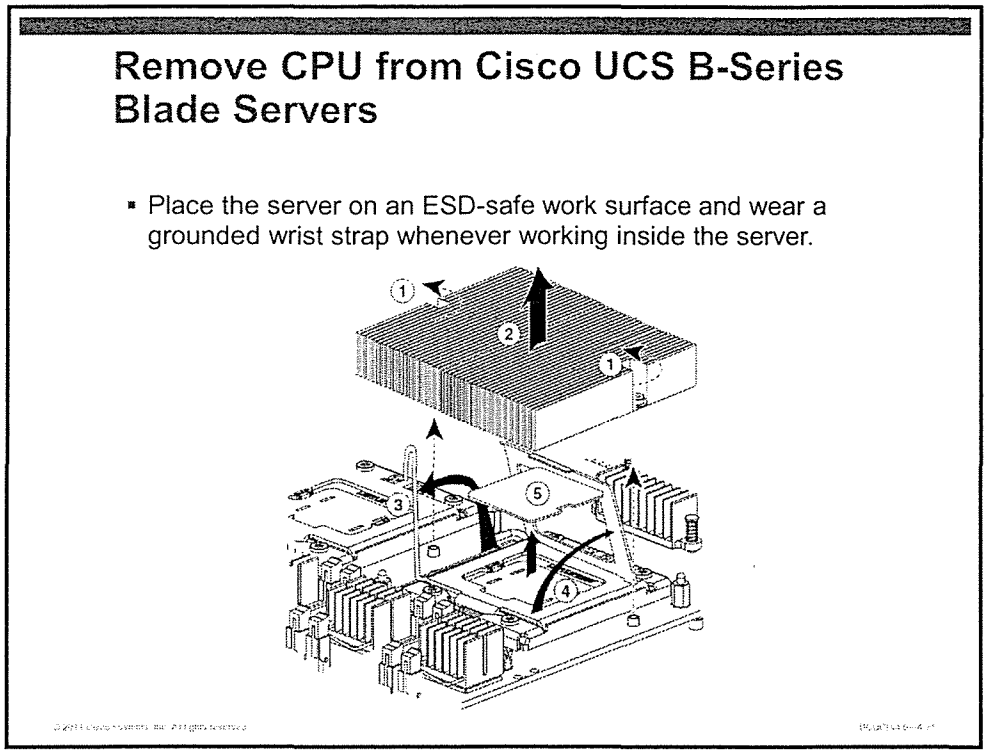
Installation of CPU into Cisco UCS B-Series Blade Servers



Follow this procedure to install a CPU into a Cisco UCS B-Series blade server:

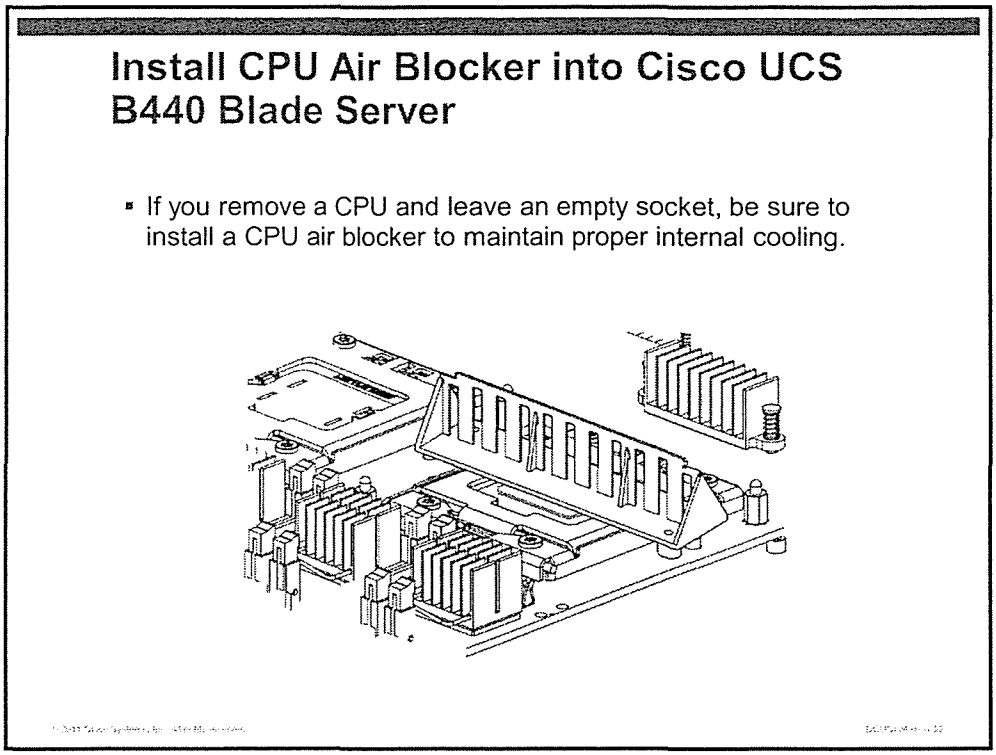
- Wear a wrist strap that is grounded to the blade server.
- Slide the CPU locking clasp down and to the side to release it (3, in the figure).
- Move the latch up until it is at a 90-degree angle with the CPU socket (2).
- Swing the CPU mounting bracket up and remove the CPU cover blank (4).
- Align the CPU with the socket. It should only fit one way.
- Lower the mounting bracket and socket latch and secure the CPU.
- Align heat sink so that the cooling slots face front-to-back. Air must flow through the heat sink.
- Carefully tighten the heat sink screws to the motherboard (6). Do not overtighten.

Remove CPU from Cisco UCS B-Series Blade Servers



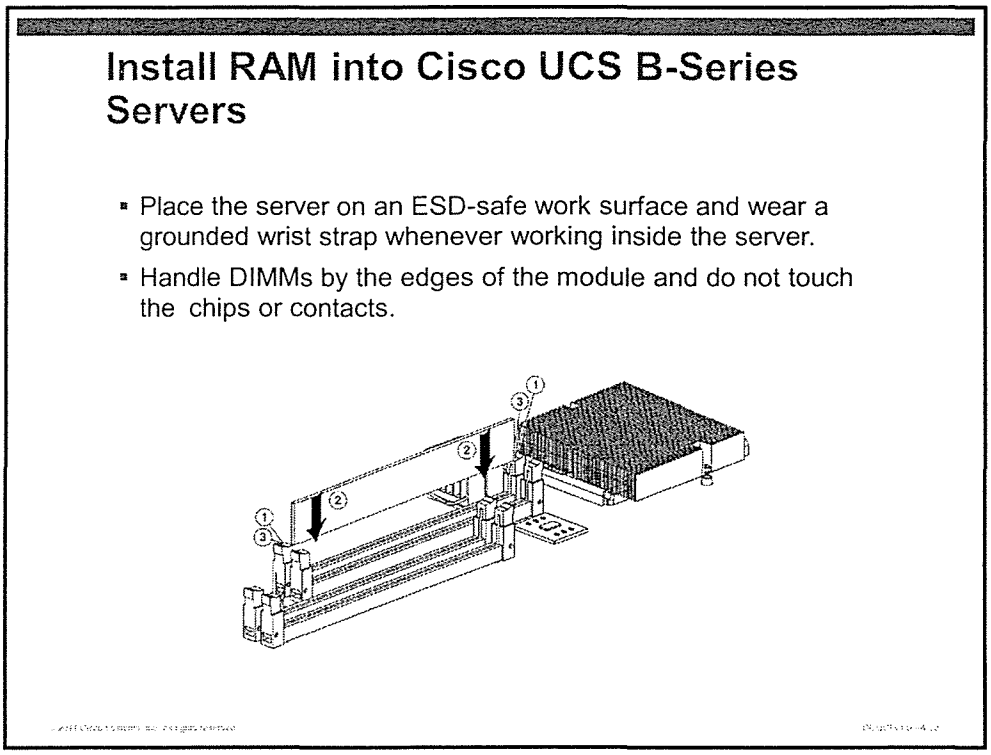
The CPU removal process is the reverse of the installation process. Be certain to replace the socket blank over the socket if you do not plan on replacing the CPU. Failure to use the socket cover can result in damage to the socket.

Install CPU Air Blocker into Cisco UCS B440 Blade Server



If you have removed a CPU from a Cisco UCS B440 Server and do not intend to replace it, you must install an air blocker. The air blocker will allow proper airflow over the components within the blade enclosure.

Install RAM into Cisco UCS B-Series Servers

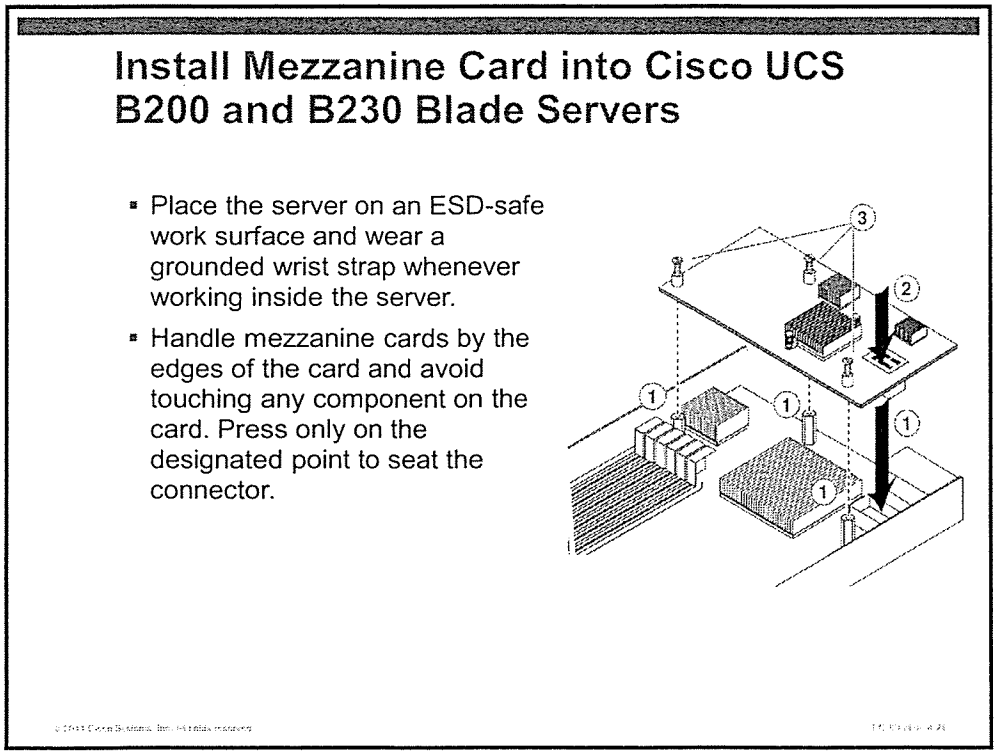


Follow this procedure to install DIMMs in any B-Series Server:

- Wear a wrist strap that is grounded to the blade server enclosure.
- Open the case.
- Fold the DIMM retainer clips away from the center of the DIMM slot (1, in the figure).
- Align the DIMM notch on the bottom of the module with the key in the slot.
- Push straight down with even pressure on both sides of the DIMM until it is firmly seated (2).
- Fold the retainer clips towards the center of the DIMM slot (3).

To remove a DIMM, reverse the process.

Install Mezzanine Card into Cisco UCS B200 and B230 Blade Servers

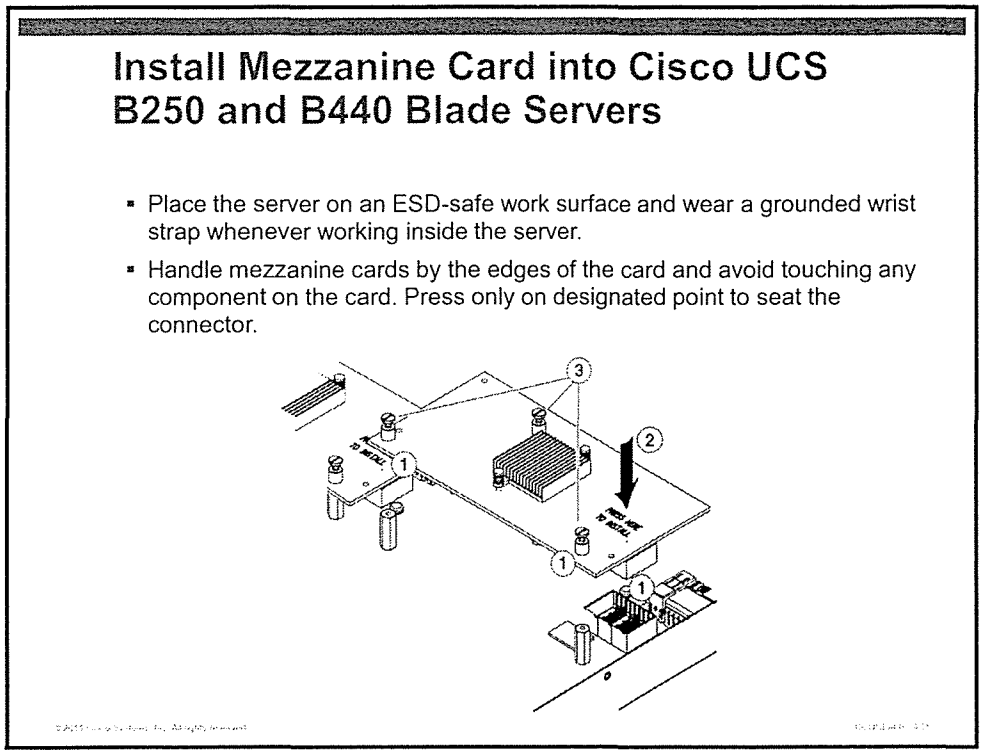


To install a mezzanine card in a Cisco UCS B200 or B230 Blade Server, follow this procedure:

- Wear a wrist strap that is grounded to the blade server enclosure.
- Open the case (1, in the figure).
- Handle the card by the edges and align the large Molex connector on the bottom of the module with the receptacle on the motherboard. (2)
- The silkscreen on the card is conspicuously marked "Press Here to Install." Press down on the marking until the card is fully seated. (2)
- Secure the three captive screws finger-tight. (3) Do not overtighten.

To remove a mezzanine card, reverse the process.

Install Mezzanine Card into Cisco UCS B250 and B440 Blade Servers



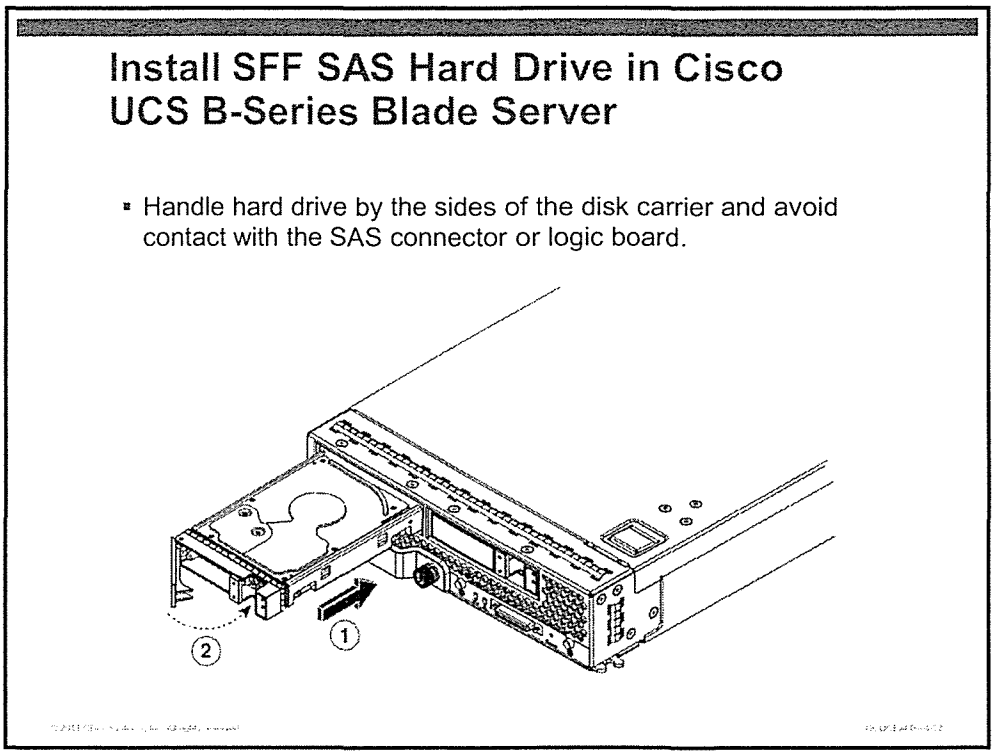
The procedure to install or remove mezzanine cards in the Cisco UCS B250 and B440 Blade Servers is identical to the procedure used with the Cisco UCS B200 and B230 Blade Servers. There are, however, version-specific rules for populating the adapters.

In Cisco UCS version 1.2, two adapters can be installed, but they must be the same type. Beginning with Cisco UCS version 1.3, two adapters can be installed and they can be different types.

Physical Installation and Removal of Local Hard Drives

This topic discusses the steps that are required for both installation and removal of local hard drives.

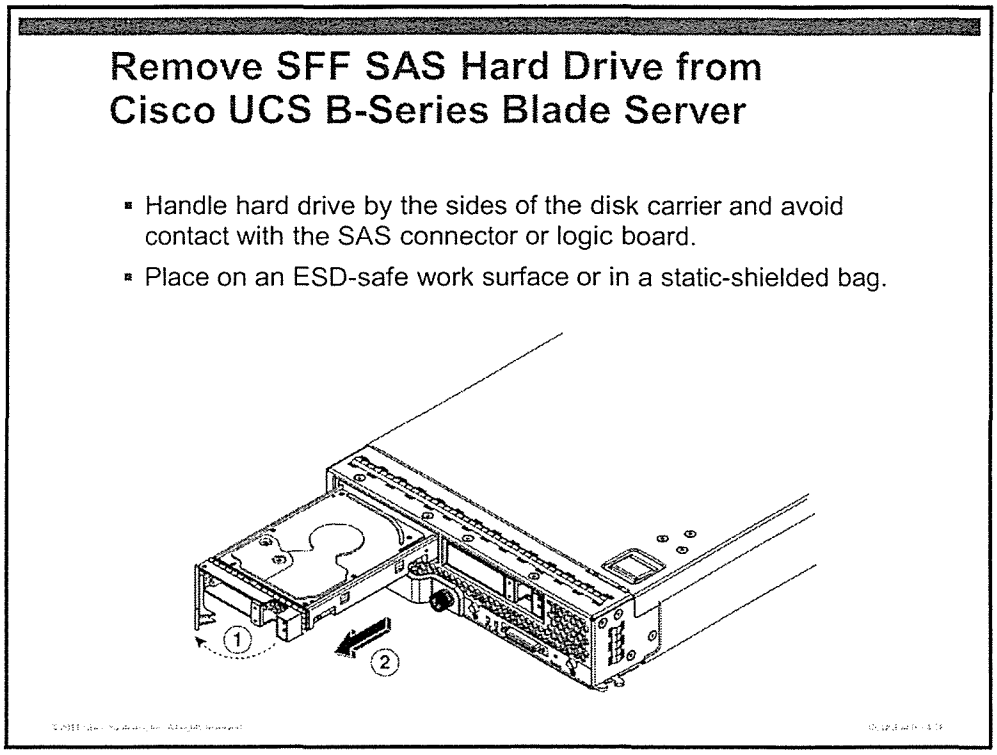
Install SFF SAS Hard Drive into Cisco UCS B-Series Blade Server



To install a small form-factor (SFF) serial attached SCSI (SAS) drive into a Cisco UCS B200, B250, or B440 Blade Servers, follow this procedure:

- Wear a wrist strap that is grounded to the blade server enclosure or chassis.
- Press the release catch on the ejector arm.
- Slide the hard drive carrier into the slot until fully seated (1, in the figure).
- Slide the ejector lever into the faceplate until it clicks into the locked position (2).

Remove SFF SAS Hard Drive from Cisco UCS B-Series Blade Server

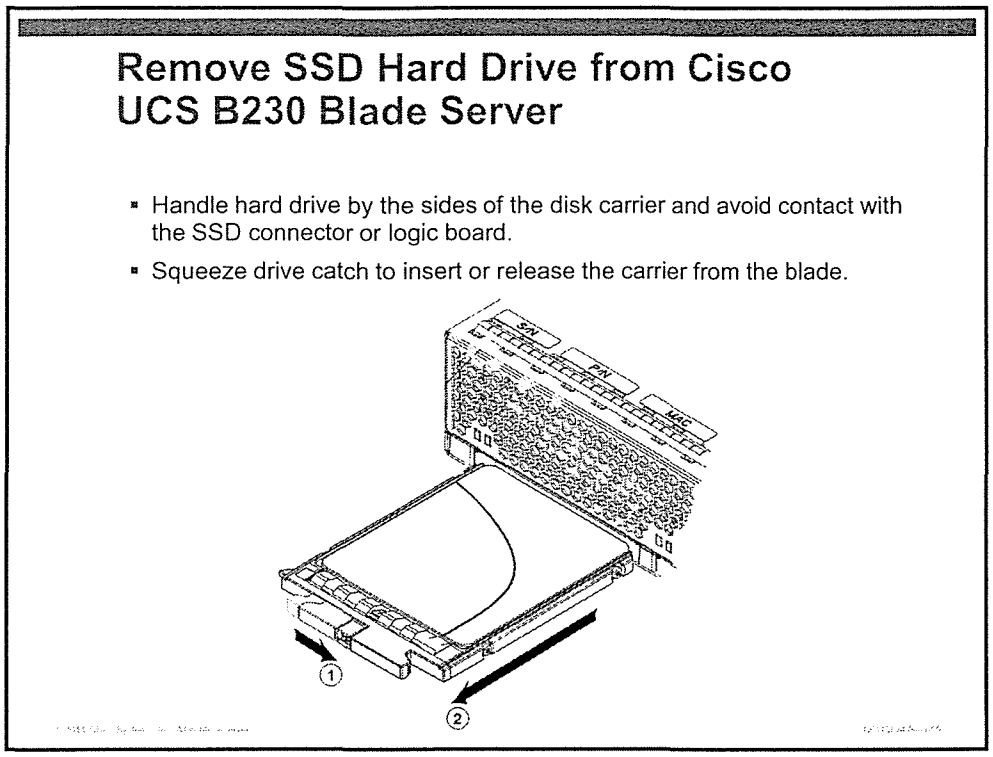


To remove a SFF SAS drive from a Cisco UCS B200, B250, or B440, follow this procedure:

- Wear a wrist strap that is grounded to the blade server enclosure or chassis.
- Press the release catch on the ejector arm and swing away from the hard drive faceplate (1, in the figure).
- Slide the hard drive carrier out of the slot (2).
- Store in a static shielded bag or enclosure.

Note	If you do not plan on replacing the removed hard drive, install a blanking plate to maintain proper airflow through the server.

Remove SSD Hard Drives from Cisco UCS B230 Blade Server



To remove an SSD drive from a Cisco UCS B230 Blade Server, follow this procedure:

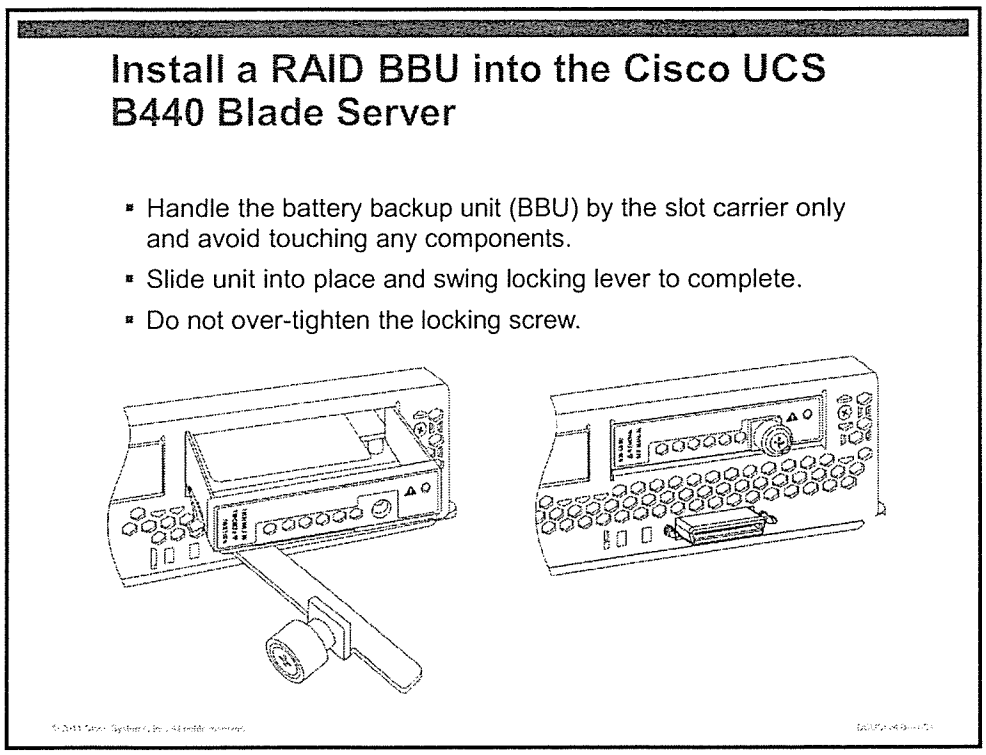
- Wear a wrist strap that is grounded to the blade server enclosure or chassis.
- Press the release catch on the solid-state drive (SSD) carrier (1, in the figure).
- Slide the SSD carrier out of the slot (2).
- Store in static-shielded bag or enclosure.

Note	If you do not plan on replacing the removed SSD, install a blanking plate to maintain proper airflow through the server.

Installation of RAID BBU and RAID Key in B440 Blades

This topic discusses how to install Redundant Array of Independent Disks (RAID) battery backup units (BBUs) and a RAID key in Cisco UCS B440 Blade Servers.

Install RAID BBU into the Cisco UCS B440 Blade Server



The LSI MegaRAID RAID adapter has the ability to speed-write transactions by employing a write cache. The controller stores write requests in RAM before they have been written to disk. If the controller loses power, any data in the write cache is lost and this can lead to data corruption.

An optional BBU is available with enough capacity to keep the write cache viable until power is restored. A fully charged BBU can supply power for up to 72 hours.

Follow these steps to install a RAID BBU into the Cisco UCS B440 Blade Server:

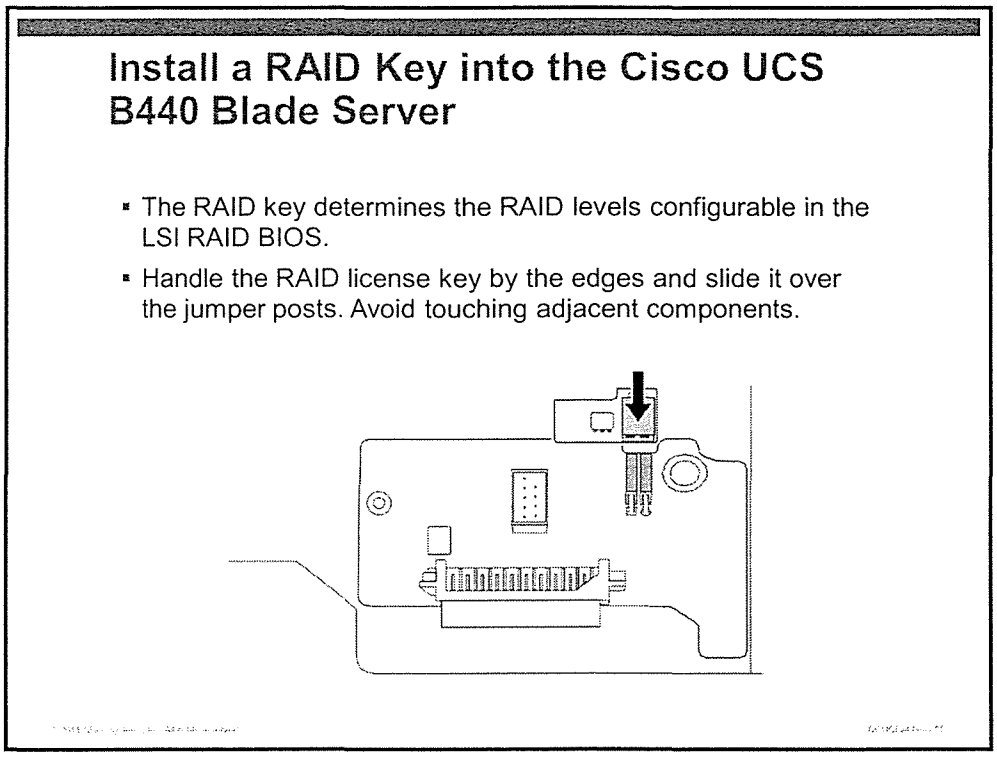
Step 1 Perform a graceful shutdown of the server operating system. Without a graceful shutdown, data may be permanently lost or corrupted.

Step 2 Remove the blanking plate from the BBU bay at the right of the server.

Step 3 Slide the BBU unit in partially, and slide the ejector lever into the faceplate of the BBU.

Step 4 Use fingers only to tighten the captive screw.

Install a RAID Key into the Cisco UCS B440 Blade Server



Depending on the RAID license key that is installed, the onboard RAID controller supports the following RAID levels:

- RAID 0 (data striping). There is no data redundancy, and all data is lost if any disk in the array fails.
- RAID 1 (disk mirroring). Data is written to two disks, providing complete data redundancy if one disk fails.
- RAID 5 (disk striping with distributed parity). Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk in the array fails.
- RAID 6 (disk striping with distributed parity across two disks). Data is striped across all disks in the array. Two parity disks are used to provide protection against the failure of up to two physical disks.
- RAID 10 (RAID 1 and RAID 0 in spanned arrays). RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- RAID 50 (RAID 5 and RAID 0 in spanned arrays). RAID 50 uses both parity and disk striping across multiple disks to provide complete data redundancy and high throughput rates.
- RAID 60 (RAID 6 and RAID 0 in spanned arrays). RAID 60 uses both distributed parity across two parity disks and disk striping across multiple disks to provide complete data redundancy and high fault tolerance.

The Cisco RAID key is the original equipment manufacturer (OEM) version of LSI MegaRAID SAS 8880EM2 SGL. If a replacement is needed, the stock LSI key will not work as a replacement because the physical connector is different. You must order replacements from Cisco.

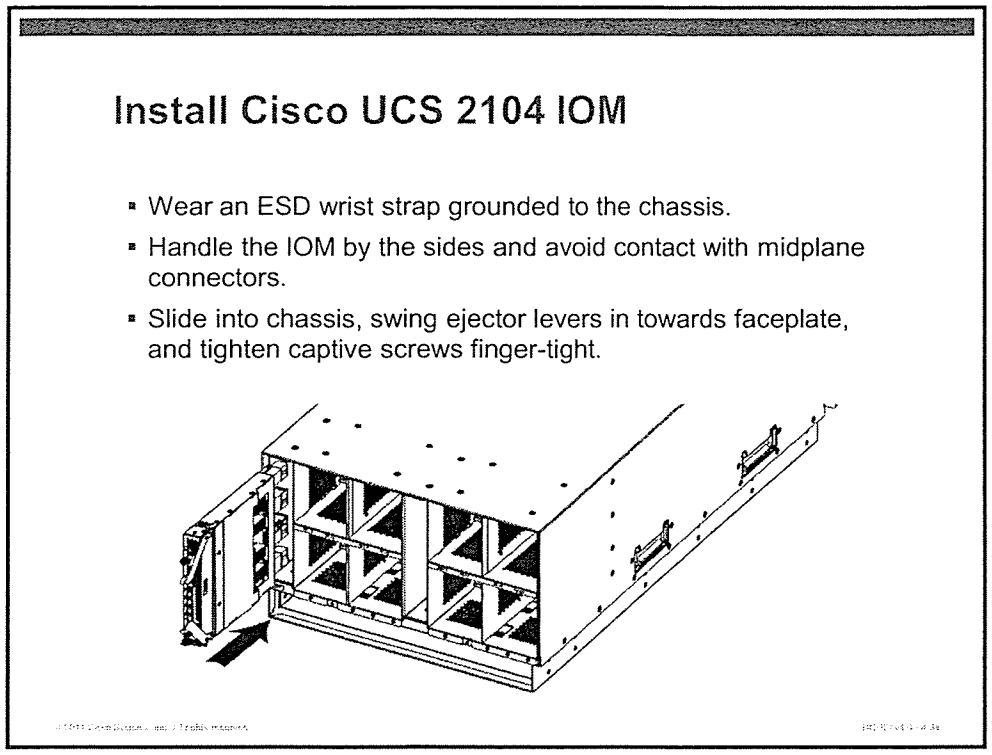
The LSI user guide can be found at the following link:

http://www.lsi.com/channel/products/raid_controllers/megaraid_8880em2/index.html

Physical Installation of I/O Modules and Power Supplies in the Cisco UCS 5108 Chassis

This topic discusses how to install I/O Modules (IOMs) and power supplies in the Cisco UCS 5108 chassis.

Install Cisco UCS 2104 IOM



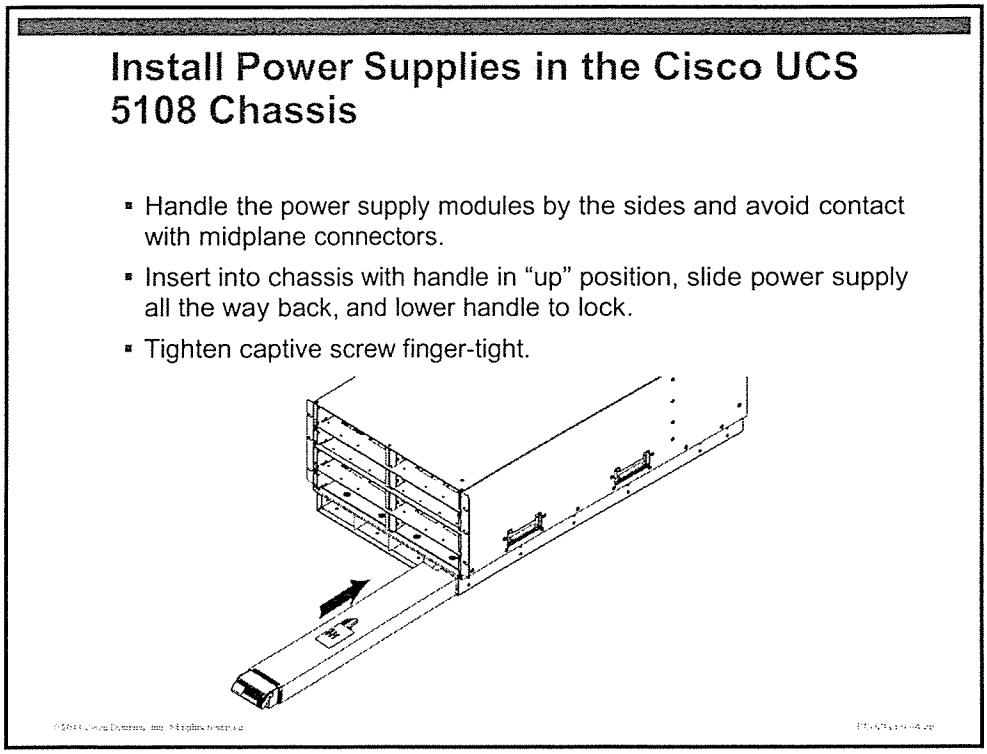
To install an IOM, follow these steps:

Step 1 Make sure that the two ejector levers at the front of the IOM are pulled fully open.

Step 2 Slide the fabric extender into the fabric extender slot, ensuring that the fabric extender is fully seated.

Step 3 Swing the ejection levers into the IOM faceplate and tighten the captive screw on each lever.

Install Power Supplies in the Cisco UCS 5108 Chassis



To install a power supply in the Cisco UCS 5108 chassis, follow these steps:

Step 1 Ensure that the handle orientation of the power supply is in the "up" position.

Step 2 Hold the power supply with both hands and slide it into the power supply bay.

Step 3 Press down the handle and give the power supply a gentle push inward. This ensures that the power supply is fully seated into the power distribution unit (PDU).

Step 4 Press the power supply handle down to lock the power supply in place.

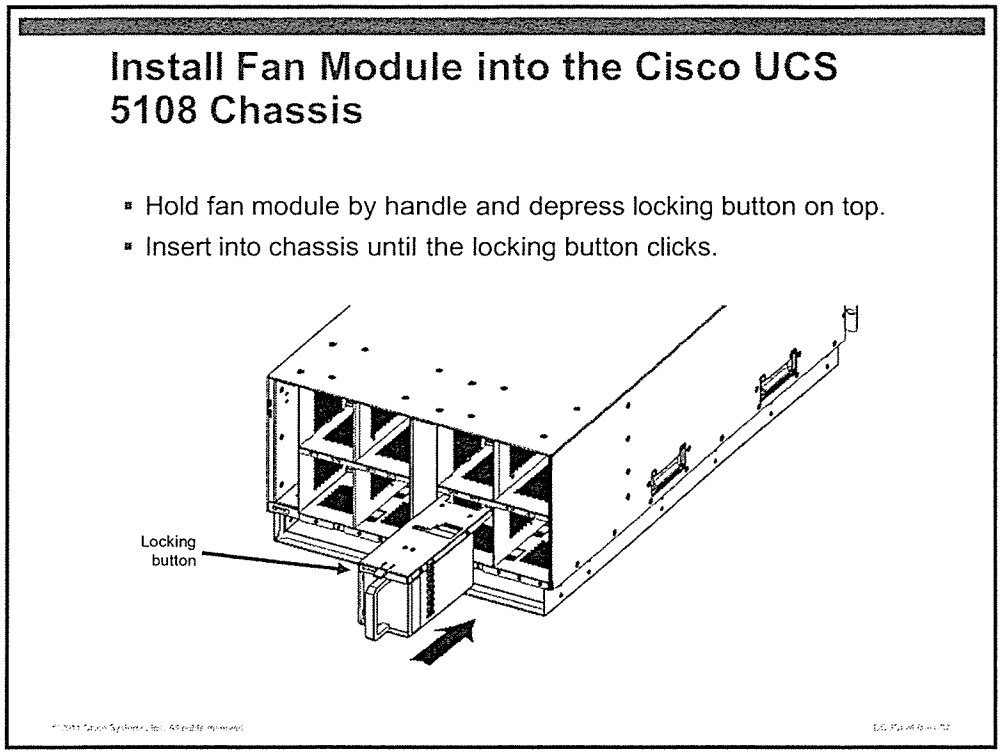
Step 5 Tighten the captive screw.

Step 6 Plug the power cable into the corresponding 220 VAC-inlet connector on the PDU at the rear of the chassis.

Installation and Removal of Fan Units

This topic discusses how to install and remove fan units.

Install Fan Module in the Cisco UCS 5108 Chassis



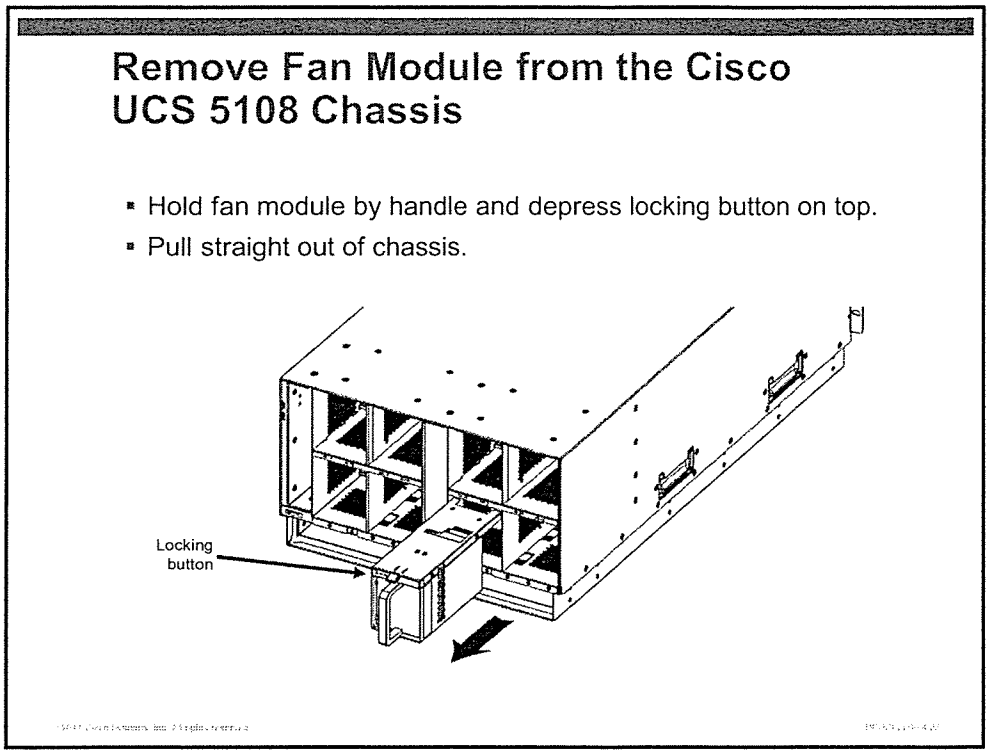
To install a fan assembly into the Cisco UCS 5108 chassis, follow these steps:

Step 1 Ensure that the handle orientation of the fan is in the "up" position with the spring latch at the top of the module.

Step 2 Push the fan module into the chassis until it seats properly and the spring latch snaps into place.

Step 3 Listen for the fan if the chassis is powered on. You should immediately hear it operating. If you do not hear it, ensure that the fan module is inserted completely in the chassis and the faceplate is flush with the outside surface of the chassis.

Remove Fan Module from the Cisco UCS 5108 Chassis



To remove a fan assembly from the Cisco UCS 5108 chassis, follow these steps:

Step 1 Depress the spring latch.

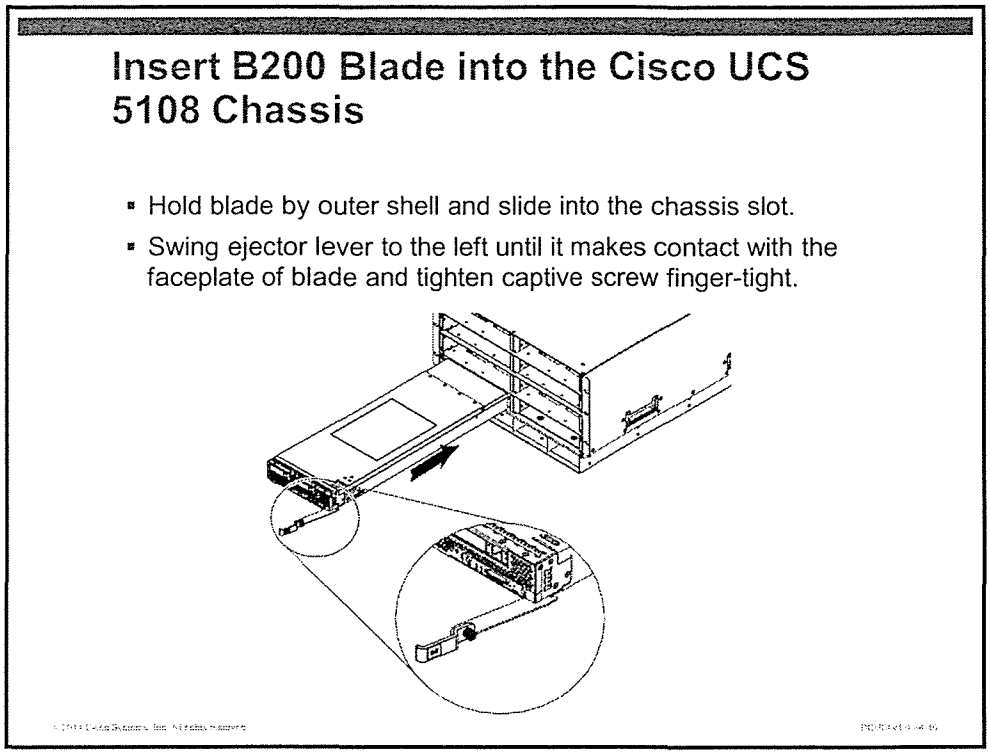
Step 2 Slide the fan module out of the chassis.

Note	Do not operate the Cisco UCS 5108 with more than one fan module removed because it can cause overheating.

Installation of B200, B230, B250, and B440 Blade Servers

This topic discusses how to install UCS B200, B230, B250, and B440 Blade Servers.

Insert B200 Blade into the Cisco UCS 5108 Chassis



To install a B200 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove blanking plate, if present.

Step 2 Wear an ESD strap that is grounded to the chassis.

Step 3 Open the ejector lever on the right front of the blade server.

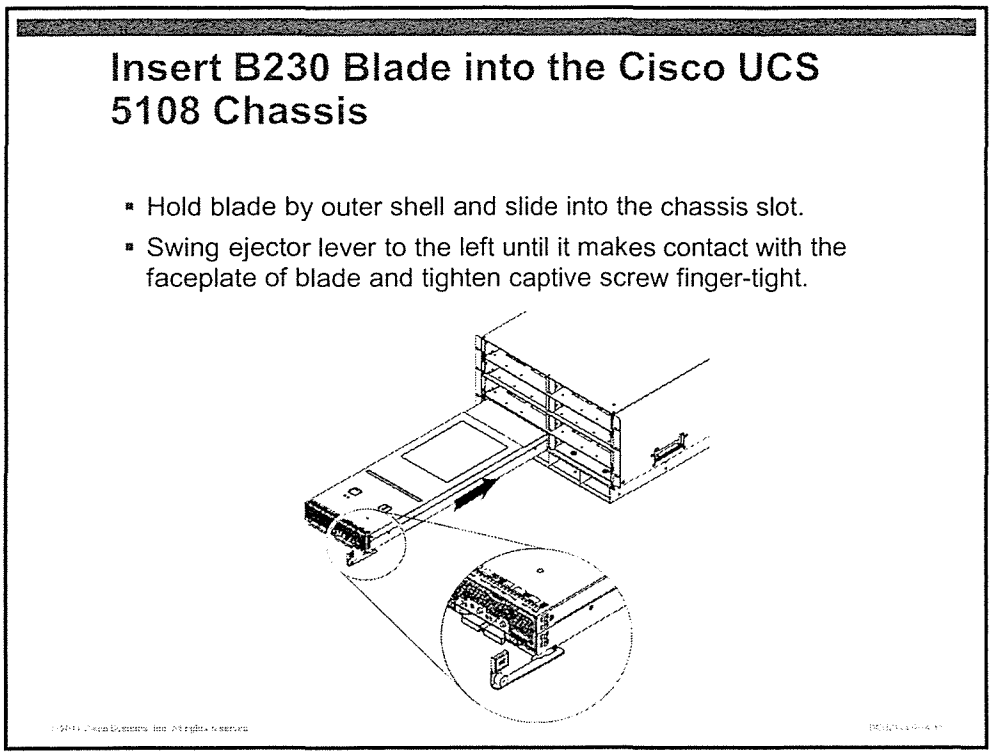
Step 4 Slide the blade into the opening until you cannot push it any farther.

Step 5 Swing the ejector lever towards the faceplate so that it engages the edge of the chassis and press the blade server all the way in.

Step 6 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

Note The blade installation procedure is the same for the B200 M1 and B200 M2.

Insert B230 Blade into the Cisco UCS 5108 Chassis



To install a B230 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove blanking plate, if present.

Step 2 Wear an ESD wrist strap that is grounded to the chassis.

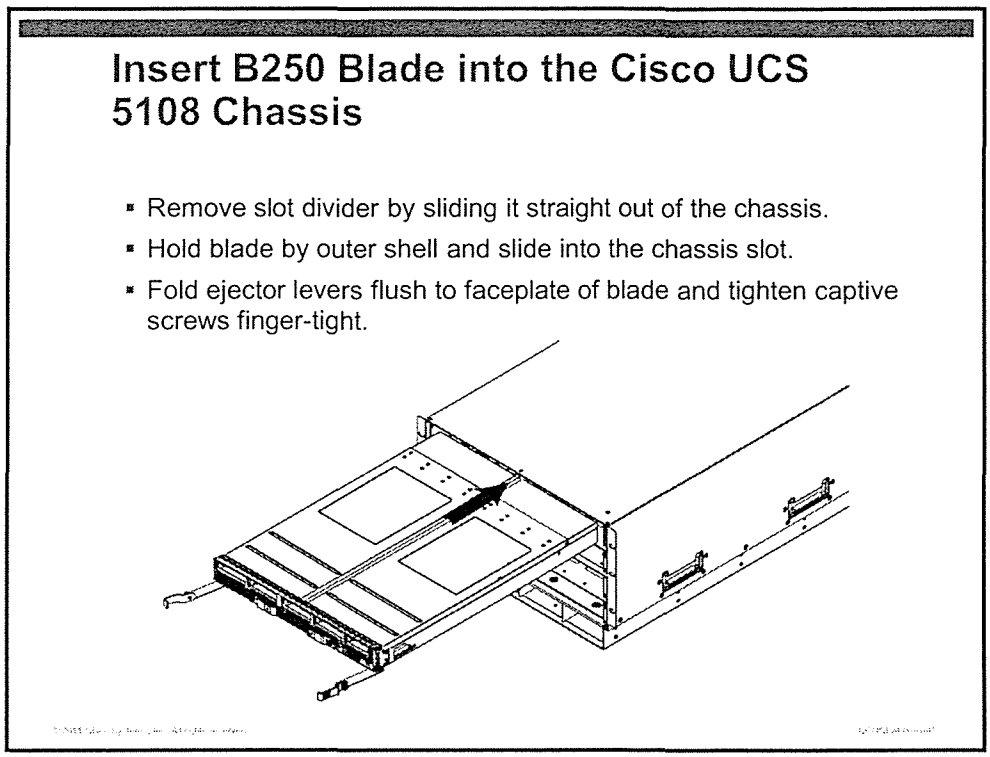
Step 3 Open the ejector lever on the right front of the blade server.

Step 4 Slide the blade into the opening until you cannot push it any farther.

Step 5 Swing the ejector lever towards the faceplate so that it engages the edge of the chassis and press the blade server all the way in.

Step 6 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

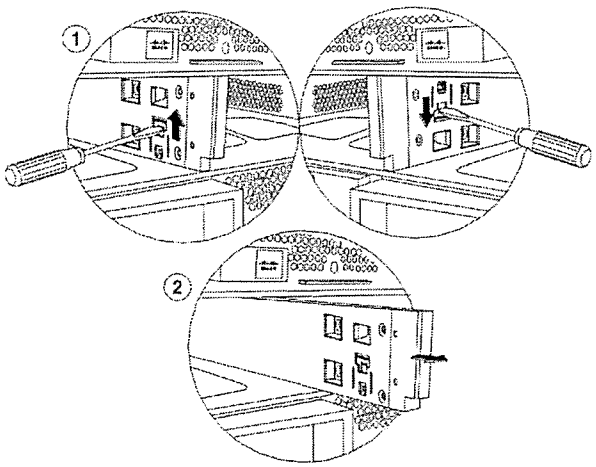
Insert B250 Blade into the Cisco UCS 5108 Chassis



To install a B250 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove blanking plates, if present.

Step 2 Remove slot divider, if present.



Step 3 Wear an ESD wrist strap that is grounded to the chassis.

Step 4 Open the ejector levers in the front of the blade server.

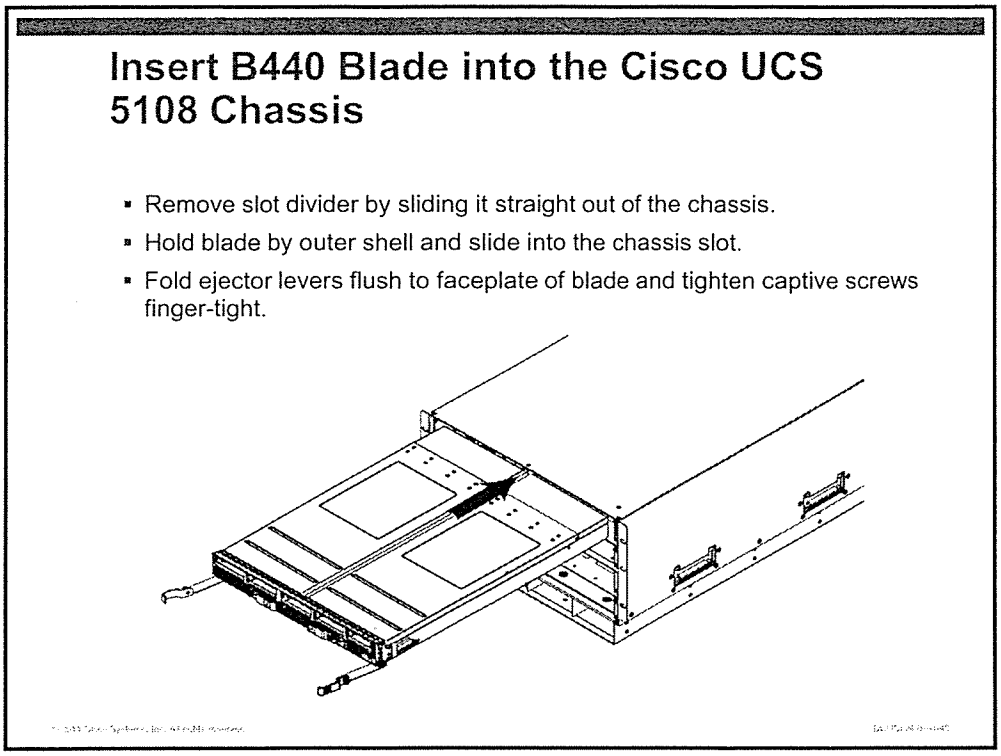
Step 5 Slide the blade into the opening until you cannot push it any farther.

Step 6 Swing the ejector levers towards the faceplate so that they engage the edge of the chassis and press the blade server all the way in.

Step 7 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

Note The blade installation procedure is the same for the B250 M1 and B250 M2.

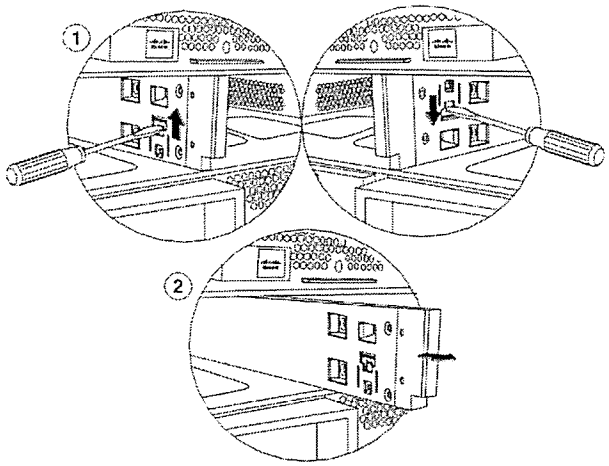
Insert B440 Blade into the Cisco UCS 5108 Chassis



To install a B440 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove blanking plates, if present.

Step 2 Remove slot divider, if present.



Step 3 Wear an ESD wrist strap that is grounded to the chassis.

Step 4 Open the ejector levers in the front of the blade server.

Step 5 Slide the blade into the opening until you cannot push it any farther.

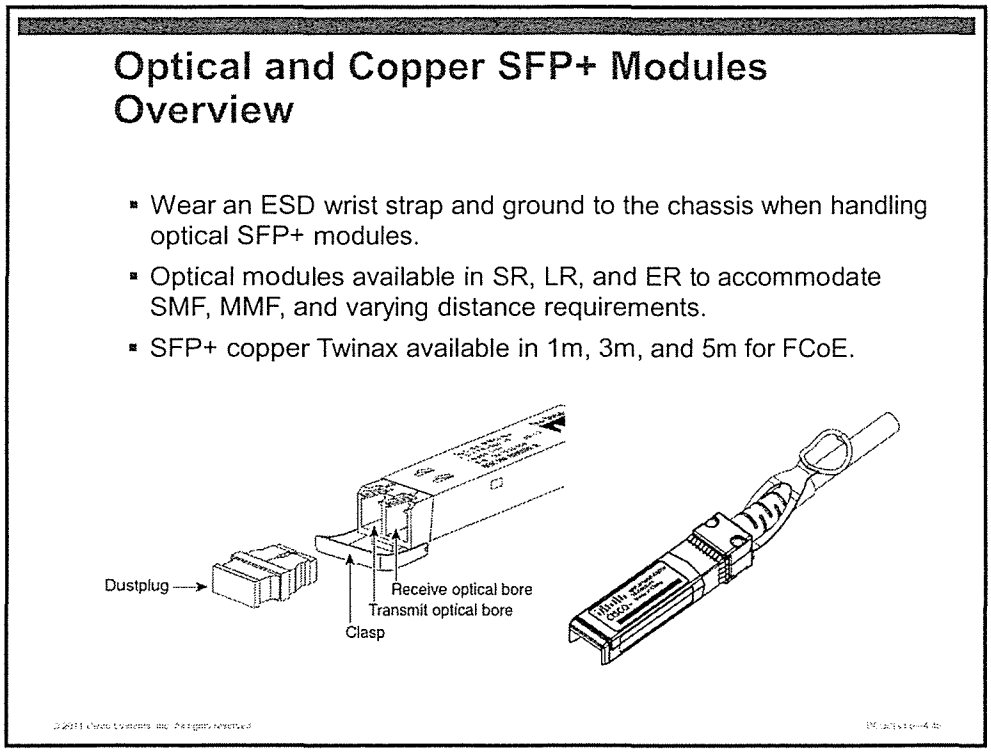
Step 6 Swing the ejector levers towards the faceplate so that they engage the edge of the chassis and press the blade server all the way in.

Step 7 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

Installation and Removal of SFP+ Copper Twinax and Optical Modules

This topic discusses how to install and remove SFP+ copper Twinax and optical modules.

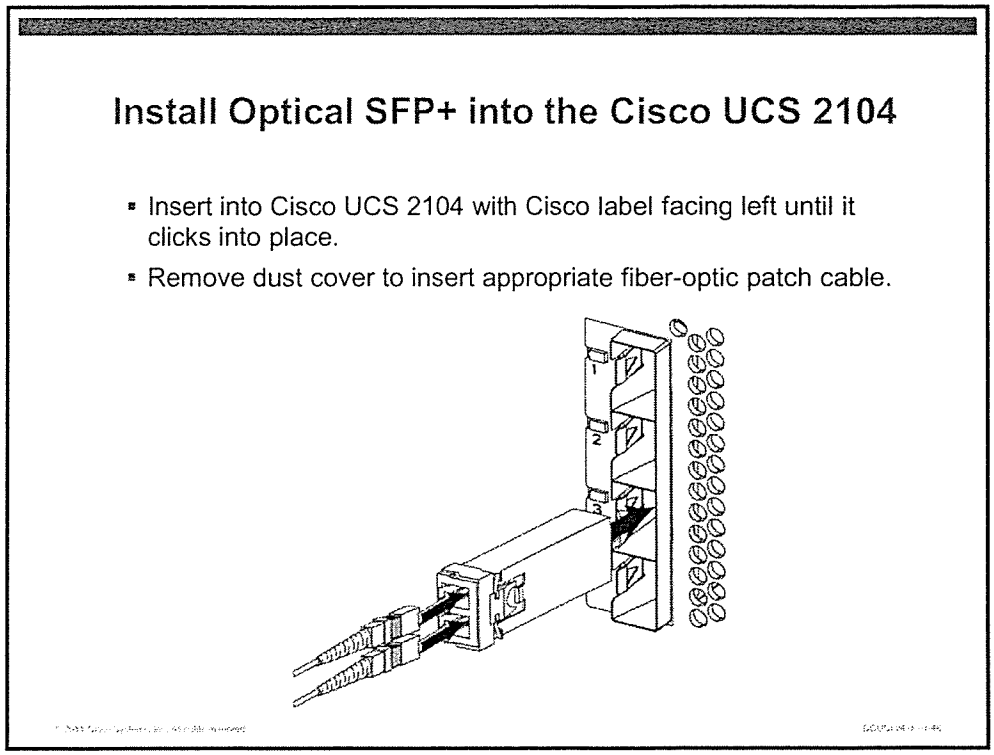
Optical and Copper SFP+ Modules Overview



Small form-factor pluggable plus (SFP+) modules are selected based on distance and media. 10-GE optical and copper SFP+ modules are available in the following types and lengths:

Part Number	SFP+ Transceiver Description
SFP-10G-SR	Cisco 10GBASE-SR SFP+ transceiver module for MMF, 850-nm wavelength
SFP-10G-LR	Cisco 10GBASE-LR SFP+ transceiver module for SMF, 1310-nm wavelength
SFP-10G-LRM	Cisco 10GBASE-LRM SFP+ transceiver module for MMF and SMF, 1310-nm wavelength
SFP-10G-ER	Cisco 10GBASE-ER SFP+ transceiver module for SMF, 1550-nm wavelength
SFP-H10GB-CU1M	Cisco 10GBASE-CU passive Twinax SFP+ cable assembly, 1 m
SFP-H10GB-CU3M	Cisco 10GBASE-CU passive Twinax SFP+ cable assembly, 3 m
SFP-H10GB-CU5M	Cisco 10GBASE-CU passive Twinax SFP+ cable assembly, 5 m
SFP-H10GB-ACU7M	Cisco 10GBASE-CU active Twinax SFP+ cable assembly, 7m
SFP-H10GB-ACU10M	Cisco 10GBASE-CU active Twinax SFP+ cable assembly, 10 m

Install Optical SFP+ into the Cisco UCS 2104 Fabric Extender



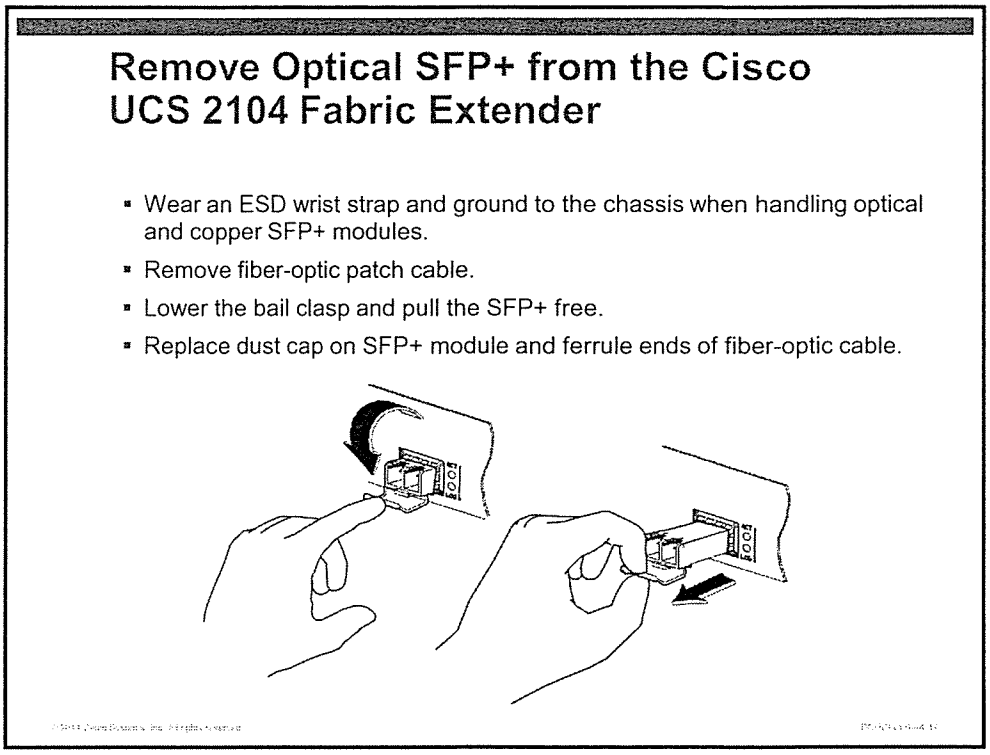
Wear an ESD wrist strap that is grounded to the chassis that you are working on whenever handling optical SFP+ modules. Follow these steps to install an optical SFP+ module in the Cisco UCS 2104:

Step 1 Slide the optical SFP+ module into the slot in the Cisco UCS 2104 or fabric interconnect until it clicks in place.

1. Remove the dust cap from the SFP+ module and the dust caps from the fiber-optic cable ferrules.

Note Store dust caps in a clean, sealable plastic bag or plastic parts box. You will need them in the future if you need to remove the fiber-optic cable from Cisco UCS components.

Remove Optical SFP+ from the UCS 2104 Fabric Extender



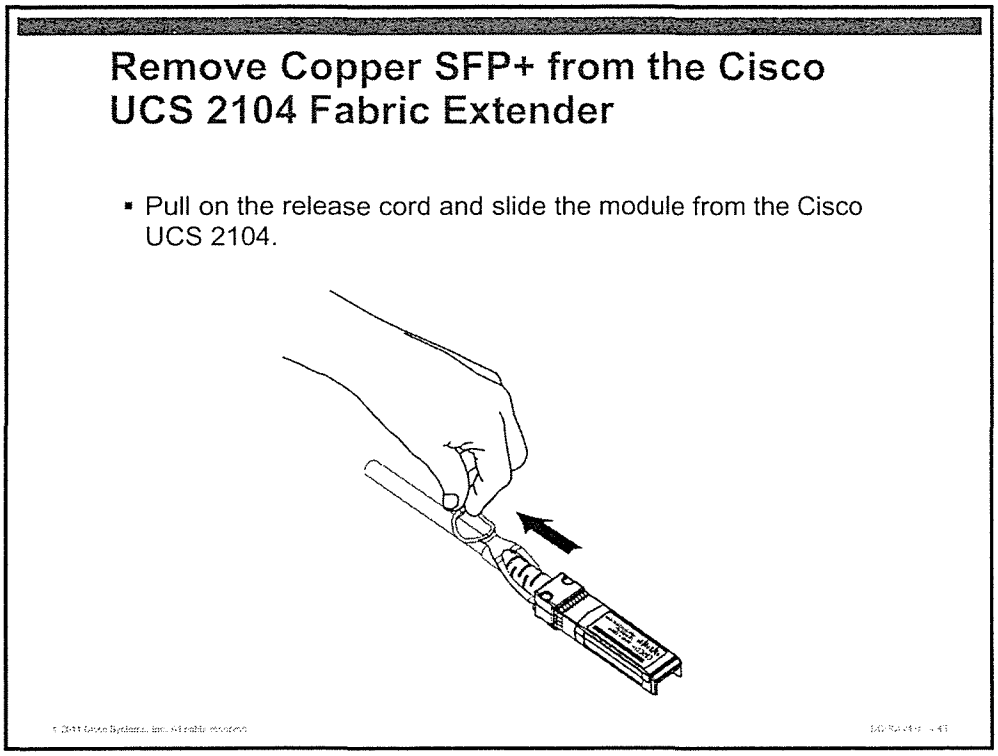
Wear an ESD wrist strap that is grounded to the chassis you are working on whenever handling optical SFP+ modules. Follow these steps to remove an optical SFP+ module:

Step 1 Remove the fiber-optic cable and place clean dust caps over the ferrules. Slide down the bail handle to release the module from the component.

Step 2 Close the bail clasp and insert a clean dust cap.

Step 3 Store optical SFP+ modules in static-shielded containment.

Remove Copper SFP+ from the Cisco UCS 2104 Fabric Extender



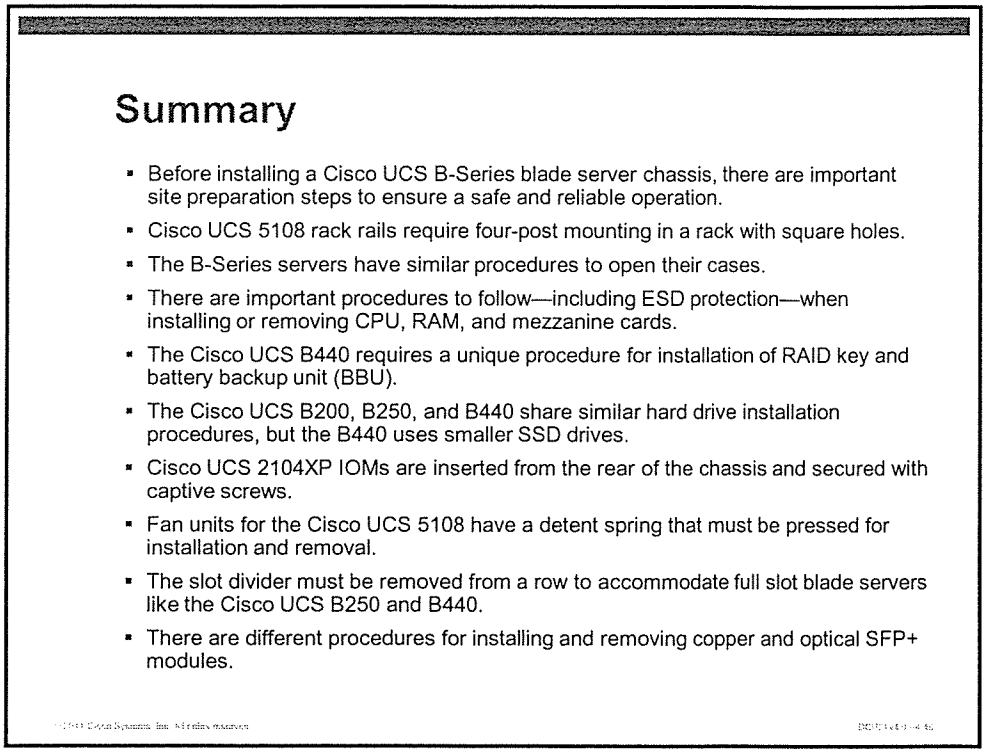
Wear an ESD wrist strap that is grounded to the chassis you are working on whenever handling optical SFP+ modules. Follow these steps to remove a copper Twinax SFP+ module:

Step 1 Grasp the looped cable and gently pull back. The module can then be slid out of the component.

Step 2 Store copper Twinax SFP+ cables in static-shielded containment.

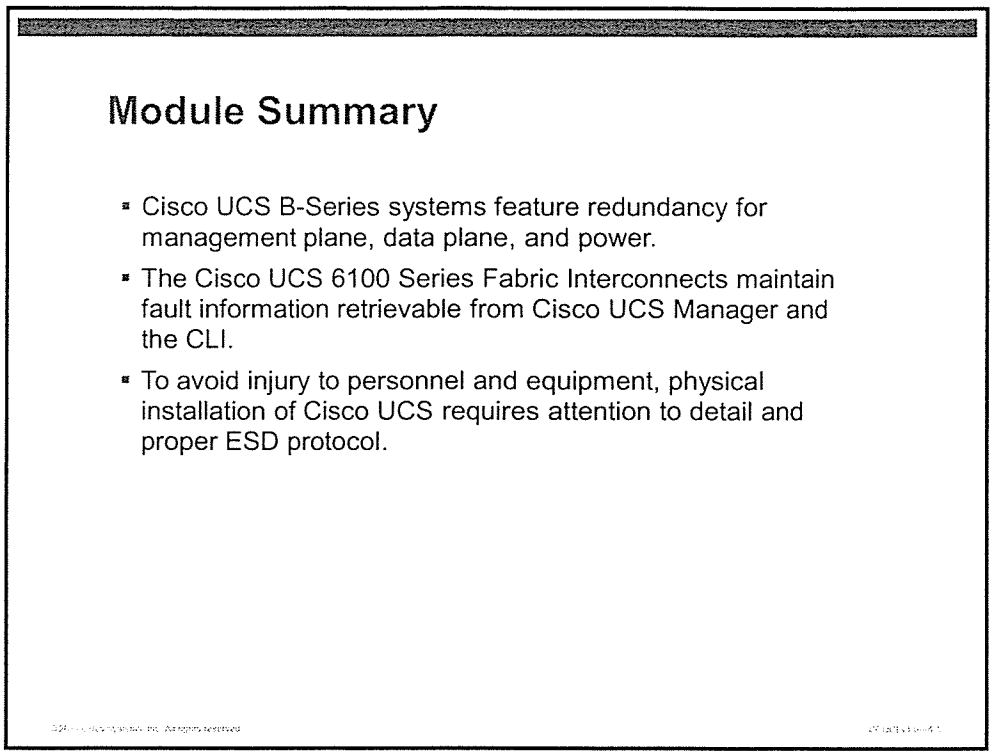
Summary

This summarizes key points from the lesson.



Module Summary

This topic summarizes the key points that were discussed in this module.



This module examines a broad range of installation and operational guidelines necessary to implement Cisco UCS B-Series server chassis and components. High availability, fault detection, and safety are the main themes.

To ensure continuous operation, the Cisco UCS 6100 Series Fabric Interconnects can be clustered to provide redundancy for management and data planes. Combined with redundant 10-GE links to the I/O modules (IOMs) in the UCS 5108 server chassis, single points of failure are eliminated.

As an implementation proceeds from power-up, knowledge of the fault reporting system provides valuable troubleshooting data. This data includes the status of hardware components and connectivity between Cisco UCS and other UCS elements. After a system is handed off to operations personnel, the fault system allows Simple Network Management Protocol (SNMP) traps to be sent to the network management system. This system provides alerts to component or connectivity failures. To meet organizational and regulatory compliance requirements, fault data and events can be archived to remote syslog servers.

An empty Cisco UCS 5108 server chassis weighs 90 lb (40.91 kg). It is vital for the safety of installers and the equipment that proper installation procedures are observed. At least two persons are required to mount the Cisco UCS 5108 server chassis into a rack.

Nearly every field-installable component can be damaged or rendered nonfunctional by ESD. It is highly recommended to have an ESD-safe staging area for any work that requires working inside a B-Series blade server. A grounded wrist strap must be worn at all times when handling CPUs, mezzanine cards, DIMMs, IOMs, generic expansion module (GEM) expansion modules, and small form-factor pluggable plus (SFP+) transceivers.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1) – Managing Port Licenses*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1_chapter13.html

- Cisco Systems, Inc. *Cisco UCS 5108 Server Chassis Installation Overview – Power Redundancy*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/overview.html

- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1) – Configuring Settings for Faults, Events, and Logs*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1_chapter42.html

- Cisco Systems, Inc. *Cisco UCS 5108 Server Chassis Installation Guide – Installing the Cisco UCS 5108 Server Chassis*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/install.html

- Cisco Systems, Inc. *Cisco UCS B200 Blade Server Installation and Service Note*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/blade.html

- Cisco Systems, Inc. *Cisco UCS B250 Extended Memory Blade Server Installation and Service Note*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/fullblade.html

- Cisco Systems, Inc. *Cisco UCS B440 High Performance Blade Server Installation and Service Note*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/quadblade.html

- Cisco Systems, Inc. *Cisco ESD Training Program*

  http://www.cisco.com/web/learning/le31/esd/WelcomeP.html

- Cisco Systems, Inc. *Cisco SFP and SFP+ Transceiver Module Installation Notes*

  http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/installation/note/78_15160.html

- Cisco Systems, Inc. *Cisco 10GBASE SFP+ Modules*

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/data_sheet_c78-455693.html

- Mirapath, Inc. *Server Lift SL-500*

  http://www.mirapath.com/rack-accessories/server-lift.html

- 3M, Inc. *3M ESD Field Service Kits*

  http://solutions.3m.com/wps/portal/3M/en_US/electronics/home/productsandservices/products/StaticControlSolutions/Products/?PC_7_RJH9U5230O8A602BK7QOMA20D0_nid=L8LLK91HNXbeZJNMXBKD0Wgl

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) Which two choices are valid for the number of fixed ports with licensing from the factory? (Choose two.) (Source: "Describing Cisco UCS B-Series Hardware Components")

A) ports 1–4 on the Cisco UCS 6120 Fabric Interconnect
B) ports 1–6 on the Cisco UCS 6140 Fabric Interconnect
C) ports 1–8 on the Cisco UCS 6120 Fabric Interconnect
D) ports 1–8 on the Cisco UCS 6130 Fabric Interconnect
E) ports 1–12 on the Cisco UCS 6140 Fabric Interconnect
F) ports 1–16 on the Cisco UCS 6140 Fabric Interconnect

Q2) From where can you copy a port license file? (Source: "Describing Cisco UCS B-Series Hardware Components")

A) from Cisco UCS Manager GUI only
B) from Cisco UCS Manager CLI in NX-OS shell only
C) EFI shell install using USB flash
D) from Cisco UCS Manager CLI in local-management shell only
E) from Cisco UCS Manager GUI or CLI in NX-OS shell only
F) from Cisco UCS Manager GUI or CLI in local-management shell only

Q3) Which three choices are valid power redundancy modes? (Choose three.) (Source: "Describing Cisco UCS B-Series Hardware Components")

A) redundant
B) nonredundant
C) hot spare
D) n+1
E) grid
F) n+2

Q4) Which statement is true about Cisco UCS power policy? (Source: "Describing Cisco UCS B-Series Hardware Components")

A) Power policy is configured on a per-chassis basis to accommodate flexible power redundancy options.
B) Power policy is global and must be configured on a chassis-by-chassis basis.
C) Chassis power policy can only be set in the chassis service profile.
D) Chassis power policy is configured globally and all chassis inherit the redundancy policy.

Q5) Which two statements are true about management and data plane redundancy? (Choose two.) (Source: "Describing Cisco UCS B-Series Hardware Components")

A) Management and data plane redundancy is achieved by redundant traces on the midplane.
B) Management and data plane redundancy requires at least one fabric interconnect and one I/O module.
C) Management and data plane redundancy is achieved by redundant traces on the Cisco UCS fabric interconnect.
D) Management and data plane redundancy is achieved by redundant traces on the I/O module.
E) Management and data plane redundancy requires at least two fabric interconnects and two I/O modules.

Q6) Which two statements are true about fabric interconnect clusters? (Choose two.) (Source: "Assembling B-Series Architecture and Features")

A) Up to four fabric interconnects can be clustered for data and management plane redundancy.
B) Two fabric interconnects are required to form a cluster and provide data and management plane redundancy.
C) Mixed models of fabric interconnects are permitted with the Advance Cluster License.
D) Feature licenses must match on both of the fabric interconnects.

Q7) Which statement is true about cluster topology validation? (Source: "Assembling B-Series Architecture and Features")

A) Cluster topology is validated by physical connections alone.
B) Cluster topology is validated by a Call Home connection to Cisco TAC.
C) Cluster topology is validated by syslog messages that are exchanged during chassis discovery.
D) Cluster topology is validated by the IOM during chassis discovery.
E) Cluster topology is validated by messages that are exchanged during chassis discovery.

Q8) Which three statements are true about cluster IP addressing? (Choose three.) (Source: "Assembling B-Series Architecture and Features")

A) The cluster virtual IP cannot be changed without erasing the configuration database and running setup.
B) The IP addresses of both fabric interconnects can be changed in the Cisco UCS Manager GUI.
C) The cluster virtual IP can be changed only in the Cisco UCS CLI.
D) The IP addresses of both fabric interconnects can be changed in the Cisco UCS Manager CLI.

Q9) Which statement is true about fault policy? (Source: "Assembling B-Series Architecture and Features")

A) Even if you set the cleared fault policy with a retention period of forever, the fault will be deleted if you acknowledge it.
B) Fault policy is disabled by default.
C) Fault policy must be configured on a fabric interconnect-by-fabric interconnect basis.

Q10) Which statement is true about syslog support? (Source: "Assembling B-Series Architecture and Features")

A) You can configure one syslog server destination.
B) You can configure two syslog server destinations.
C) You can configure three syslog server destinations.
D) You can configure four syslog server destinations.
E) You can configure unlimited syslog server destinations.

Q11) What is the voltage threshold at which you can feel a static shock? (Source: "Installing Cisco UCS B-Series Hardware")

A) 10 V
B) 30 V
C) 100 V
D) 300 V
E) 3000 V
F) 10000 V

Q12) Which two of these statements are true about rack-mounting a Cisco UCS 5108 chassis? (Choose two.) (Source: "Installing Cisco UCS B-Series Hardware")

A) It requires a two-post rack with square holes.
B) It requires a four-post rack with square holes.
C) Two persons are required to lift the chassis into the rails.
D) It requires a two-post rack with round holes.
E) It requires a four-post rack with round holes.
F) Two persons are required to lift the chassis into the rails with side handles.

Q13) Which two statements are true regarding Cisco UCS 5108 airflow considerations? (Choose two.) (Source: "Installing Cisco UCS B-Series Hardware")

A) Airflow is front-to-back.
B) The fan exhaust must be unobstructed for 12 in (30.5 cm).
C) Air flow is side-to-side.
D) The fan exhaust must be unobstructed for 24 in (61 cm).
E) Cool air must be sourced from the raised floor plenum.

Q14) Which two statements are correct about the differences between the B200 M1 and B200 M2? (Choose two.) (Source: "Installing Cisco UCS B-Series Hardware")

A) The B200 M1 uses plastic baffles to direct air over DIMM modules.
B) The B200 M2 uses aluminum baffles to improve air over DIMM modules.
C) The B200 M2 requires Intel Xeon 5600 Series CPUs.
D) The B200 M2 uses plastic baffles to direct air over DIMM modules.
E) The B200 M1 requires Intel Xeon 5600 Series CPUs.

Q15) Which statement is correct about installing a power supply in the Cisco UCS 5108 chassis? (Source: "Installing Cisco UCS B-Series Hardware")

A) Slide the power supply into the slot and swing both ejector arms towards the faceplate and hand-tighten the two captive screws.
B) Slide the power supply into the chassis with the handle up and push the handle down to complete the connection.
C) Slide the power supply into the slot and swing the right ejector arm towards the faceplate and hand-tighten the captive screw.
D) Slide the power supply into the slot and swing the right ejector arm towards the faceplate and hand-tighten the captive screw.
E) Slide the power supply into the chassis with the handle down and push the handle up to complete the connection.

Module Self-Check Answer Key

Q1) C, F

Q2) D

Q3) B, D, E

Q4) D

Q5) A, E

Q6) B, D

Q7) E

Q8) B, C, D

Q9) A

Q10) C

Q11) C

Q12) B, C

Q13) A, D

Q14) C, D

Q15) B

Module 5

Cisco UCS Connectivity Configuration and Management

Overview

After all of the components of the Cisco Unified Computing System (UCS) are racked, assembled, and powered on, component physical and logical configuration is the next step towards making the system available for operation. When the physical links are in place from the Cisco UCS server chassis to the fabric interconnect, you will understand the addressing and policy requirements and options available for LAN and SAN connectivity to the blade servers.

Module Objectives

Upon completing this module, you will be able to articulate the requirements to make proper physical interconnections. You will also be able to identify and select the correct context in the Cisco UCS Manager interfaces to configure, troubleshoot, and monitor your Cisco UCS deployment.

This ability includes being able to meet these objectives:

- Configure Cisco UCS B-Series physical connectivity
- Explore the UCS B-Series user interfaces
- Configure compute node LAN connectivity
- Distinguish compute node SAN connectivity

Lesson 1

Configuring Cisco UCS B-Series Physical Connectivity

Overview

To understand Cisco UCS design, you need to understand the components that are used for LAN, SAN, and management access in the path from the fabric interconnect down to the B-Series blade servers. This lesson will describe the components of Cisco UCS B-Series physical connectivity.

Objectives

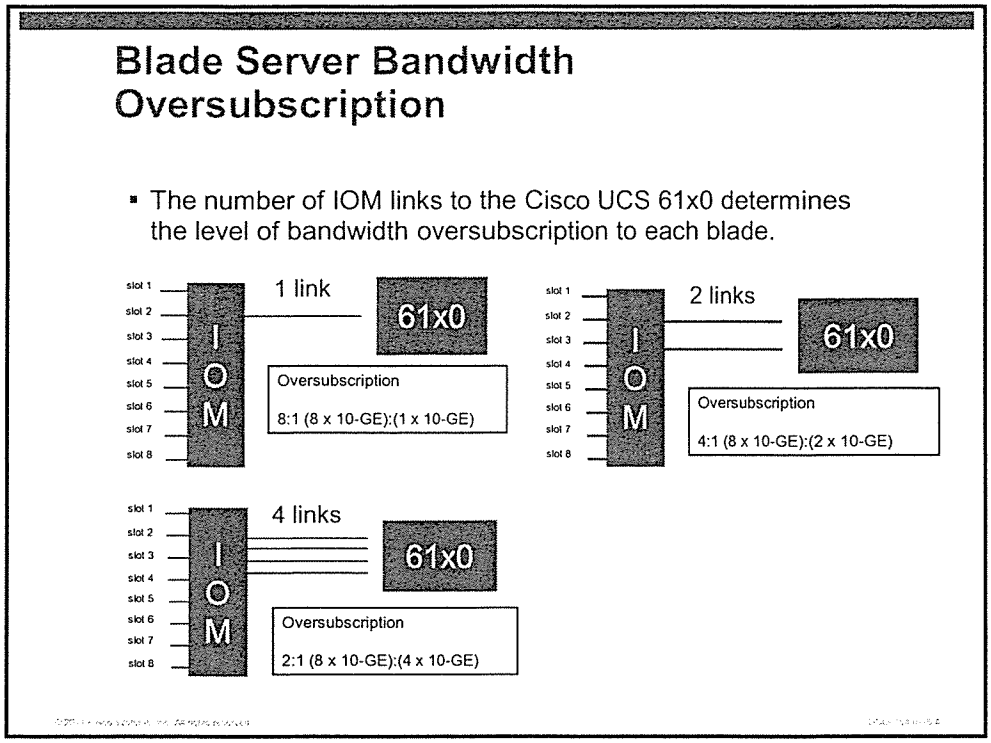
Upon completing this lesson, you will be able to define physical management and data plane paths from the fabric interconnect through the I/O module and over the traces of the Cisco UCS 5108 server chassis midplane. This ability includes being able to meet these objectives:

- Describe the relationship between I/O uplinks and bandwidth oversubscription
- Describe I/O module architecture, including CMC, I/O MUX, and CMS
- Describe the Cisco IMC management component of the B-Series blades
- Describe the discovery process and how to monitor using finite state machine output

I/O Uplinks and Bandwidth Oversubscription

This topic discusses how link policy relates to bandwidth oversubscription and the number of chassis in a Cisco UCS system.

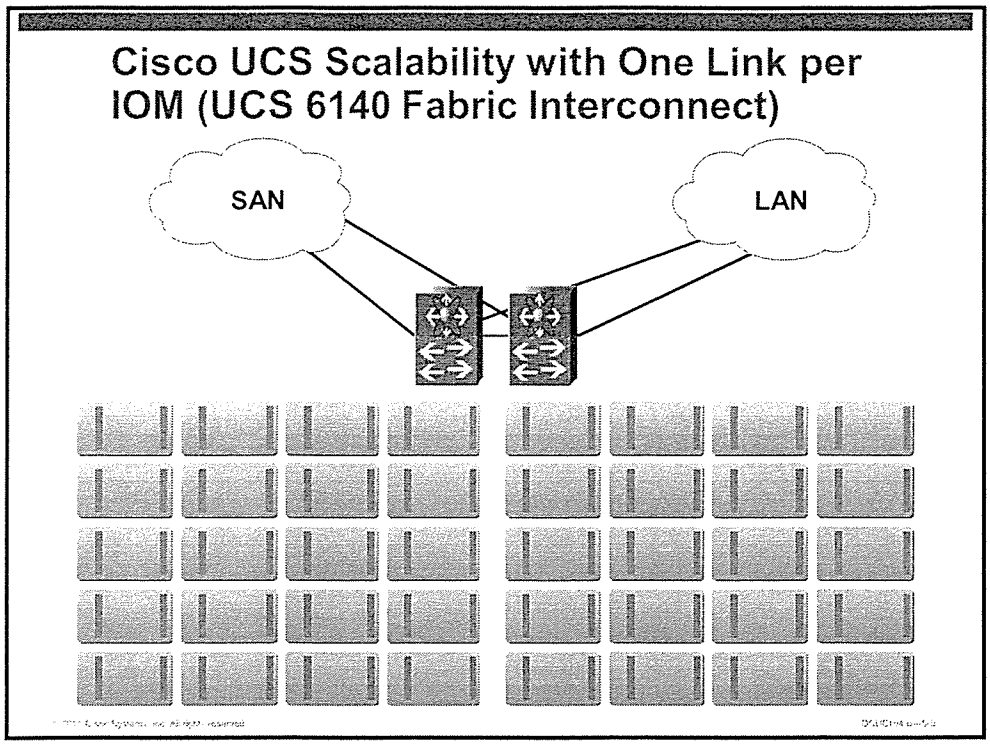
Blade Server Bandwidth Oversubscription



Each Cisco UCS 5108 server chassis supports two I/O modules (IOMs). Each IOM supports one, two, or four 10-Gigabit Ethernet links to each fabric interconnect in the cluster. One IOM connects to fabric A and one to fabric B.

With a four-link configuration, there is 40-Gb/s available bandwidth on each IOM. Although the data plane is active on both fabrics, they are designed to operate in active-standby mode. With eight blade servers in a chassis and four links from the IOM, the effective oversubscription rate is 2:1. With two links, the oversubscription rate is 4:1, and with one link per IOM, the rate is 8:1.

Cisco UCS Scalability with One Link per IOM (6140 Fabric Interconnect)



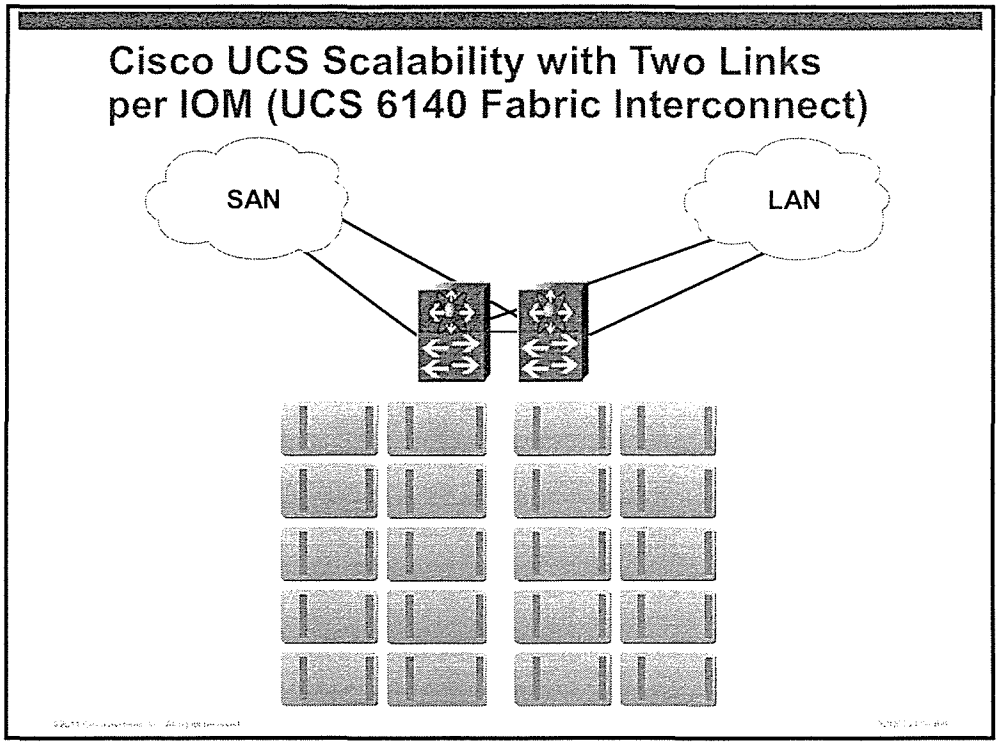
The number of links from the IOM to the fabric interconnect also determines how many chassis can constitute a given Cisco UCS system. Each fabric interconnect has a finite number of 10-Gigabit Ethernet ports available for connections to IOMs.

This design allows for the maximum number of chassis, but has the highest oversubscription rate of 8:1.

Fabric Interconnect Model	Maximum Chassis with 1 Link Per IOM
6120	20*
6140	40*

*The maximum number of chassis that are supported by a fabric interconnect is determined by the version of Cisco UCS Manager.

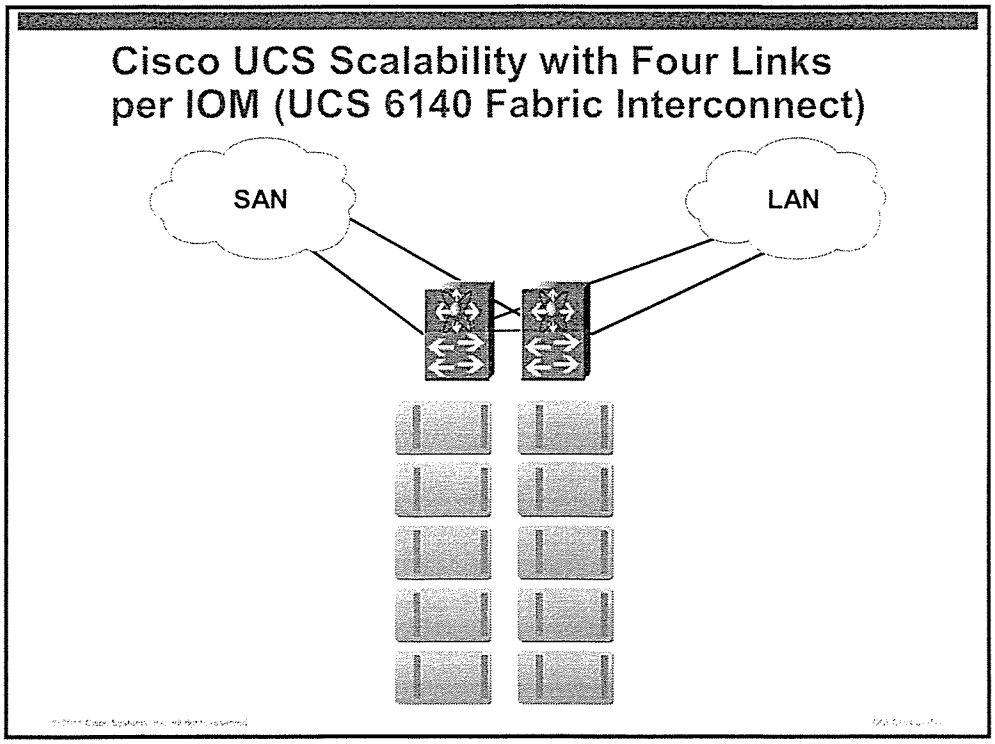
Cisco UCS Scalability with Two Links per IOM (6140 Fabric Interconnect)



In Cisco UCS systems with two links per IOM, you achieve a good balance of scalability and bandwidth. This design allows for half the number of chassis, but lowers the oversubscription rate of 4:1.

Fabric Interconnect Model	Maximum Chassis with 2 Links Per IOM
6120	10
6140	20

Cisco UCS Scalability with Four Links per IOM (UCS 6140 Fabric Interconnect)

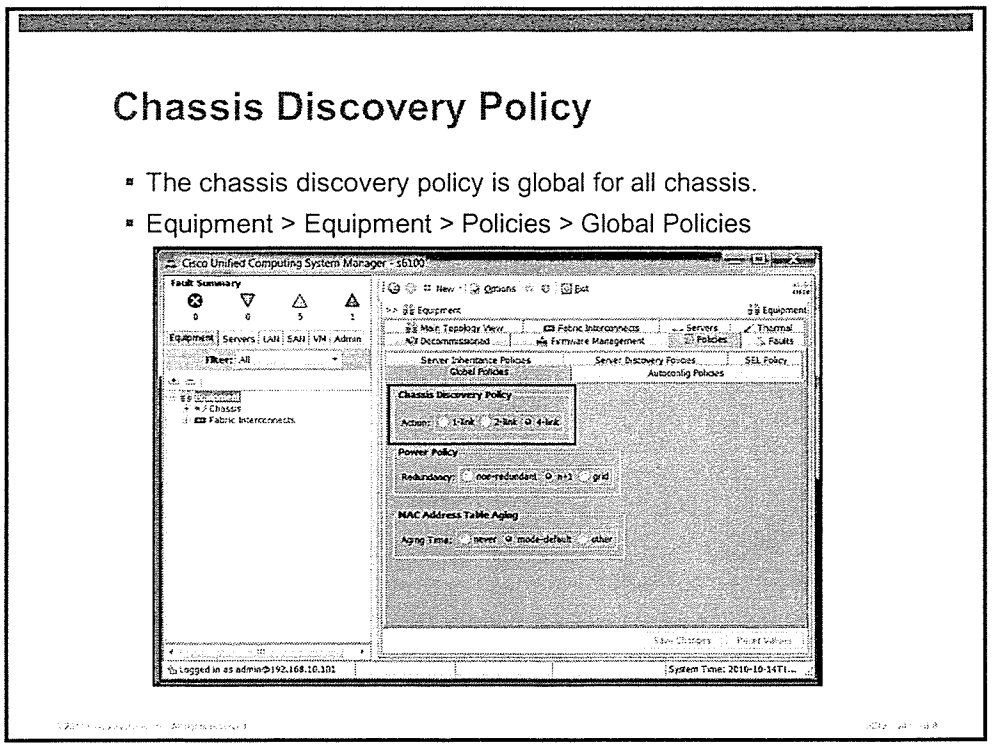


In Cisco UCS systems with four links per IOM, the oversubscription rate drops to 2:1, but the least number of chassis can be connected. The Cisco UCS designer will make the decision of how many links to employ based on application bandwidth requirements.

Fabric Interconnect Model	Maximum Chassis with 4 Links Per IOM
6120	5
6140	10

Note As of Cisco UCS Manager version 1.3, the maximum number of chassis is 14.

Chassis Discovery Policy



The chassis discovery policy is a global policy for all chassis that are connected to the fabric interconnects. It sets the *minimum* number of IOM links required for chassis discovery.

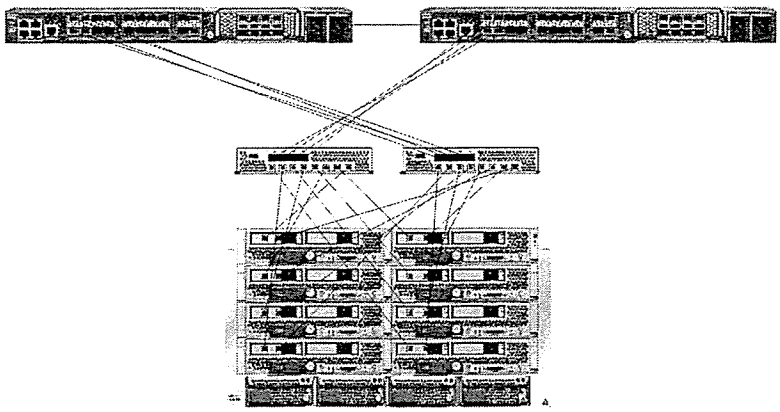
The policy is flexible to allow either a uniform number of links or a mixed number of links per chassis. The recommended configuration is to set the chassis discovery policy to the lowest number of IOM links allowed on any chassis.

As an example, if you set the policy to one link, a chassis with four links would initially be discovered as a one-link chassis. After you reacknowledge that chassis, the remaining three links would be recognized and become available to service blade servers.

Number of Actual Links	1-Link Policy	2-Link Policy	4-Link Policy
1 Link to IOM	Chassis discovered as a 1-link topology	Chassis will not be discovered	Chassis will not be discovered
2 Links to IOM	Chassis discovered initially as a 1-link topology. After chassis reacknowledge, two links active	Chassis discovered as a 2-link topology	Chassis will not be discovered.
4 Links to IOM	Chassis discovered initially as a 1-link topology. After chassis reacknowledge, 4 links active	Chassis discovered initially as a 2-link topology. After chassis reacknowledge, 4 links active	Chassis discovered as a 4-link topology

Chassis Physical Connections

Equipment > Chassis 1 > Hybrid Display

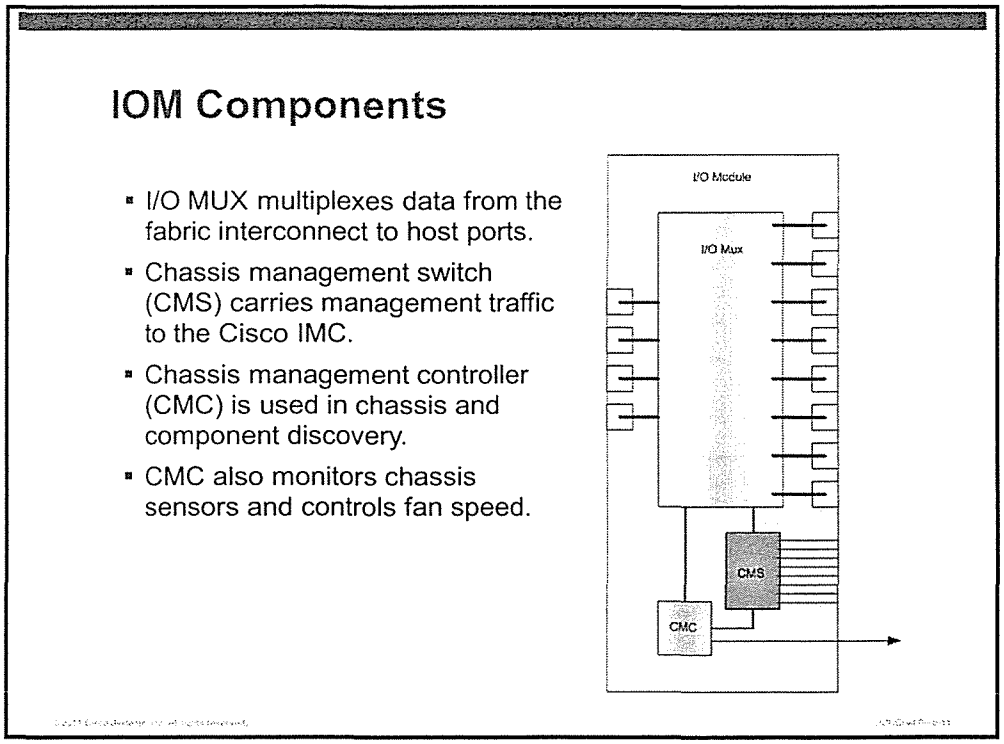


Use UCS Manager hybrid view from each chassis to validate the physical connections from the server host through the IOMs to the fabric interconnects. The eight connections from the servers to each IOM are made across the chassis midplane and internal. The four connections from each IOM to the fabric interconnects represent external, physical links.

IOM Architecture, Including CMC, I/O MUX, and CMS

This topic introduces the internal structure of the IOM.

IOM Components



The IOM is often referred to as a fabric extender (FEX). It acts as a virtual line card to the Cisco UCS 6100 Series Fabric Interconnects. Because it multiplexes eight 10-Gigabit Ethernet host ports over one, two, or four 10-Gigabit Ethernet links to the fabric interconnect, comparisons can be drawn to the Cisco Nexus 2000 Series fabric extenders that connect hosts to the Nexus 5000 switch.

The IOM has more functionality than simply fabric extension, however. In addition to the I/O MUX, there are two other important components: the chassis management controller (CMC) and the chassis management switch (CMS).

The CMC is responsible for these primary functions:

- It controls and monitors the chassis fan speed.
- It monitors and logs ingress and egress temperature sensors.
- It controls chassis fault identification.
- It monitors voltages and current within the chassis and can change the power state of power supplies, based on demand.
- It detects presence, insertion, and removal of Cisco UCS blades.
- It reads the IDs of the chassis, Cisco UCS blades, and IOMs.

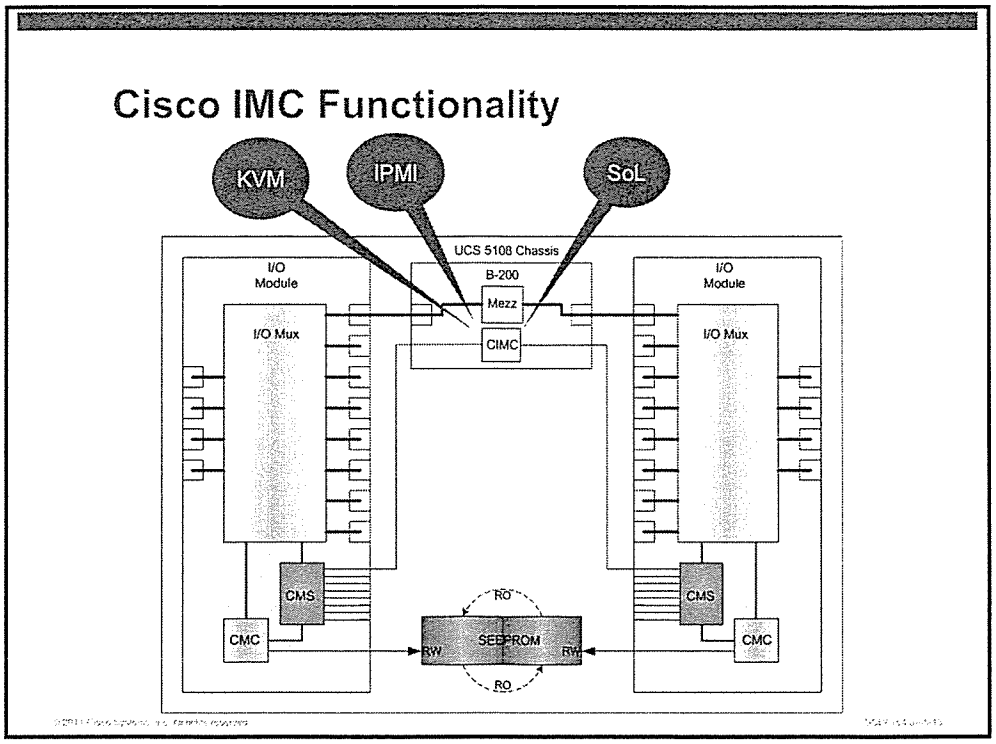
The CMS provides a 100-Mb dedicated connection to the baseboard Cisco Integrated Management Controller (IMC) in each server. It is by this link that keyboard, video, and mouse (KVM) over IP, Serial over LAN (SoL), and Intelligent Platform Management Interface (IPMI) data travels to the I/O MUX to Cisco UCS Manager and external management connections.

There are redundant traces across the midplane for management and data plane communications.

Cisco IMC Management Component of the B-Series Blades

This topic discusses the functionality of the Cisco IMC and how it is used for remote management and monitoring.

Cisco IMC Functionality



The Cisco IMC is a chip on the motherboard of each blade server. The Cisco IMC provides for thermal, power, and general health monitoring of the blade. This data is polled by the CMC and relayed to Cisco UCS Manager.

The Cisco IMC also enables KVM over IP, SoL, and an IPMI 2.0-compliant interface.

KVM over IP allows Cisco UCS administrators to connect remotely to the console of any server in the Cisco UCS system with KVM control.

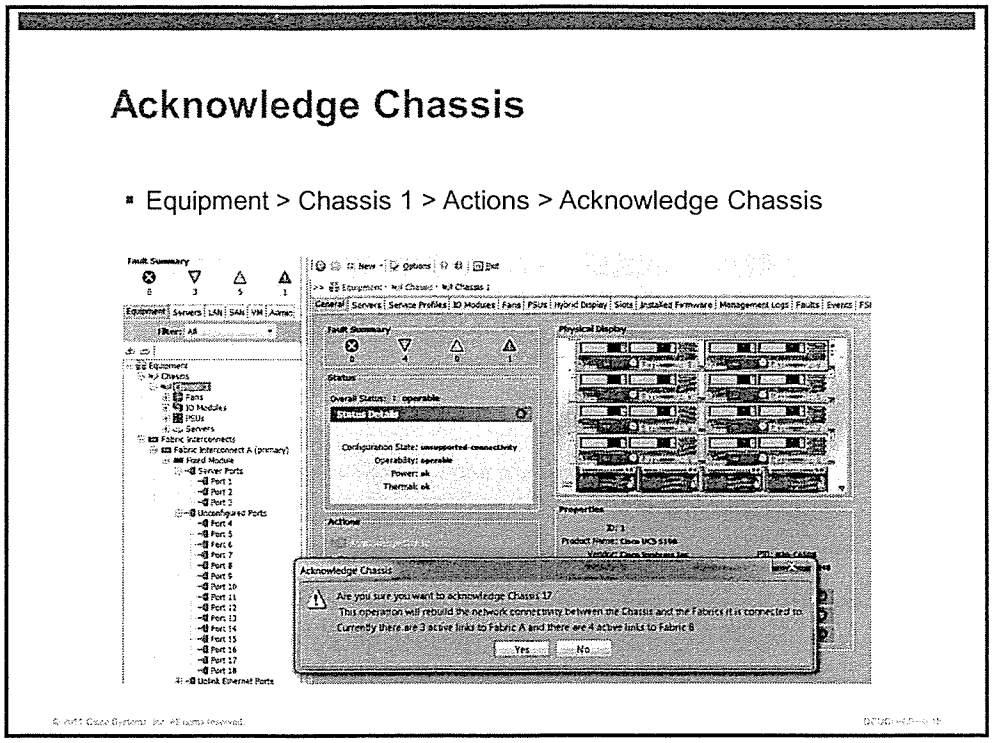
Serial over LAN (SoL) allows an external User Datagram Protocol (UDP) connection to the serial console port.

IPMI provides external access to the Cisco IMC, even if the server is powered off in standby mode. IPMI connections can poll sensors on the blade and power control. A server can be remotely powered on or off via IPMI.

Discovery Process and How to Monitor It

This topic discusses the chassis and server discovery processes and how to monitor discovery via the finite state machine (FSM).

Acknowledge Chassis



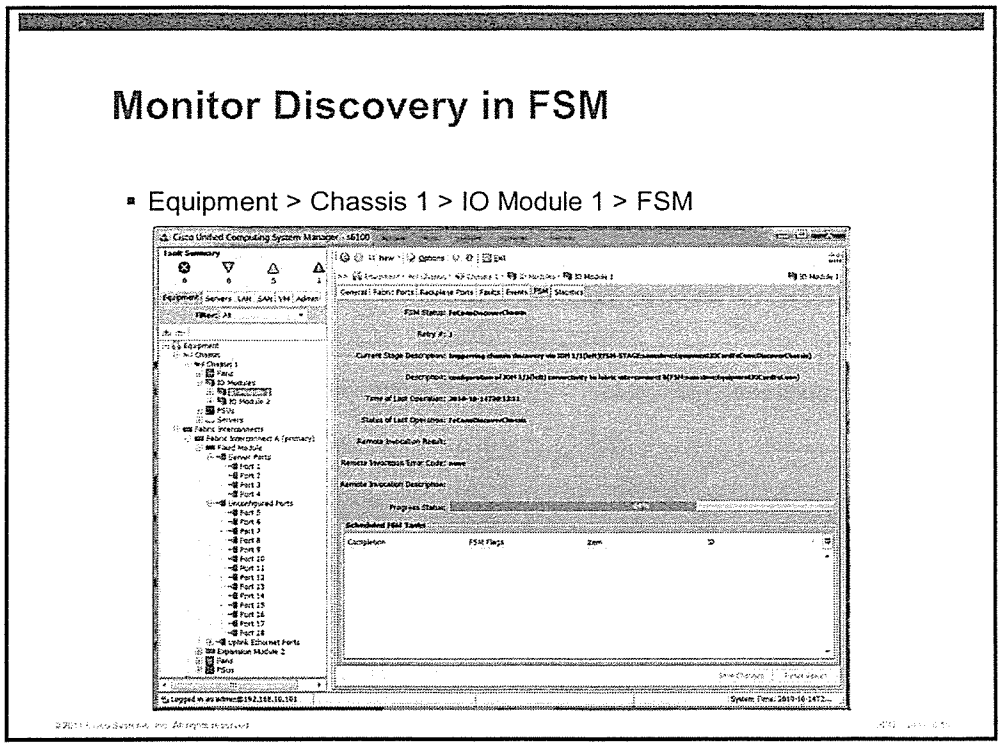
Chassis discovery occurs when a chassis is initially connected to the fabric interconnect and Cisco UCS Manager detects that a new server link has become active. A connection is made to the CMC. The CMC sends information about the chassis inventory (IOM, fans, power supplies, serial numbers, part IDs, and so on) to Cisco UCS Manager.

If server presence is detected, the inventory of the server (or servers) will be sent to Cisco UCS Manager. The details of the inventory include serial number, vendors, CPU type, installed DIMMs, adapter cards, hard drives, BIOS, and Cisco IMC.

All of the inventory details are stored as managed objects by the data management engine (DME).

To observe chassis discovery, you can reacknowledge the chassis and monitor the process.

Monitor Discovery in FSM



After the chassis has been reacknowledged, you can watch the process in the FSM tab of either IOM.

An FSM is a series of logical transitions that occur in a specific order. The chassis and server discovery processes are examples of where an FSM is used to validate a complex series of events.

Summary

Summary

- The number of links from the fabric interconnect to the IOM determines the amount of bandwidth oversubscription to each blade.
- The IOM is a fabric extender that manages data and management plane communications, manages component discovery and controls, and monitors low-level chassis operations.
- The Cisco IMC provides access to KVM over IP, SoL, and IPMI.
- The CMC component is responsible for the discovery process when components are added to the Cisco UCS system.

Lesson 2

Exploring the Cisco UCS B-Series User Interfaces

Overview

As an implementation engineer or service technician, it is important that you are able to navigate the Cisco Unified Computing System (UCS) Manager GUI and command-line interface (CLI) to configure, monitor, and troubleshoot Cisco UCS deployments.

Objectives

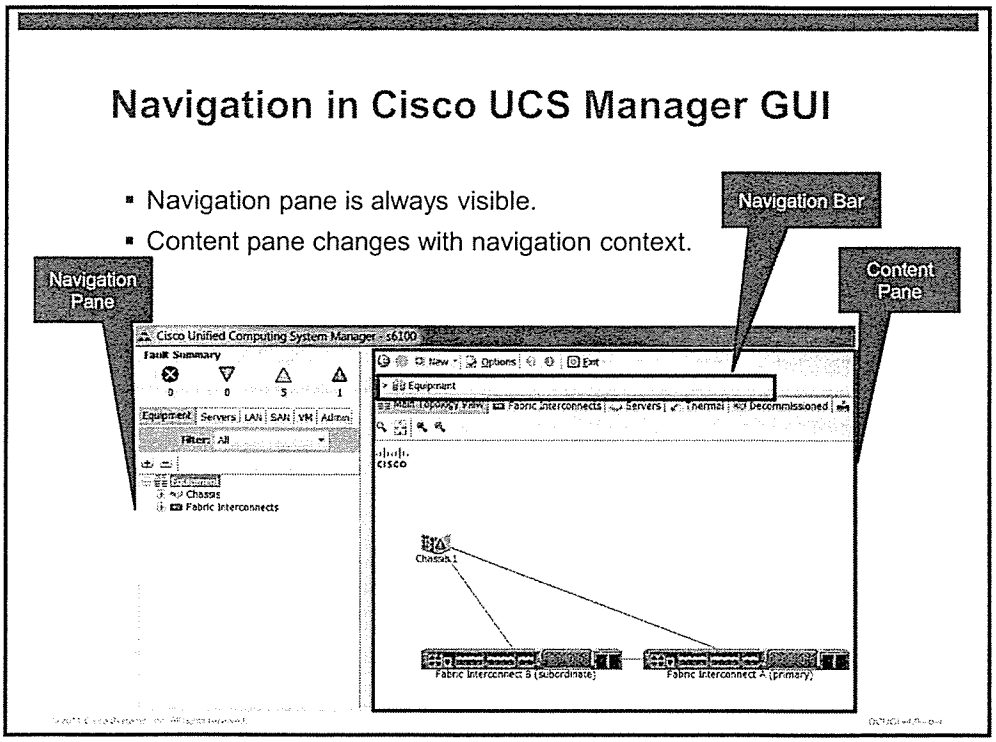
Upon completing this lesson, you will be able to navigate the Cisco UCS Manager GUI and understand the functions that are monitored or configured in the interface. This ability includes being able to meet these objectives:

- Navigate the layout of the Cisco UCS Manager GUI
- Describe the features that are available in the navigation window
- List the main features of the Cisco UCS Manager
- Access the Cisco UCS Manager CLI
- Connect to the CLI shells

Cisco UCS Manager GUI

This topic describes the Cisco UCS Manager GUI and how to use its navigation features.

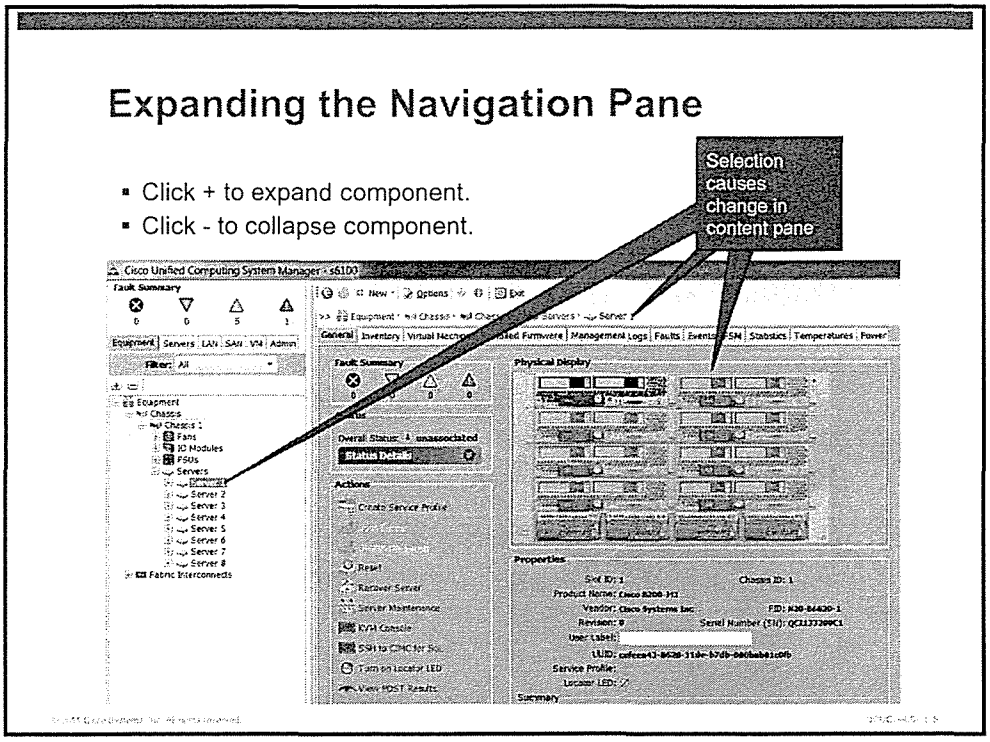
Navigation in Cisco UCS Manager GUI



The Cisco UCS Manager GUI is divided into two primary panes. The navigation pane allows you to move through the configuration elements for physical and logical components. The content pane displays the current context of the navigation pane. As you move through the navigation pane hierarchy, the Navigation Bar above the content pane indicates your path in the hierarchy. You can click any element in the navigation bar to change the current context of the content pane.

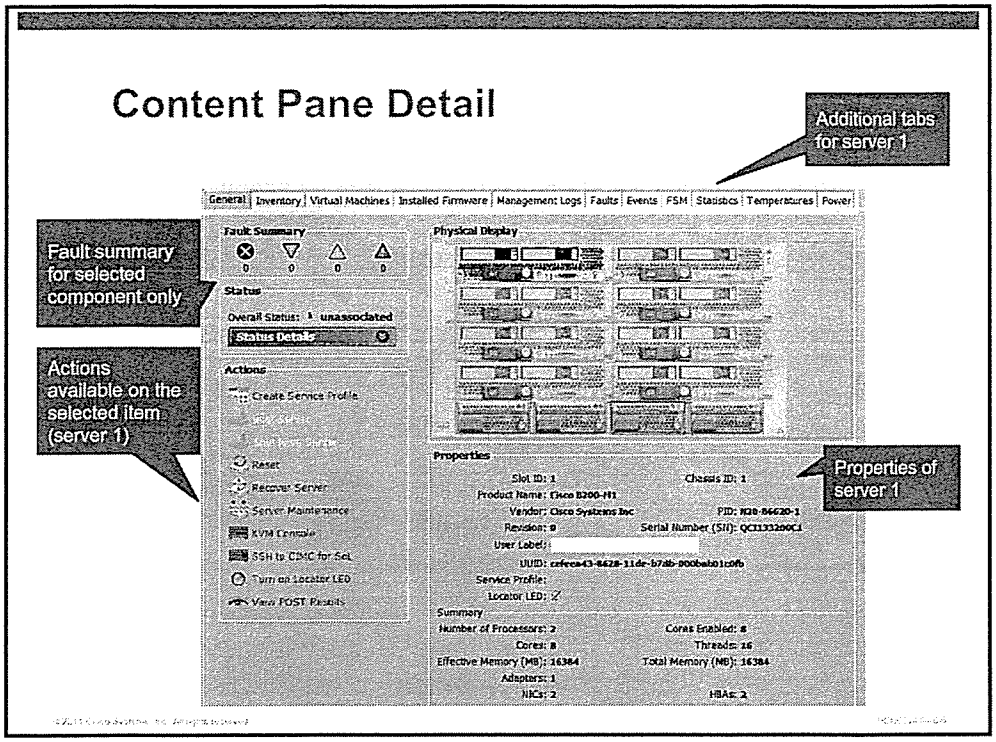
Note	The Navigation Bar is sometimes referred to casually as "the breadcrumb trail."

Expanding the Navigation Pane



In the navigation pane, clicking a "+" sign expands elements in the hierarchy and the "-" sign collapses them. When you select items in the navigation pane, the context in the content pane changes to match the element that is selected in the navigation pane.

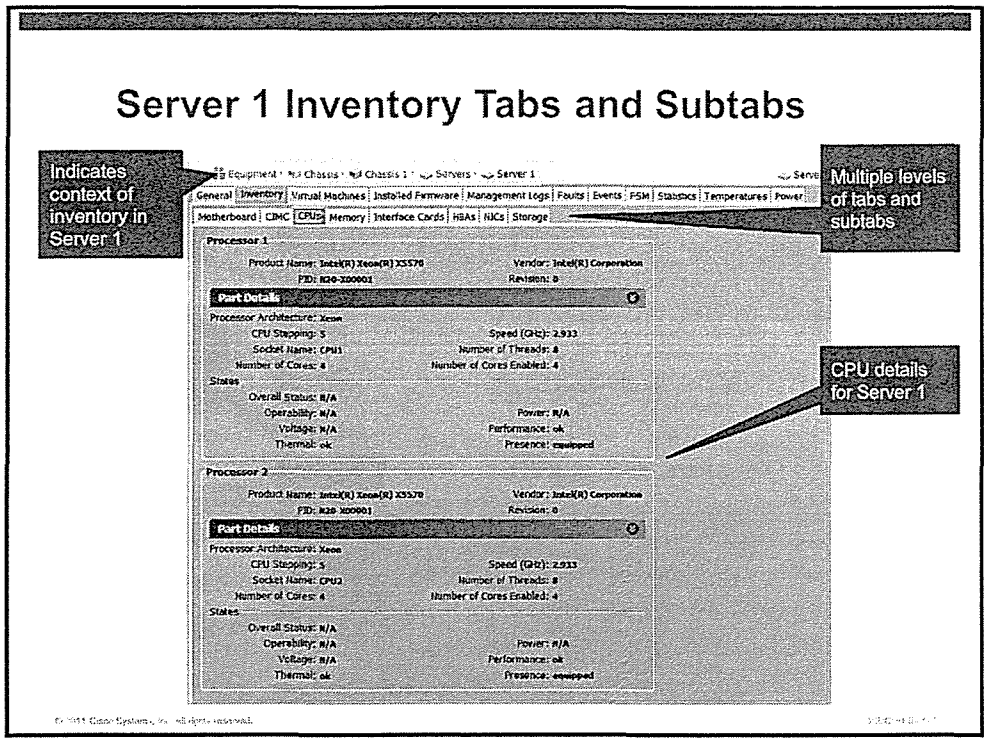
Content Pane Detail



The content pane context shown in the figure was generated by selecting Chassis 1, Server 1 in the navigation pane. The fault summary in the content pane is specific to faults active on the selected component. In this case, there are no active faults on Server 1.

Most content panes include an action pane. With Server 1, you have power control and utilities such as the keyboard, video, mouse (KVM) console. For elements such as servers, there is more information available than will fit into a single window, and there are labeled tabs directly above the content pane.

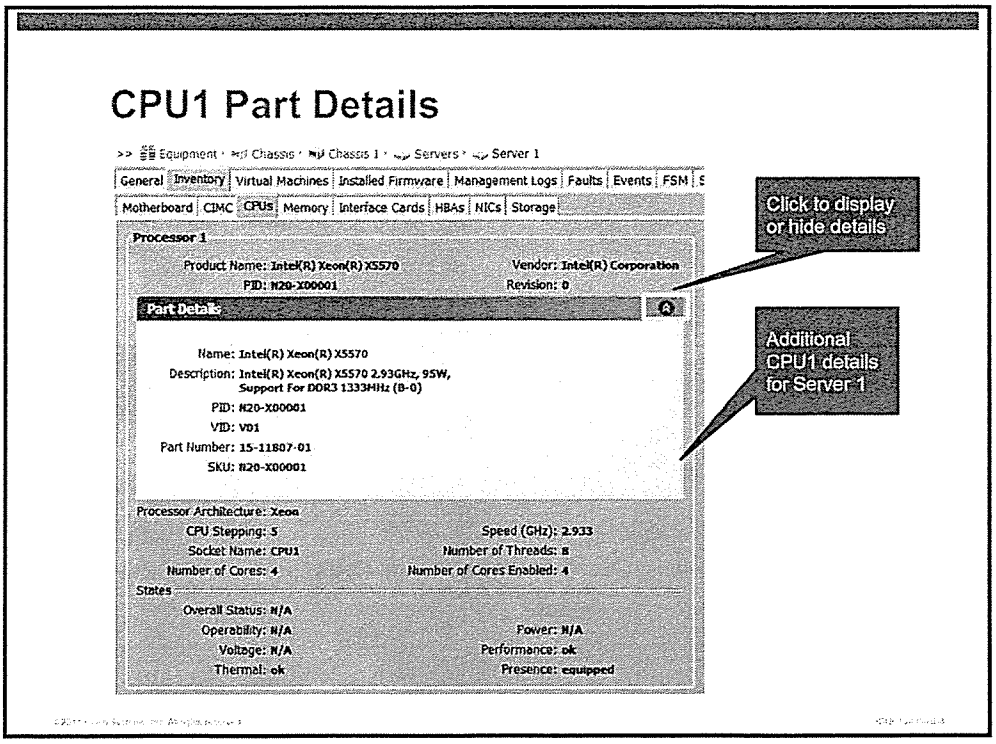
Server 1 Inventory Tabs and Subtabs



From the context strip, it is clear that the content pane is displaying information about Server 1 in Chassis 1.

If a selector tab has more information than can be displayed in the content pane, there may be multiple levels of subtabs. By selecting Inventory > CPU, the content pane shifts context to Server 1 CPU data.

CPU1 Part Details

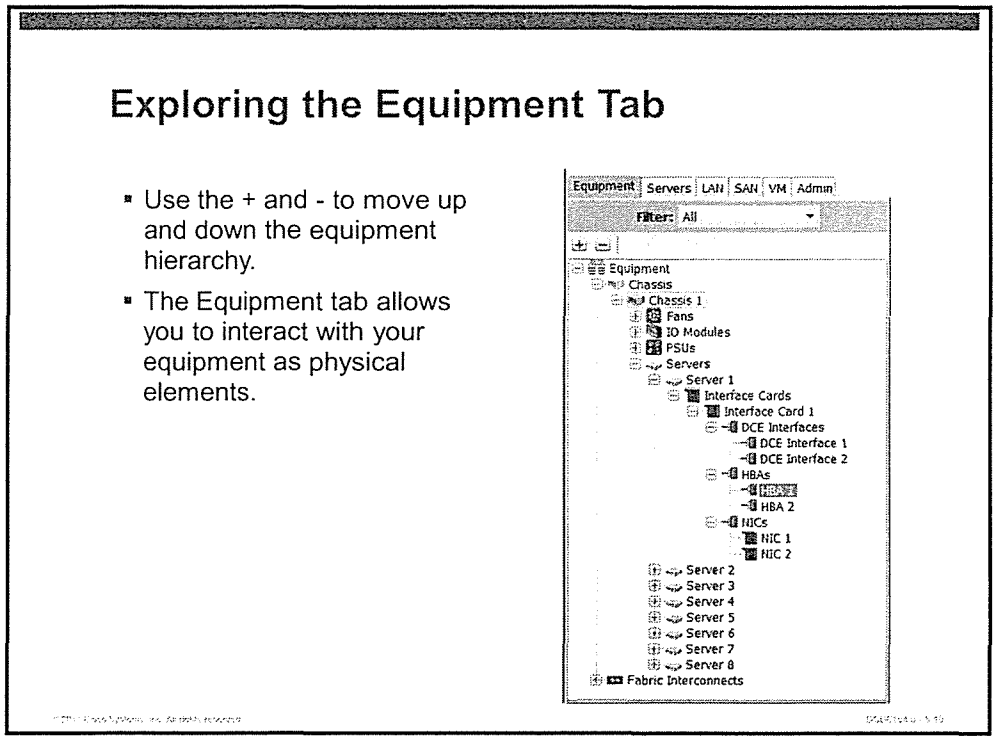


When an element in the content pane includes a double arrow icon, you can click the double-arrow icon for additional details about that element. In the example that is shown, there is additional detail about CPU1. Click the arrows again to collapse the detail display.

Navigation Window

This topic describes the six tabs in the navigation pane.

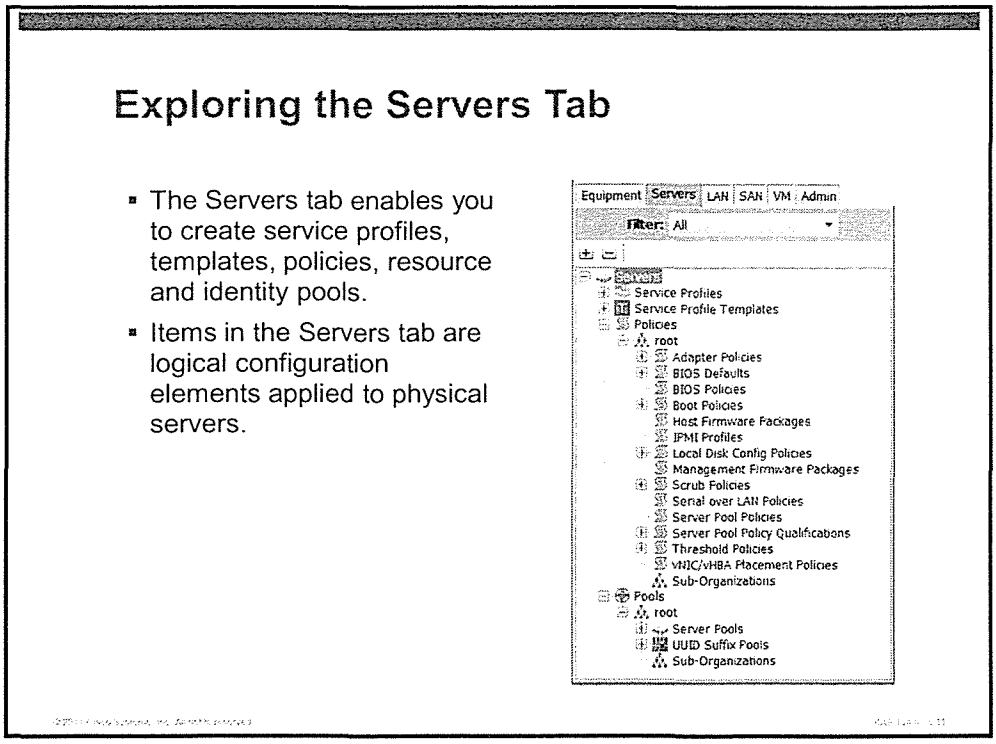
Exploring the Equipment Tab



The Equipment tab allows you to select and interact with Cisco UCS components at the physical level. As you expand into the equipment hierarchy, any element that you select will be featured in the content pane.

The major categories in the Equipment tab include Chassis and Fabric Interconnects.

Exploring the Servers Tab

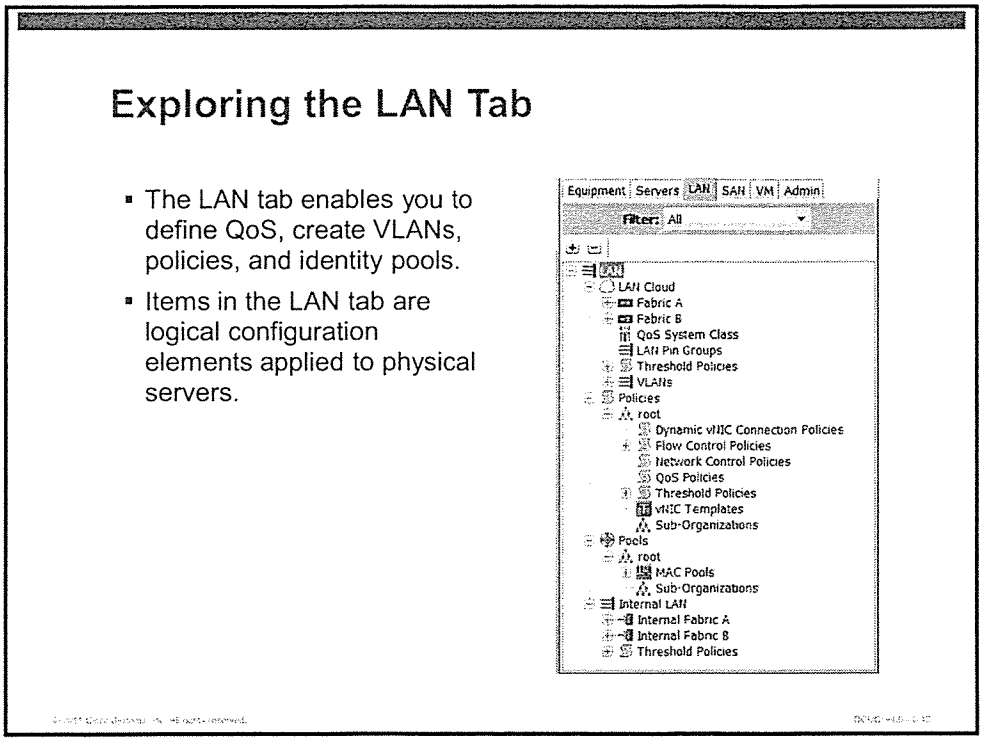


The Servers tab enables you to create, modify, and delete logical server components and apply them to physical servers.

The major categories in the Server tab include the following:

- Service Profiles
- Service Profiles Templates
- Policies
- Pools

Exploring the LAN Tab

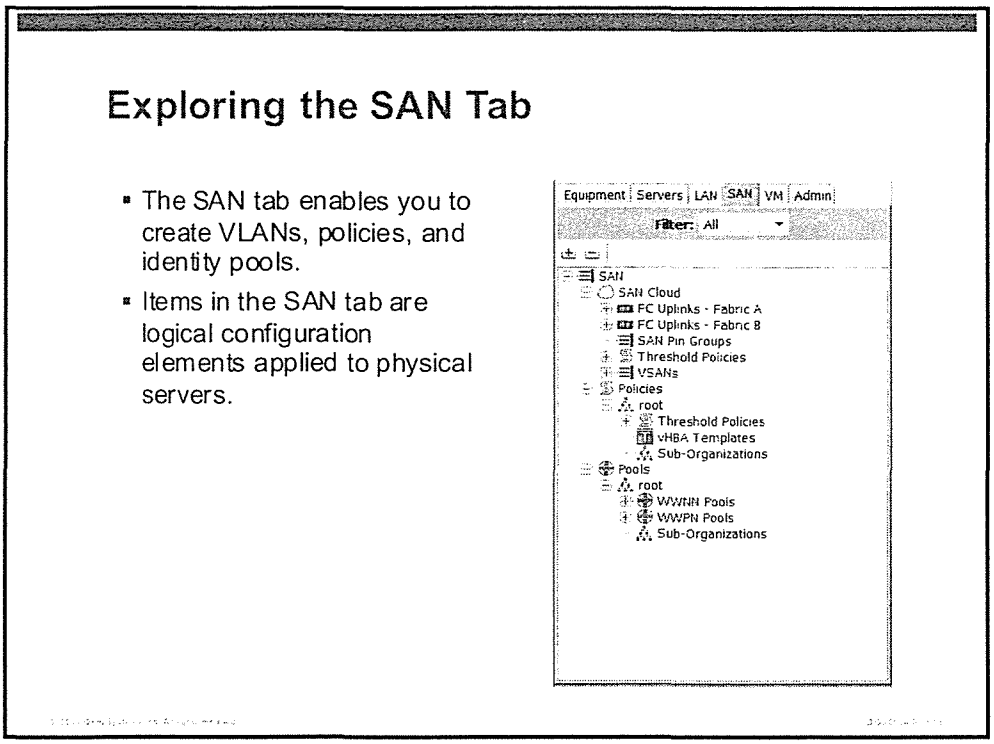


The LAN tab enables you to create, modify, and delete configuration elements that are associated with the Ethernet network.

The major categories in the LAN tab include the following:

- LAN Cloud
- Policies
- Pools
- Internal LAN

Exploring the SAN Tab

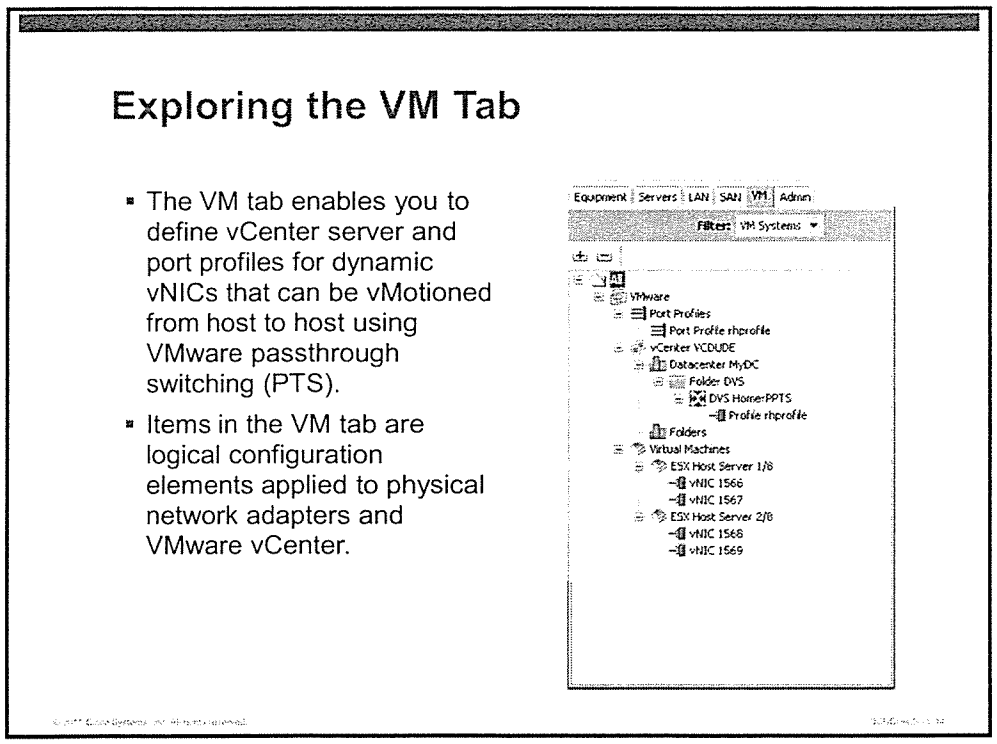


The SAN tab enables you to create, modify, and delete configuration elements that are associated with the Fibre Channel SAN and Fibre Channel over Ethernet (FCoE) communications.

The major categories in the SAN tab include the following:

- SAN Cloud
- Policies
- Pools

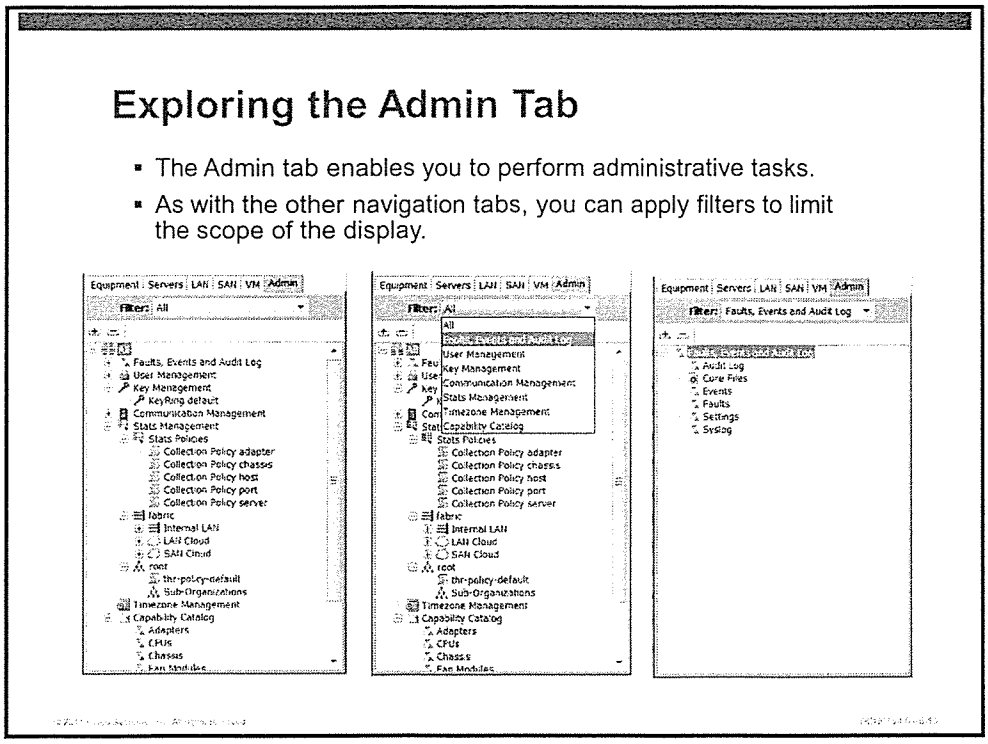
Exploring the VM Tab



The VM tab enables you to create, modify, and delete configuration elements that are associated with VMware vSphere. In Cisco UCS Release 1.3, the M81KR Virtual Interface Card (VIC) supports dynamic virtual network interface cards (VNICs) and VMware pass-through switching (PTS).

The major categories in the VM tab include Port Profiles and Virtual Machines.

Exploring the Admin Tab



The Admin tab enables you to create, modify, and delete configuration elements that are associated with general Cisco UCS administration tasks. With so many major categories in the Admin tab, it is convenient to make use of category filtering to display only the elements of interest. Filtering is available in all navigation tabs, but is only demonstrated here.

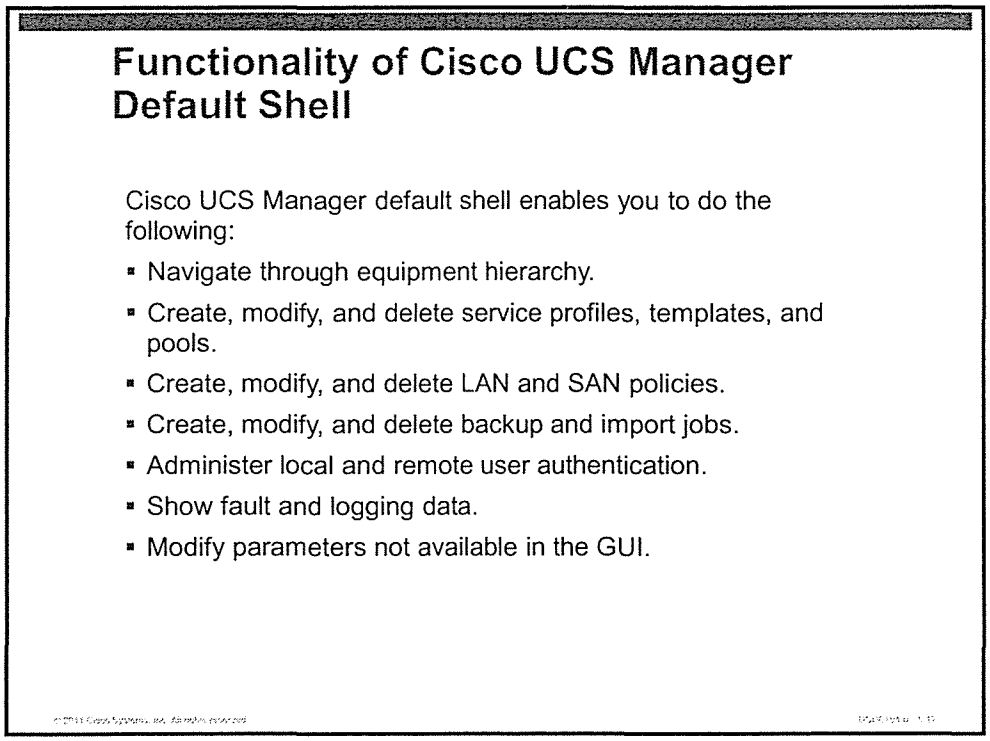
The major categories in the Admin tab include the following:

- Faults, Events, and Audit Log
- User Management
- Key Management
- Communications Management
- Stats Management
- Timezone Management
- Capability Catalog

Main Features of the Cisco UCS Manager

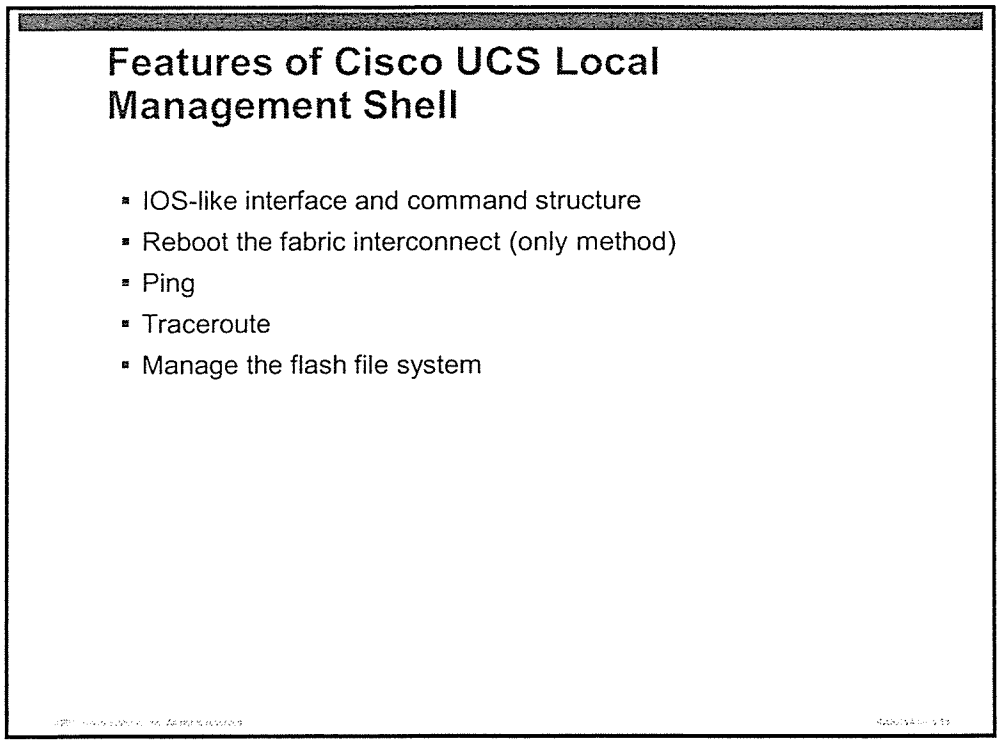
This topic describes the seven Cisco UCS CLI shells in more detail.

Functionality of Cisco UCS Manager Default Shell



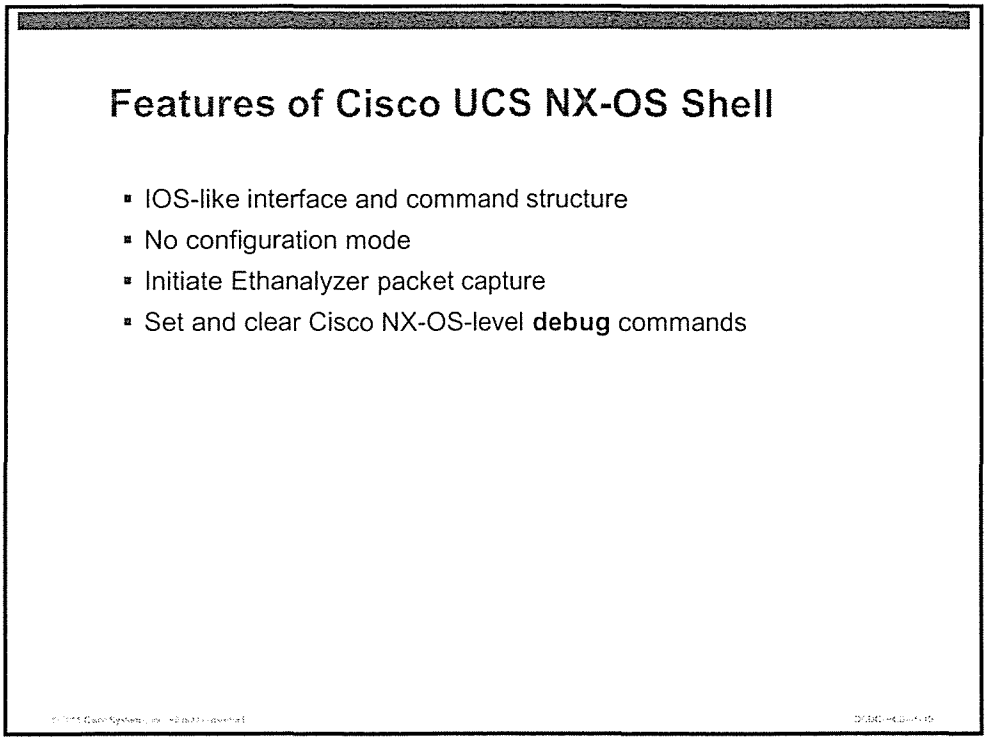
The default Cisco UCS CLI shell provides access to all of the functionality of the Cisco UCS Manager GUI plus additional features not available in the GUI.

Features of Cisco UCS Local Management Shell



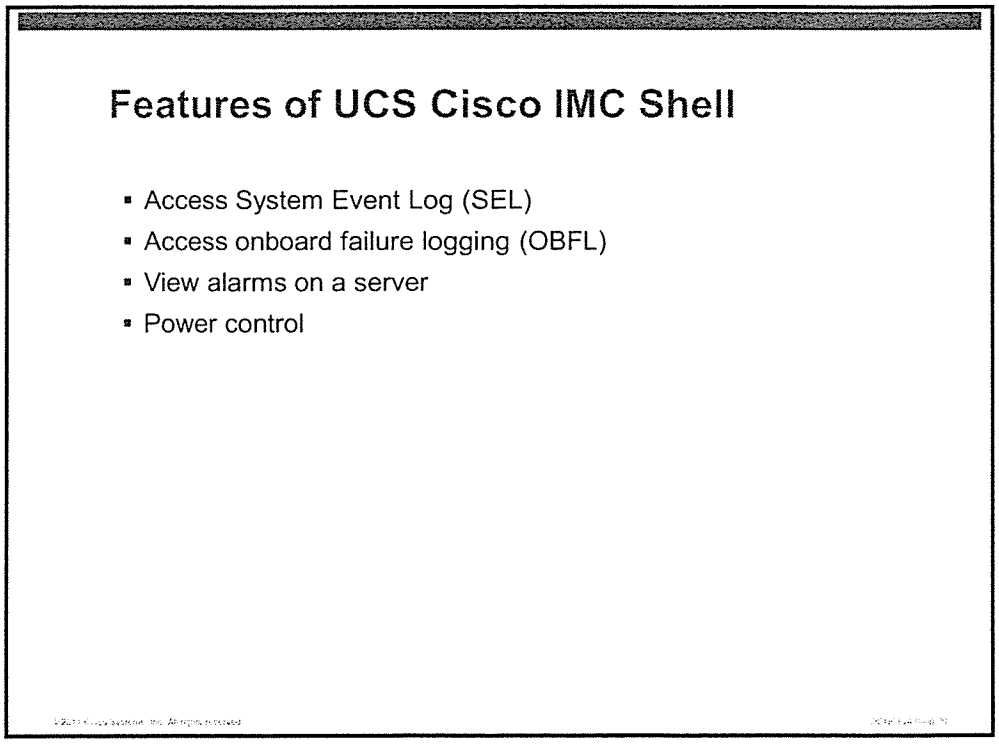
The Local Management Interface will seem familiar and intuitive to experienced Cisco IOS users. The Local Management Interface provides access to system utilities, file system management, and reboot control for a given fabric interconnect.

Features of Cisco UCS NX-OS Shell



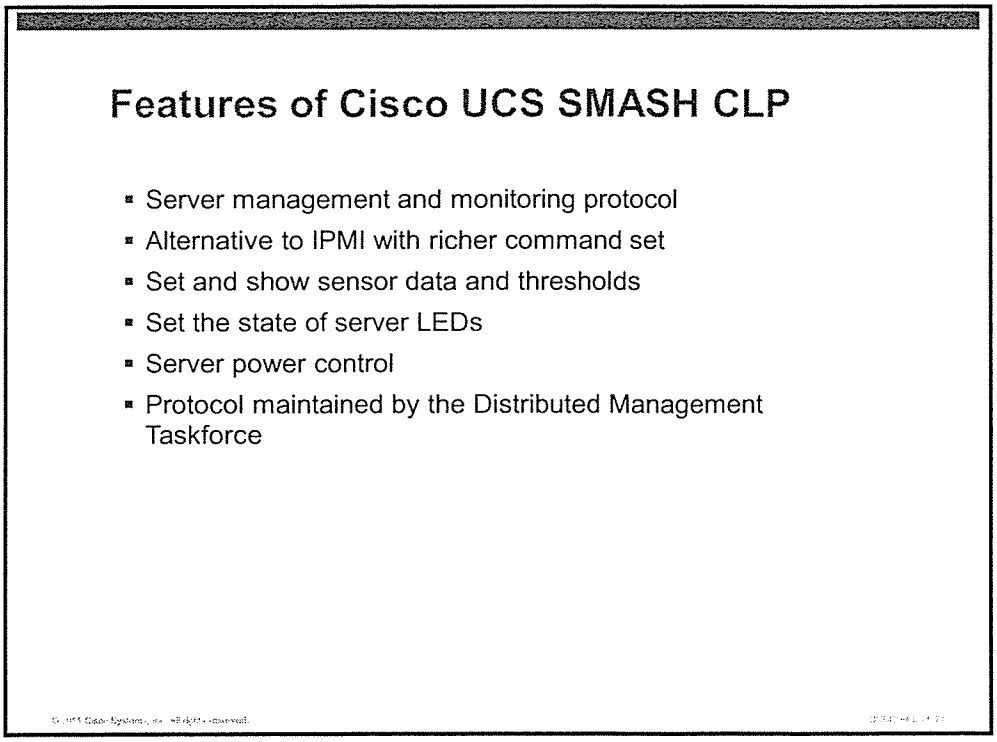
The Cisco Nexus Operating System (NX-OS) shell interface will seem familiar and intuitive to experienced Cisco IOS users. Cisco NX-OS is a read-only shell. You cannot enter NX-OS configuration mode. If configuration mode was available, it would be possible to create out-of-band changes that would not be consistent with the Cisco UCS data management engine (DME) database. This could result in unexpected operation or system connectivity failures that would be very difficult to troubleshoot.

Features of UCS Cisco IMC Shell



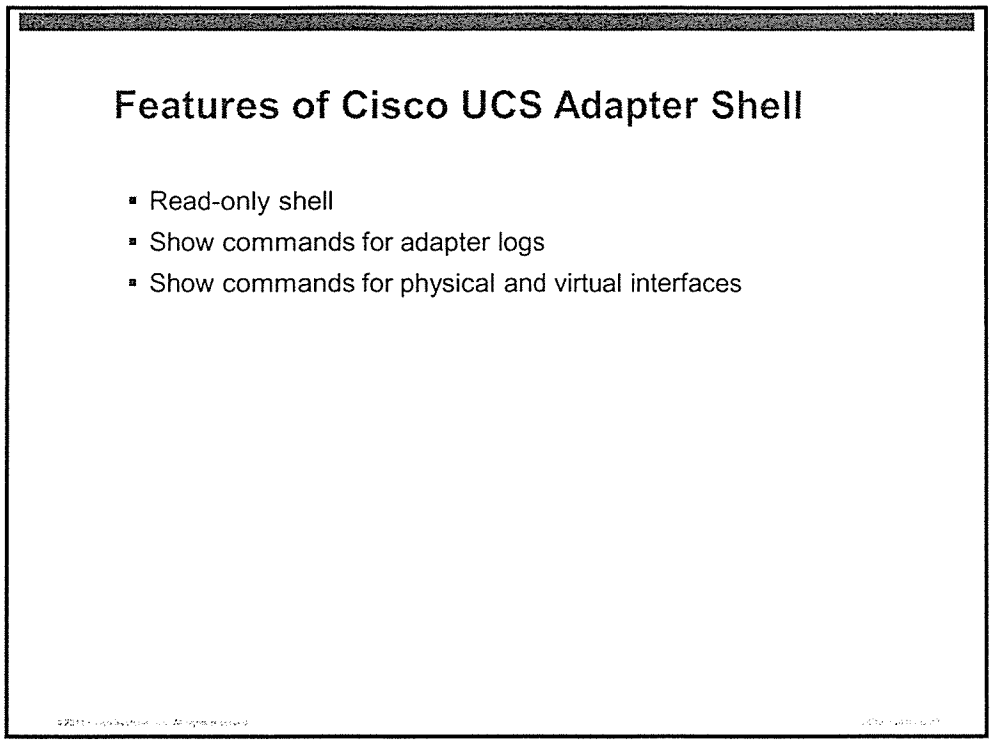
The Cisco Integrated Management Controller (IMC) shell connects to the baseboard management controller on a server motherboard. This shell provides an alternative to using the Intelligent Platform Management Interface (IPMI) protocol to retrieve log data, sensor data, and power control. Nearly all of the features available in this shell are also available in the Cisco UCS Manager GUI.

Features of Cisco UCS SMASH CLP



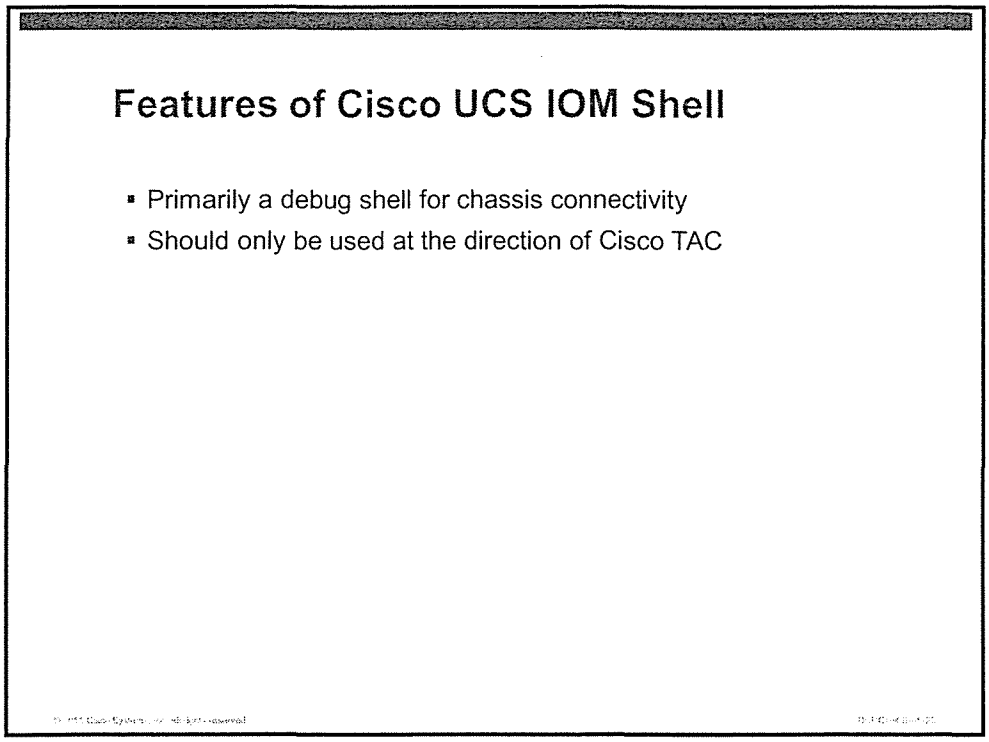
Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) shell offers a wealth of standards-based command-line tools for monitoring and managing heterogeneous brands of servers. It lends itself well to scripted automation. Thorough knowledge of the protocol will be required to gain the maximum benefit from this shell.

Features of Cisco UCS Adapter Shell



The adapter shell is a read-only facility to gather low-level information about the operation of mezzanine adapters. It is unlikely that you will access this shell without guidance from Cisco Technical Assistance Center (TAC).

Features of Cisco UCS IOM Shell

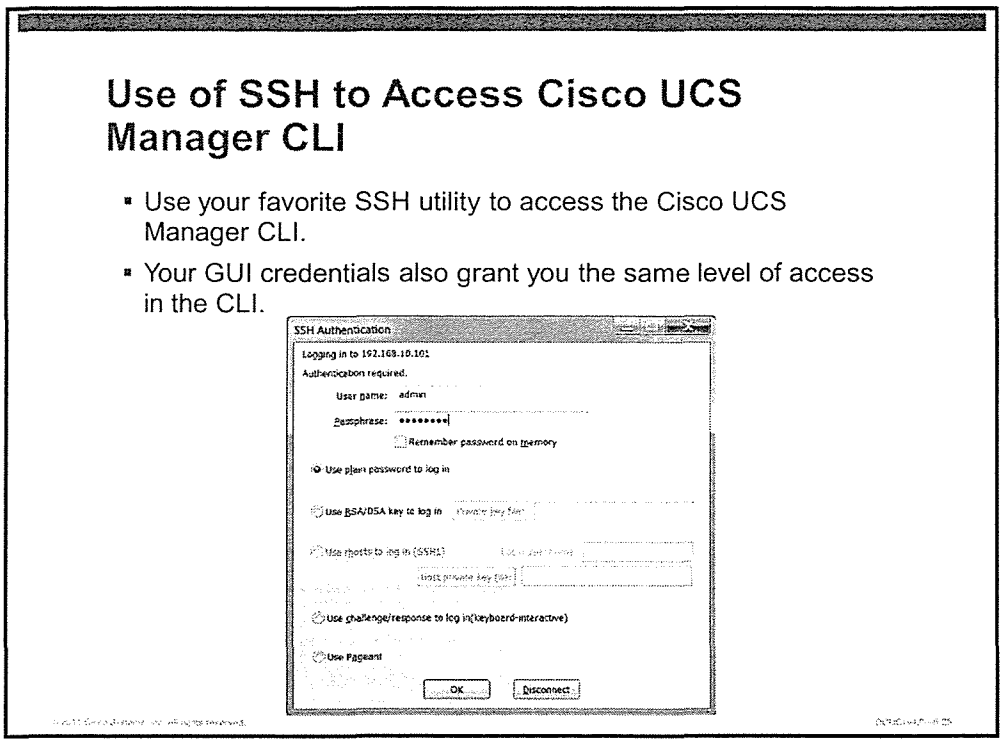


The I/O module (IOM) shell is a low-level debugging shell that is meant for experienced Cisco TAC engineers. It is possible to render an I/O module inoperable if this tool is used improperly. Use with great caution.

Access the Cisco UCS Manager CLI

This topic discusses how to access and navigate the Cisco UCS Manager CLI.

Use of SSH to Access Cisco UCS Manager CLI

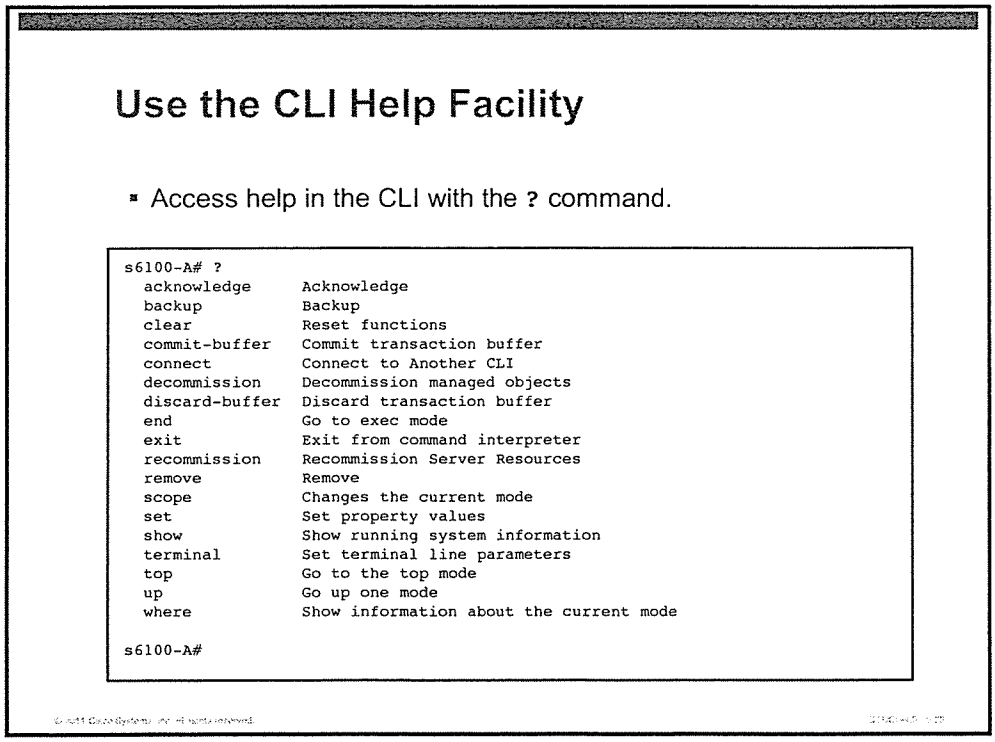


The Secure Shell (SSH) protocol has been in widespread use for over 10 years. It allows Remote Terminal access to the Cisco UCS Manager CLI over an encrypted session. Although Telnet is available, it is disabled by default.

There are many free SSH utilities for Microsoft Windows, including Tera Term and PuTTY. On Linux hosts, SSH is likely available from a terminal interface.

The Cisco UCS Manager CLI uses the same authentication credentials as the Cisco UCS Manager GUI.

Use the CLI Help Facility

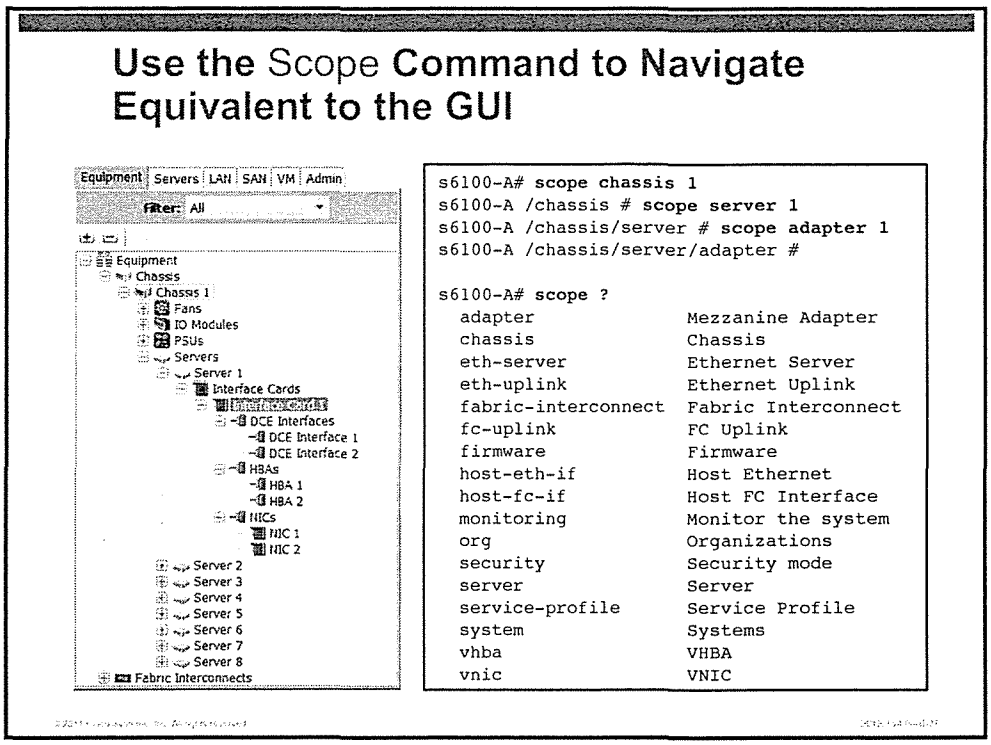


After you authenticate to Cisco UCS Manager CLI, you will arrive at the default shell. If you use SSH to access the IP address of the cluster virtual IP, you will connect to the active management node in the cluster. This is a best practice unless you need to change a parameter specific to a fabric interconnect.

Access the available commands by entering the **?** command and pressing **Enter**.

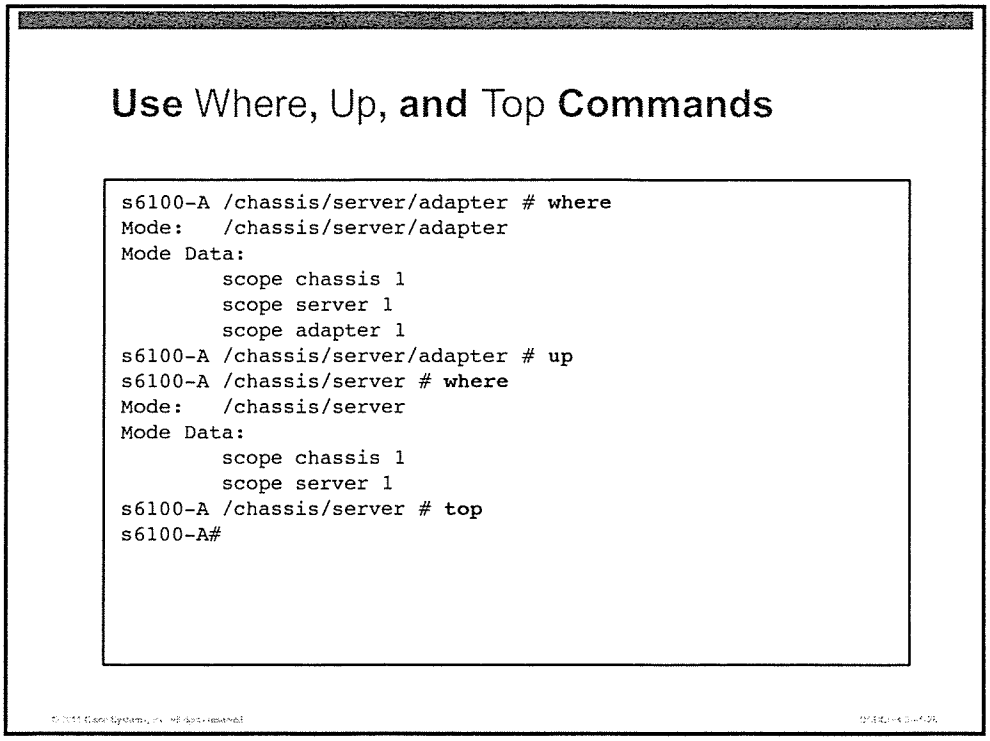
The CLI is IOS-like and features tab command completion and command history.

Use the Scope Command to Navigate Equivalent to the GUI



The **scope** command allows you to move through the equipment tab hierarchy to locate the element that needs to be monitored or configured. The example in the figure shows how to use the **scope** command to move to the identical position as shown in the navigation pane.

Use Where, Up, and Top Commands

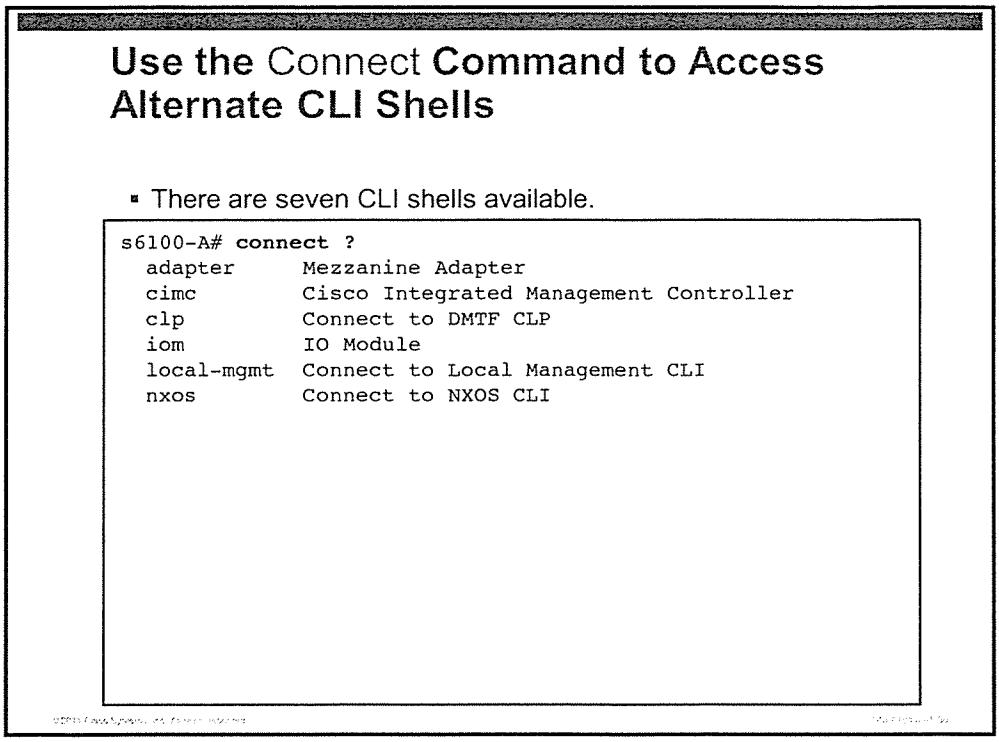


As you move down the configuration hierarchy, the CLI prompt changes to reflect the new context. To determine which component the current context applies to, use the **where** command. The **up** command moves the context up one level in the hierarchy. The **top** command moves the context to the root.

Connect to the CLI Shells

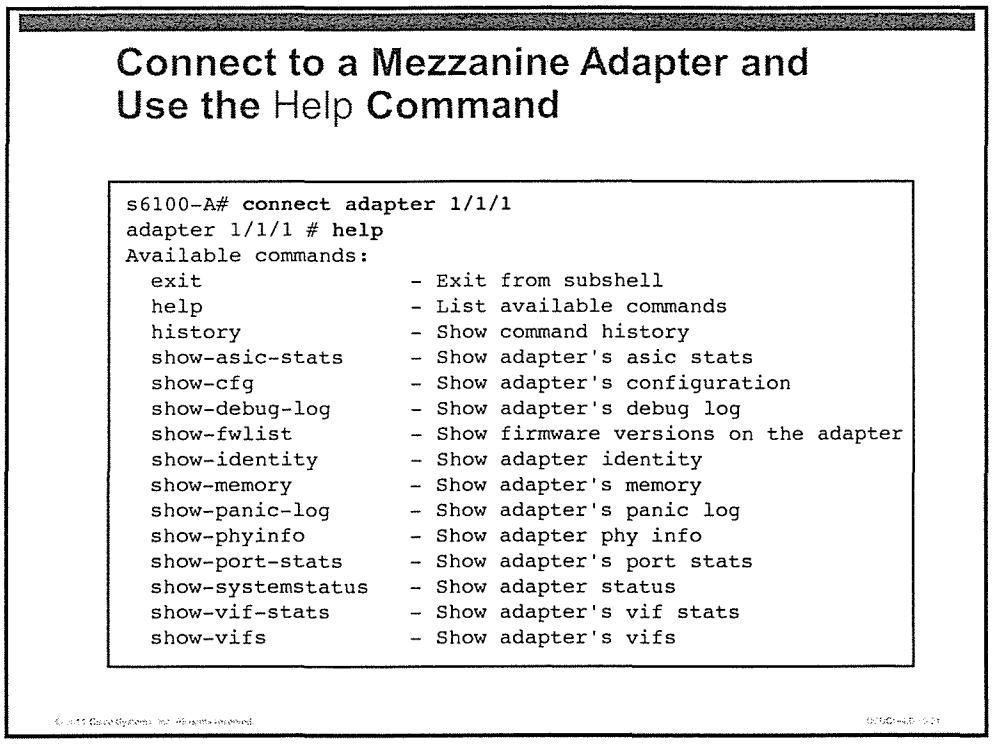
This topic discusses how to connect to the six alternate CLI shells available in Cisco UCS Manager.

Use the Connect Command to Access Alternate CLI Shells



When you log in to Cisco UCS Manager CLI, the default shell is dedicated to creating, modifying, and deleting objects from the DME database. It is equivalent in function to the Cisco UCS Manager GUI. It does not include tools for copying files, managing files in the flash file system, or utilities like ping and traceroute. The **connect** command provides access to alternate shells that provide functionalities not available in the default shell.

Connect to a Mezzanine Adapter and Use the Help Command



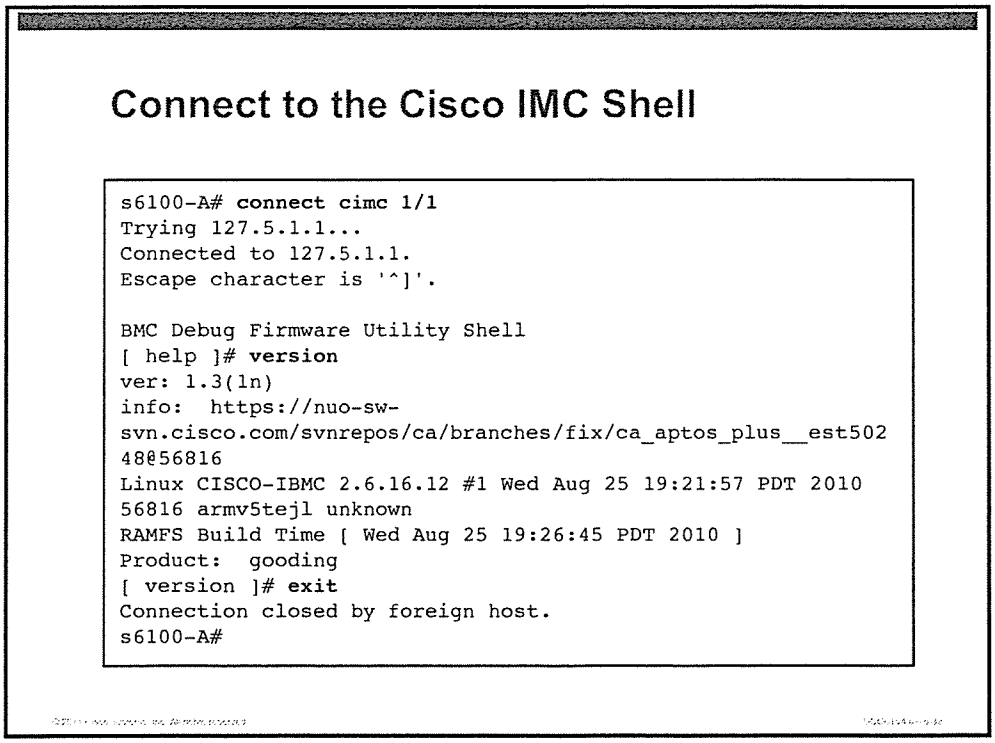
The syntax of the **connect adapter** command requires a three-part argument consisting of chassis number, server number, and adapter number. The command in the example connects to chassis 1, server 1, adapter 1.

The adapter shell allows access to information that might be necessary to troubleshoot connectivity problems. Cisco TAC may ask you to provide the output of adapter **show** commands to assist you with an open issue.

Note Half-slot blades (B200, B230) have only one adapter. Full-slot blades (B250, B440) include two adapter slots, so the adapter can be either "1" or "2."

Note The **show** commands in the adapter shell require that the server is powered on and the adapter has initialized.

Connect to the Cisco IMC Shell



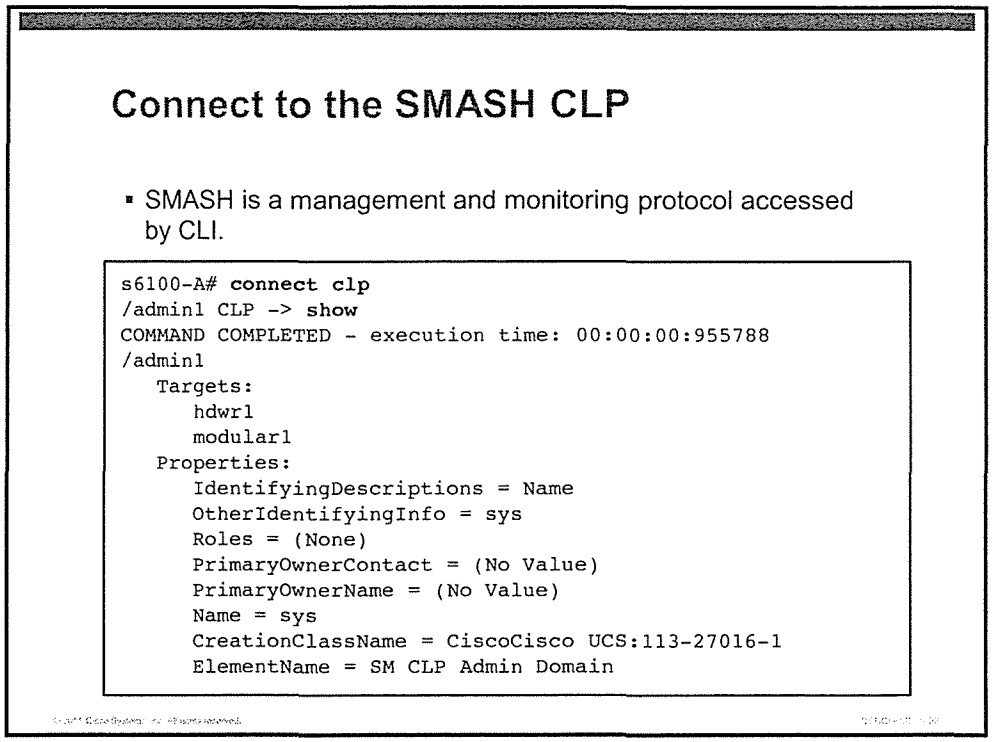
The syntax of the **connect cimc** command requires a two-part argument consisting of chassis number and server number. The command in the example connects to chassis 1, server 1.

The Cisco IMC shell allows access to information that might be necessary to troubleshoot server hardware problems. Cisco TAC may ask you to provide the output of **cimc** commands to assist you with an open issue.

Most of the information available in this shell is also available in the Cisco UCS Manager GUI and IPMI.

Note	Previous to Cisco UCS Manager version 1.3, the Cisco Integrated Management Controller was referred to as the Baseboard Management Controller (BMC). The terms "Cisco IMC" and "BMC" are used interchangeably, depending on the Cisco document that you are reading or to whom you are speaking. The term Cisco Integrated Management Controller is also used to refer to the GUI configuration tool of the Cisco UCS C-Series rack servers.

Connect to the SMASH CLP



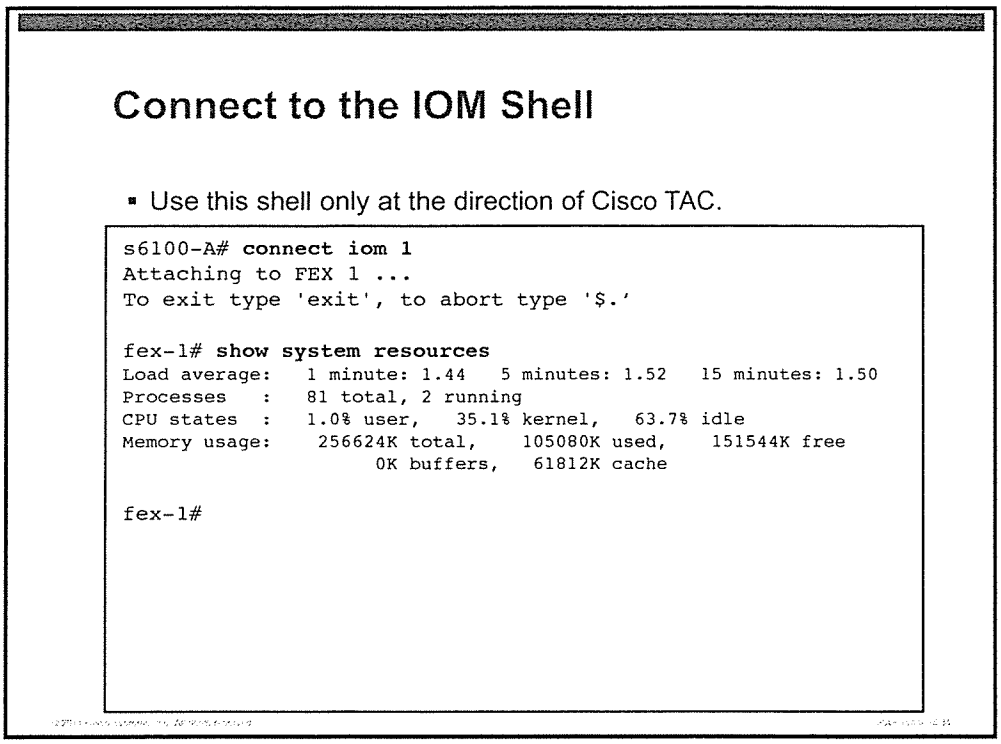
Systems Management Architecture for Server Hardware Command-Line Protocol (SMASH CLP) is a standards-based CLI. It is designed to allow scripted management of heterogeneous servers independent of machine state or operating systems state.

The syntax of the **connect clp** command requires no additional arguments. The command in the example connects to the Cisco UCS system globally. The scope of SMASH CLP management extends to all servers in a Cisco UCS implementation.

SMASH CLP is a robust protocol and will require a thorough understanding of its capabilities before implementing it.

All of the capabilities of this shell are also available in the Cisco UCS Manager XML API.

Connect to the IOM Shell



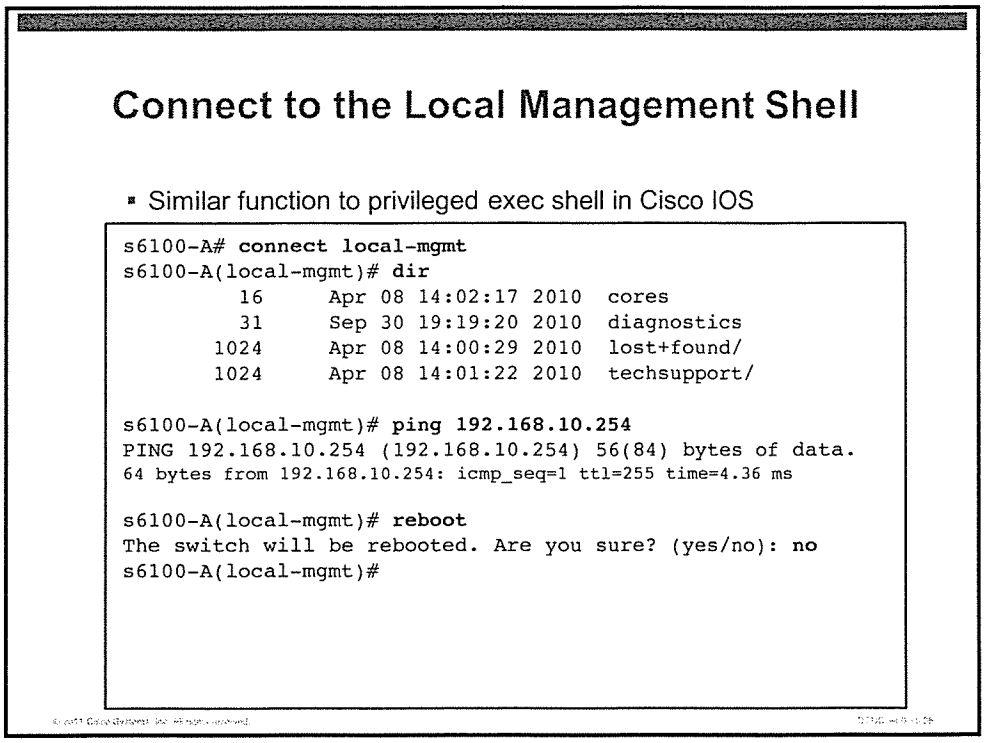
The syntax of the **connect iom** command requires a two-part argument consisting of chassis number and IOM number. The command in the example connects to chassis 1, IOM 1.

The IOM shell is a low-level debug shell and allows access to information that might be necessary to troubleshoot chassis discovery and connectivity problems. Cisco TAC may ask you to provide the output of commands in the IOM shell to assist you with an open issue.

Use of the IOM shell should be guided by a Cisco TAC engineer.

Note	Improper use of the IOM shell renders an IOM unstable or unusable.

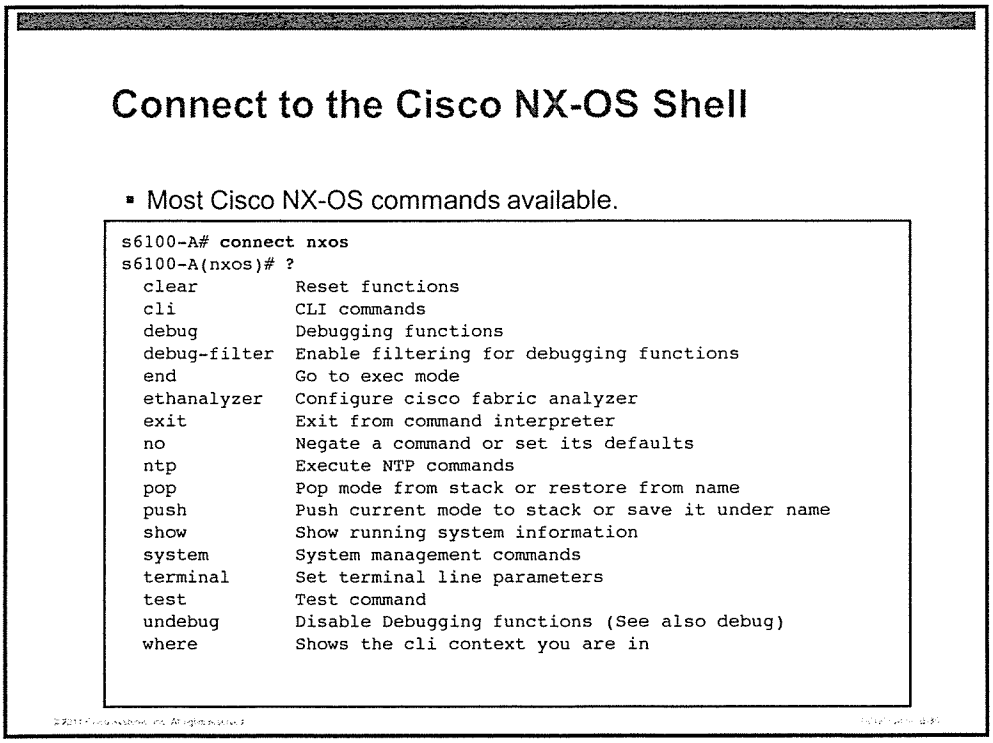
Connect to the Local Management Shell



The syntax of the **connect local-mgmt** command requires no additional arguments. The Local Management Interface shell provides access to utilities such as ping and traceroute. It is the only shell that allows administrators to reboot a fabric interconnect.

If you use SSH to access the cluster virtual IP address, you will connect to the active management node (fabric interconnect). If you need to make a configuration change to a specific fabric interconnect, use SSH to access its explicit IP address.

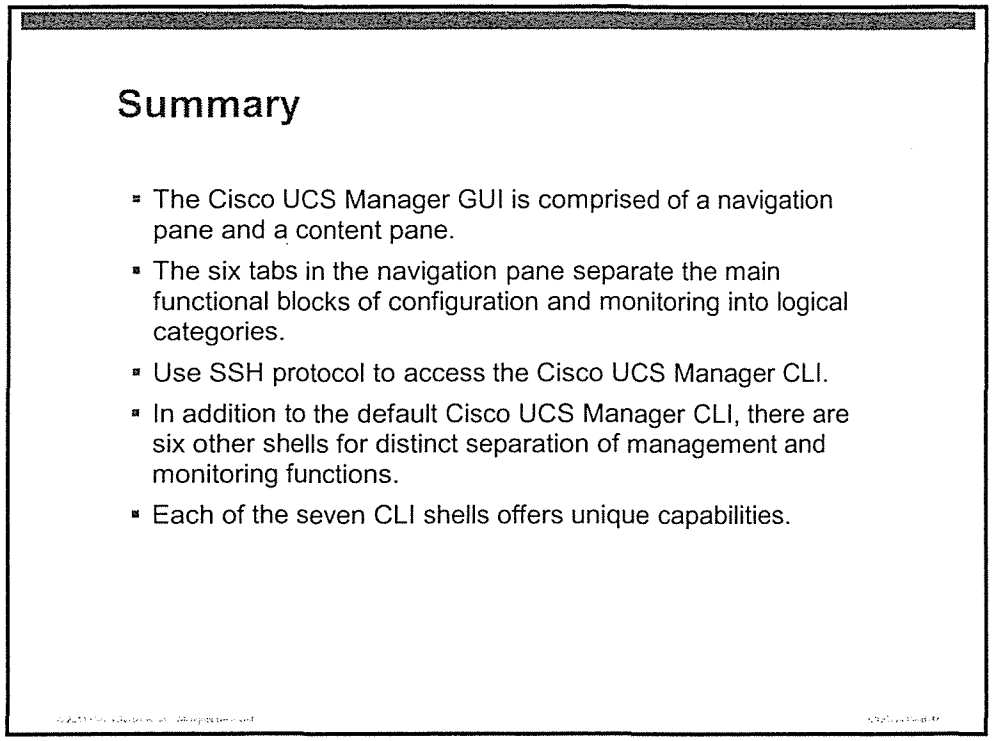
Connect to the Cisco NX-OS Shell



The syntax of the **connect nxos** command requires no additional arguments. The NX-OS shell provides access to operating system **show** commands useful for troubleshooting interface and connectivity issues. Cisco NX-OS is the base operating system of Cisco UCS 6100 Series fabric interconnects. All Cisco UCS functions are loaded by NX-OS.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 3

Configuring Compute Node LAN Connectivity

Overview

Unified fabric is an important value that Cisco UCS offers customers. Use of Fibre Channel over Ethernet (FCoE) protocol greatly reduces cable counts and complexity from the server chassis to the access layer. Correctly configuring LAN Ethernet components is critical for the operation of FCoE. The LAN configuration is the foundation on which all server connectivity and high availability relies.

Objectives

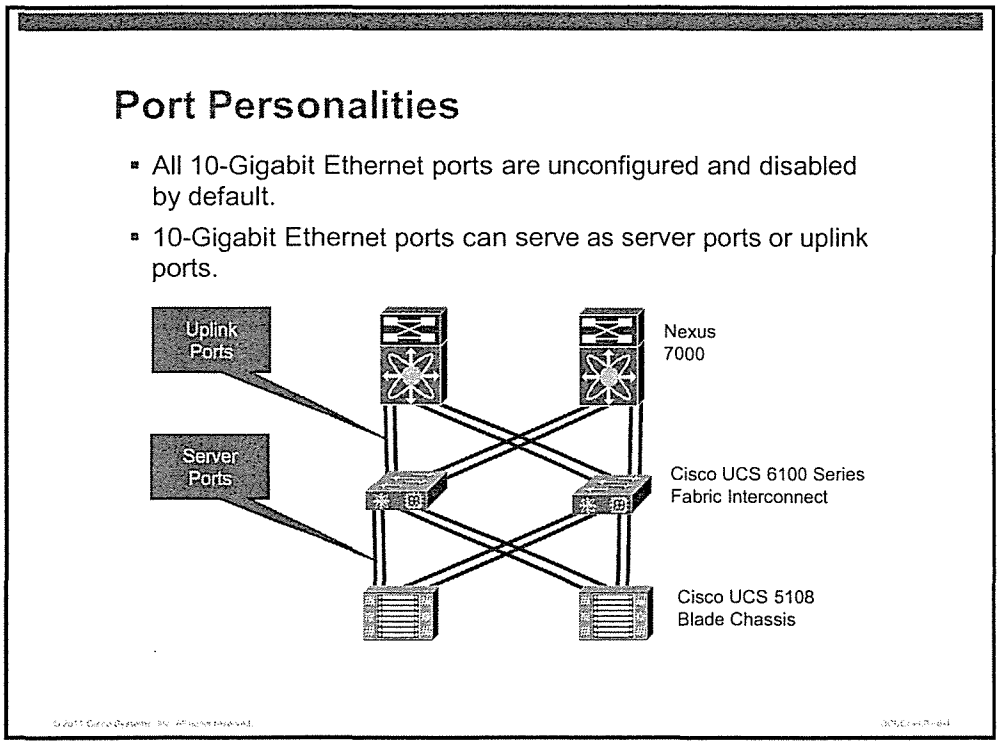
Upon completing this lesson, you will be able to describe the advantages of end-host mode and differentiate between I/O module (IOM) pinning and uplink pinning. You will also understand how to configure VLANs and port channels. This ability includes being able to meet these objectives:

- Differentiate between the three port personality states of 10-Gigabit Ethernet interfaces on the Cisco UCS fabric interconnect
- Describe the requirements and configuration of port channels from the Cisco UCS fabric interconnect to a northbound switch
- Describe end-host mode and its importance in forwarding over multiple Layer 2 links and maintaining a loop-free topology
- Differentiate end-host mode with switched mode
- Describe the requirements for configuring VLANs in Cisco UCS Manager
- Describe the role of vNICs to abstract MAC addresses into a service profile
- Describe static IOM pinning and recovery from link failure
- Describe automatic uplink pinning and recovery from failure
- Describe the configuration of manual uplink pinning and recovery from failure

Port Personality States of 10-Gigabit Ethernet Interfaces on the Cisco UCS Fabric Interconnect

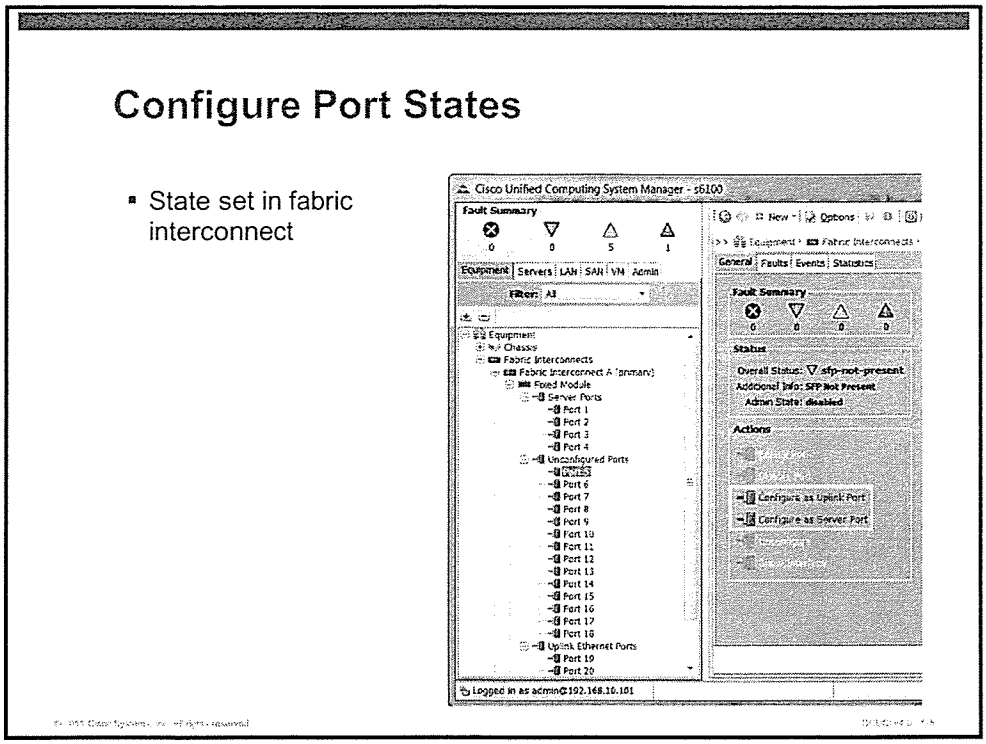
This topic describes the three port states for Ethernet ports on the fabric interconnect.

Port Personalities



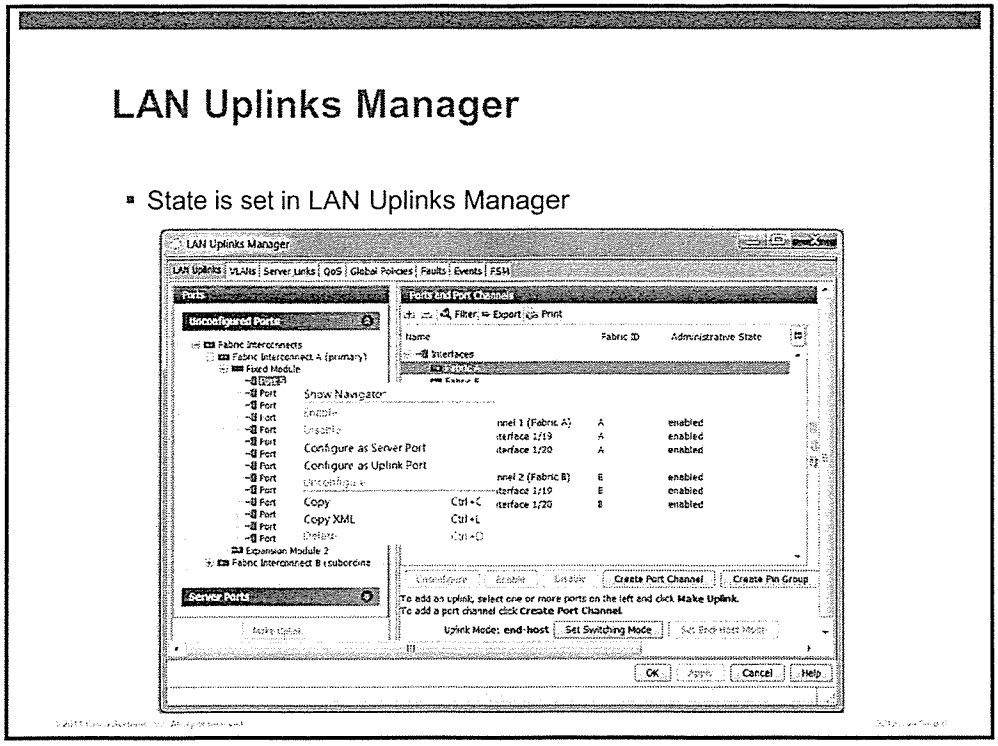
Ethernet ports on the fabric interconnect can be in one of three states: unconfigured, server, or uplink. By default, all Ethernet ports on the fabric interconnect are unconfigured. A state of either server or uplink must be configured before the port will pass traffic.

Configure Port States



Port states can be defined in several places. For this example, select the Equipment tab. Then, expand the inventory of a fabric interconnect and select an unconfigured port. On the content pane, select whether the port should be an uplink to a northbound switch or southbound to an IOM (server port).

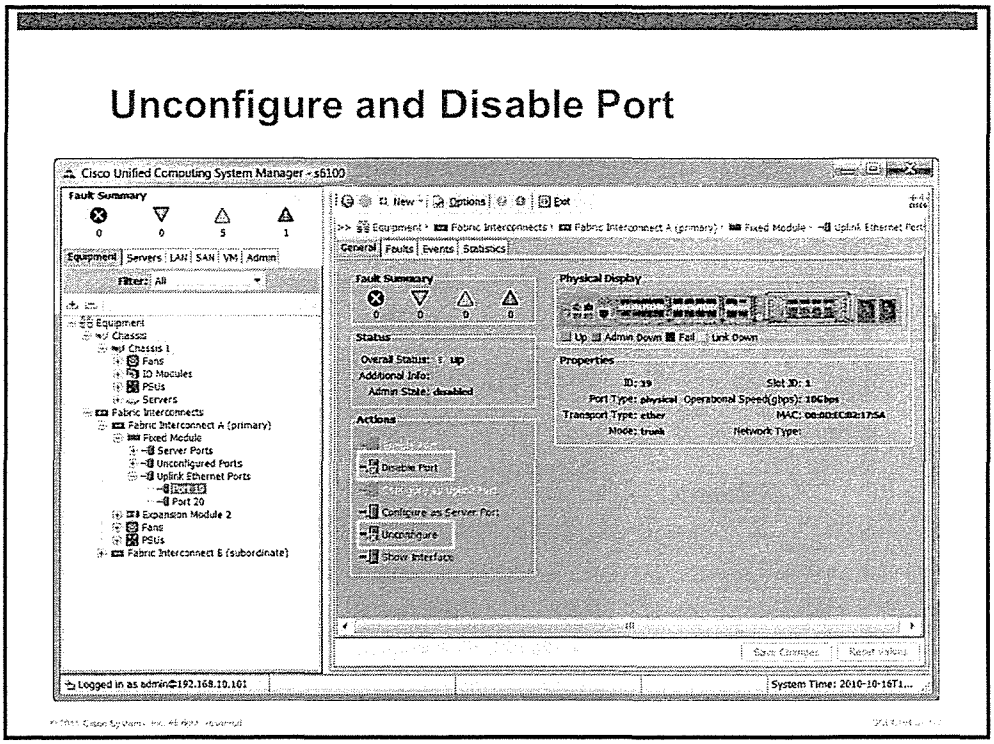
LAN Uplinks Manager



The LAN Uplinks Manager is another tool that can be employed to configure a port state.

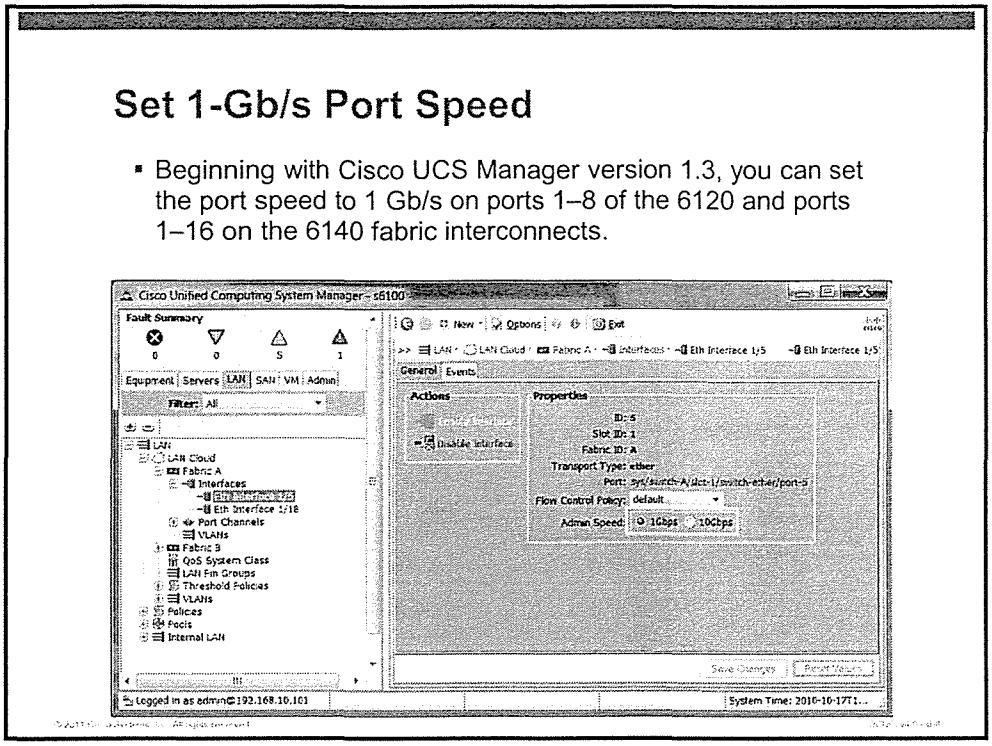
From the Equipment tab of the navigation pane, select a fabric interconnect. Then, select the General tab in the content pane. A link to the LAN Uplinks Manager is available there to configure port state, VLANs, server links, quality of service (QoS), and MAC aging policy.

Unconfigure and Disable Port



To decommission a port, select the port in the Equipment tab. In the General tab of the content pane, click the **Disable Port** and **Unconfigure** links. The configuration change requires you to click **Save Changes** in the lower-right corner of the content pane.

Set 1-Gb/s Port Speed



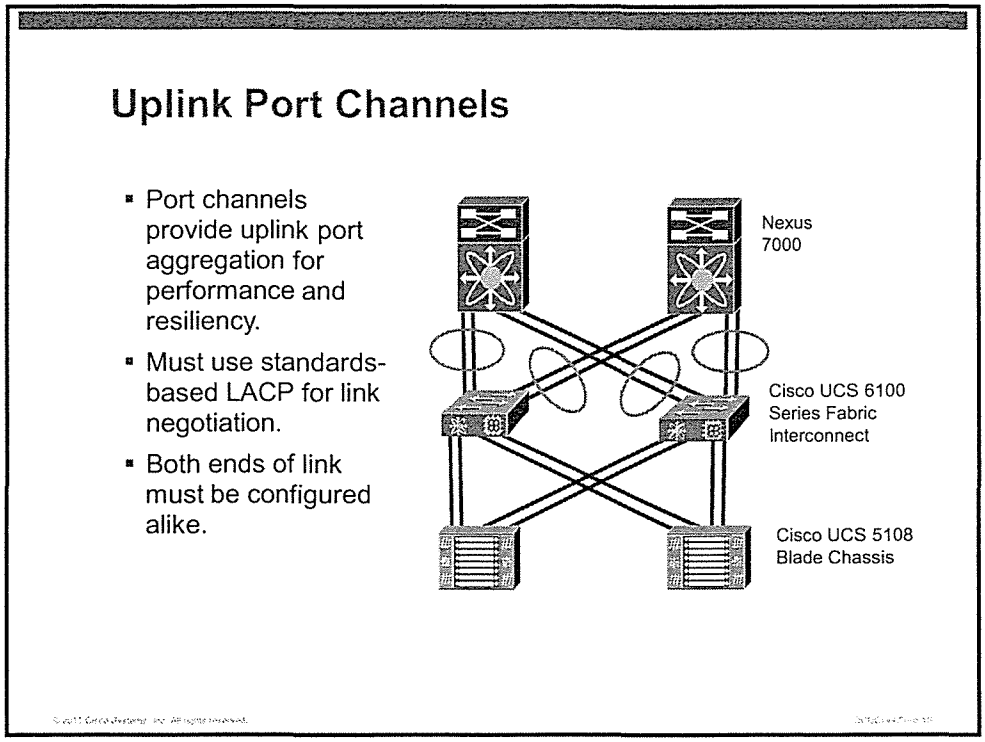
Beginning in Cisco UCS manager version 1.3, the first eight ports on the Cisco UCS 6120 Fabric Interconnect and the first 16 ports on a UCS 6140 Fabric Interconnect can be set to 1 Gb/s. This capability is only available for uplink ports. The IOM ports can only operate at 10 Gb/s.

Operating at 1 Gb/s requires 1-Gb small form-factor pluggable (SFP) modules on each end of the link.

Requirements and Configuration of Port Channels from the Cisco UCS Fabric Interconnect to a Northbound Switch

This topic describes the requirements and configuration of port channels from the Cisco UCS fabric interconnect to a northbound switch.

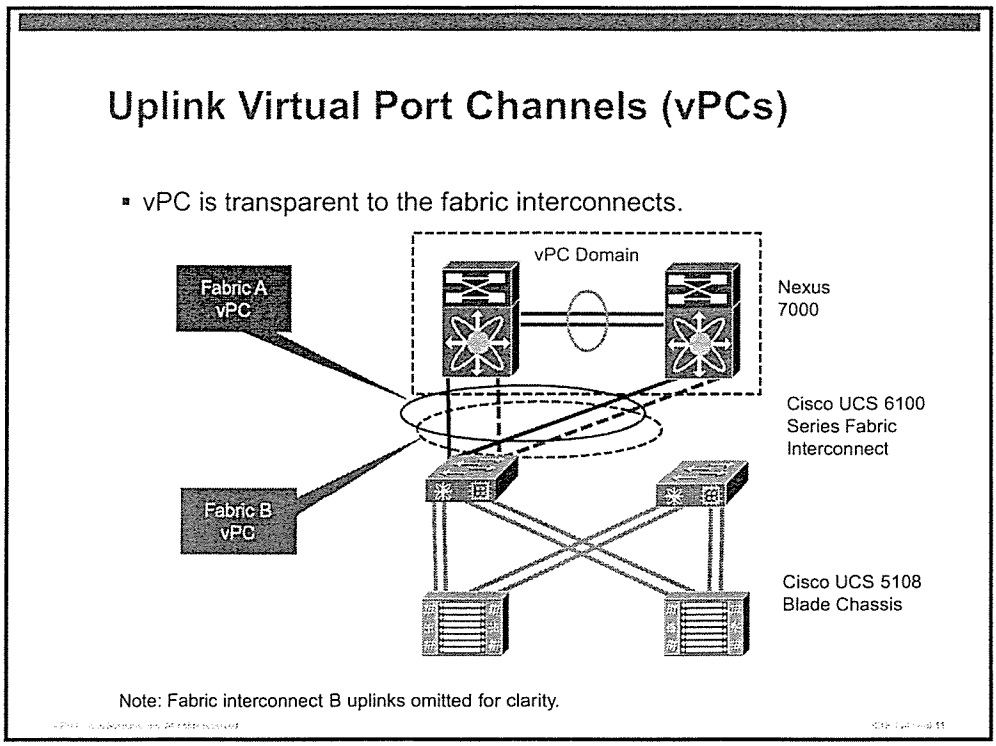
Uplink Port Channels



Port channels (sometimes referred to as EtherChannels) allow multiple links to be bonded into an aggregation channel. Not only does this bonding increase the available bandwidth of the uplink, it is no longer a single point of failure.

The fabric interconnect offers the standards-based Link Aggregation Control Protocol (LACP) to negotiate the link with its peer switch. Both ends of all links must be configured correctly.

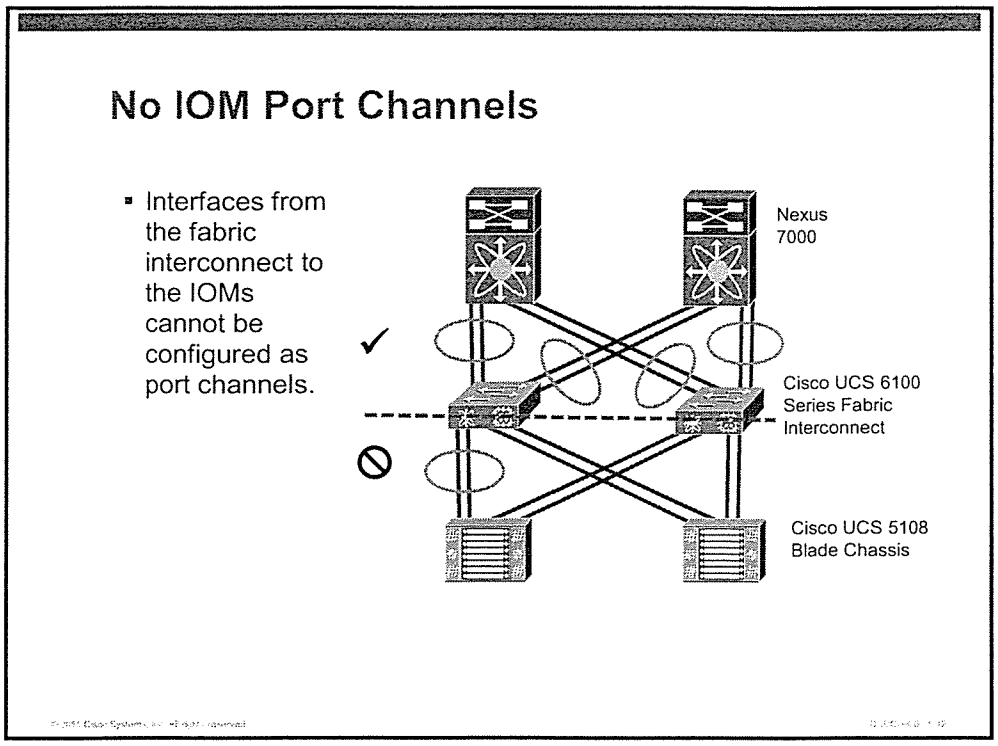
Uplink Virtual Port Channels (vPCs)



Normally, all links in a port channel must terminate on the same switch. The Nexus 7000 Series Switches support a feature called virtual port channel (vPC). vPC allows for bandwidth aggregation like a traditional port channel, but adds the benefit of a redundant path without the need to run Spanning Tree Protocol. Spanning Tree recovery on path failure can be tuned as low as six seconds, but a port channel can recover in less than one second.

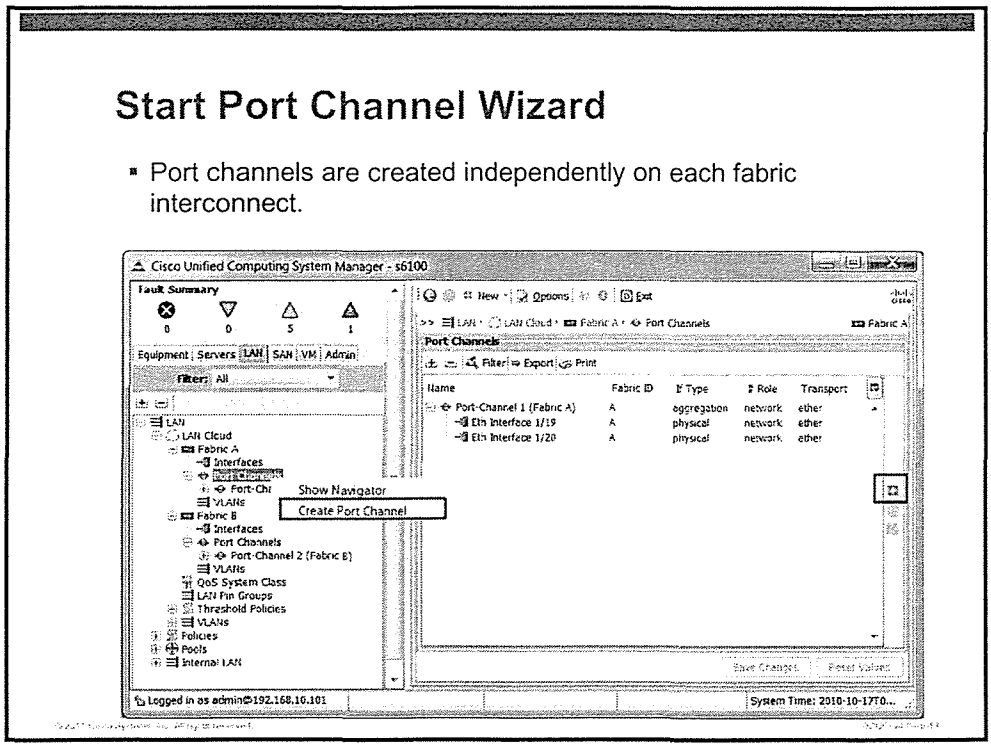
All vPC configuration is performed on the Nexus 7000 uplink switch. The fabric interconnect is unaware that the port channel is split between two switches.

No IOM Port Channels



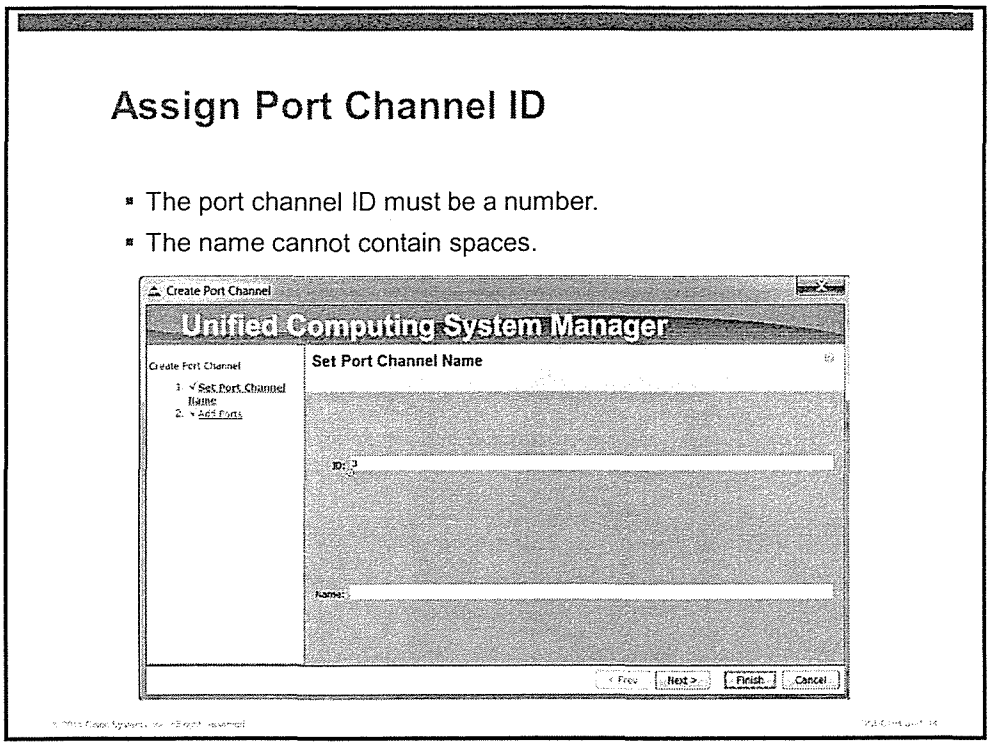
Any interface with the port state of "server" cannot become a member of a port channel unless the state is changed to "uplink." It is not possible to configure an IOM port channel.

Start Port Channel Wizard



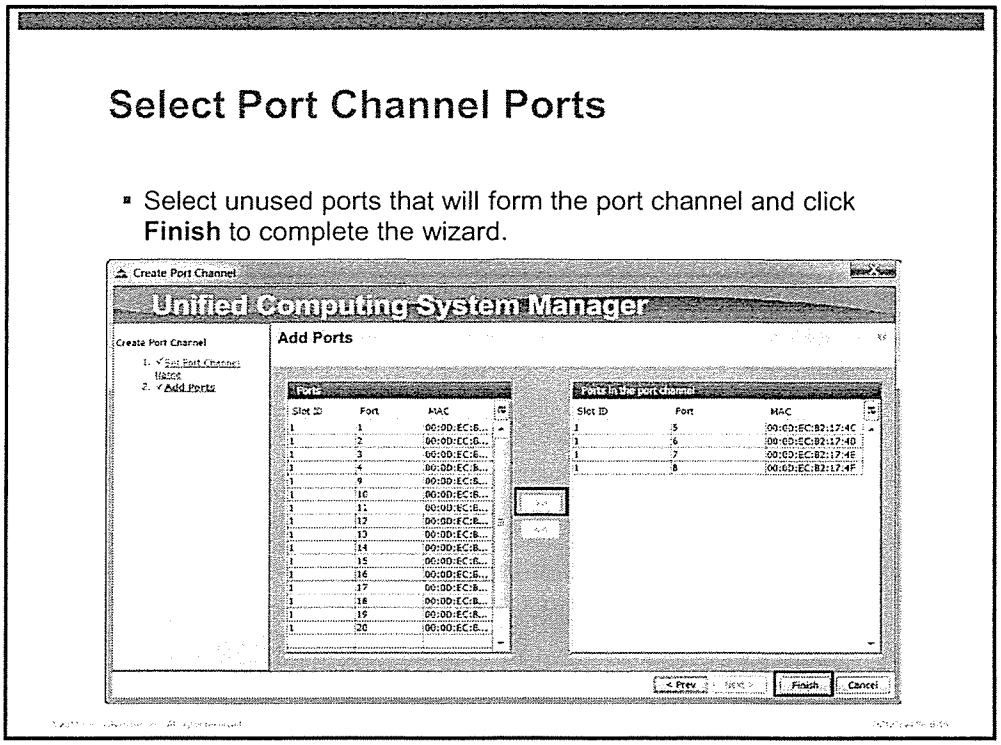
To start a port channel wizard, click the **LAN** tab in the navigation pane and expand one of the fabric interconnects. When you click port channels, you can either right-click to start the wizard or click the plus sign (+).

Assign Port Channel ID



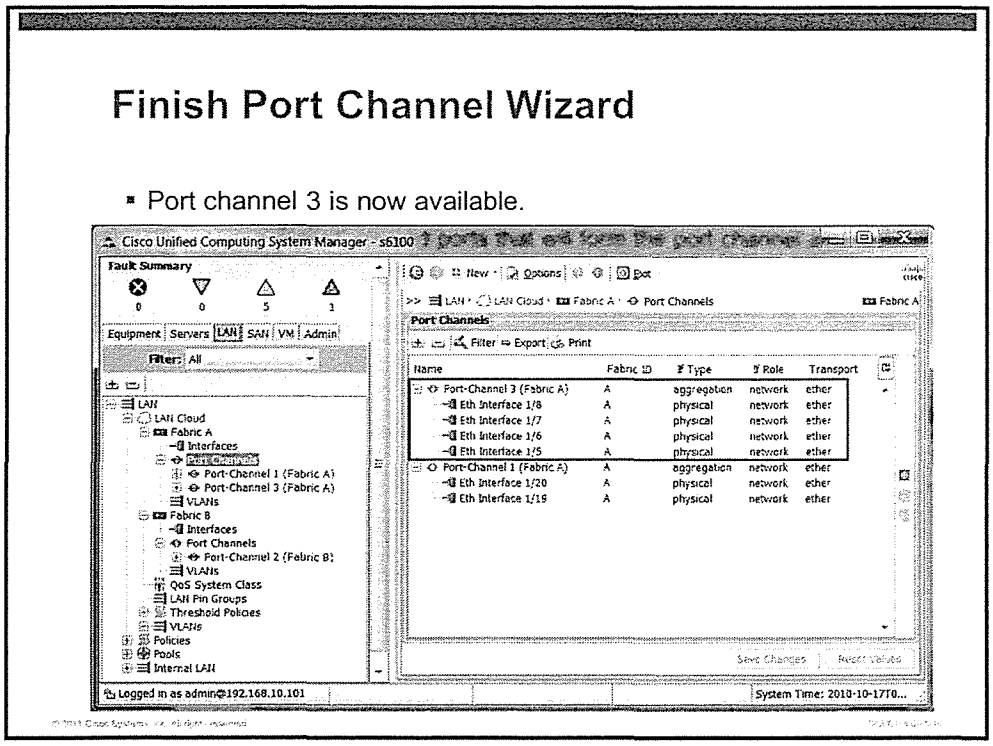
The first step in a port channel wizard is to assign a port channel ID to the new port channel. A port channel ID must be unique on that fabric interconnect. Optionally, a name can be assigned and associated with a port channel ID. The name cannot contain spaces.

Select Port Channel Ports



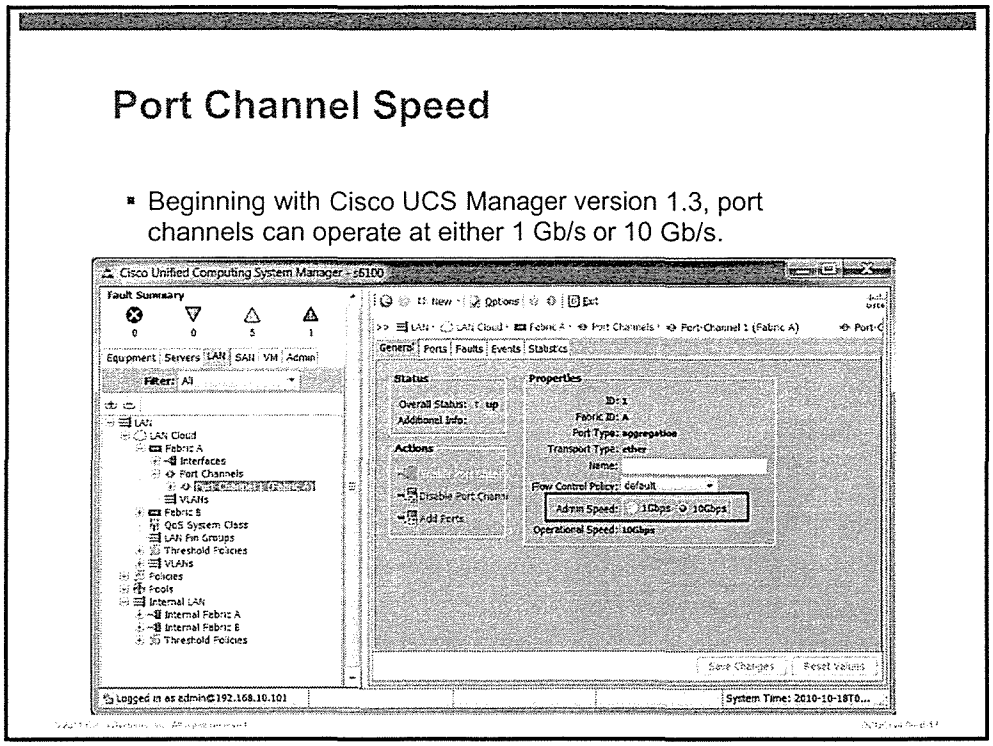
In the left portion of the window, select the interfaces that should participate in a port channel. Click the double right-arrow button to move those interfaces into the new port channel. Click **Finish** in the lower-right corner of the dialog box to complete the port channel creation wizard.

Finish Port Channel Wizard



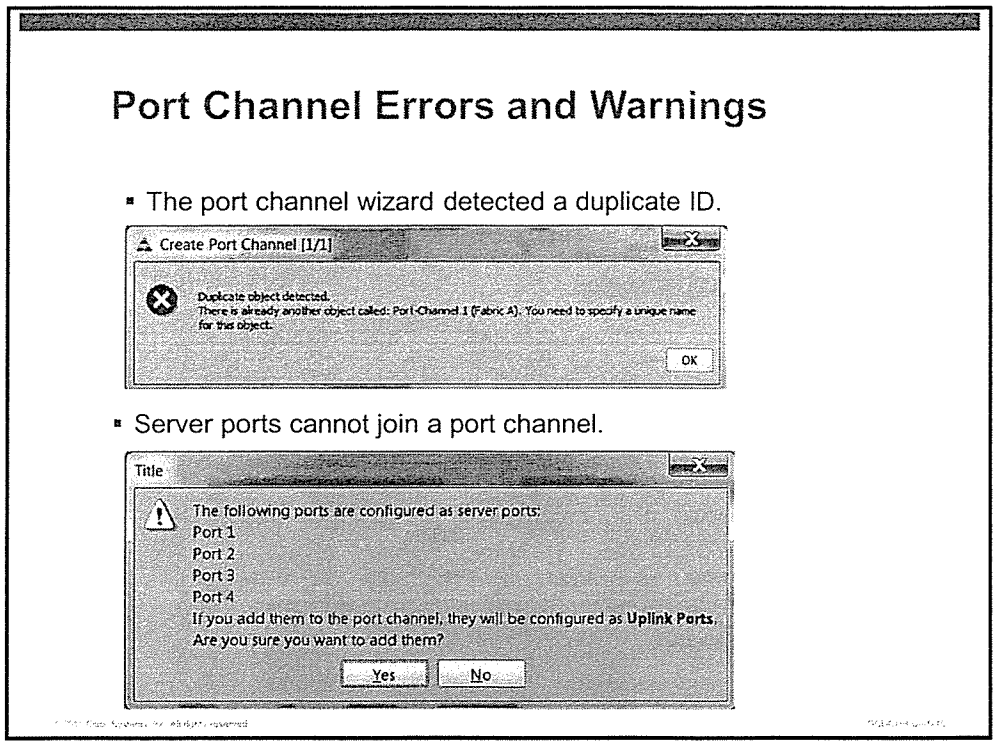
The new port channel now appears in the fabric interconnect inventory.

Port Channel Speed



In the LAN tab of the navigation window, click a configured port channel. In the General tab of the content pane, click one of the radio buttons to the right of Admin Speed to change port channel speed.

Port Channel Errors and Warnings

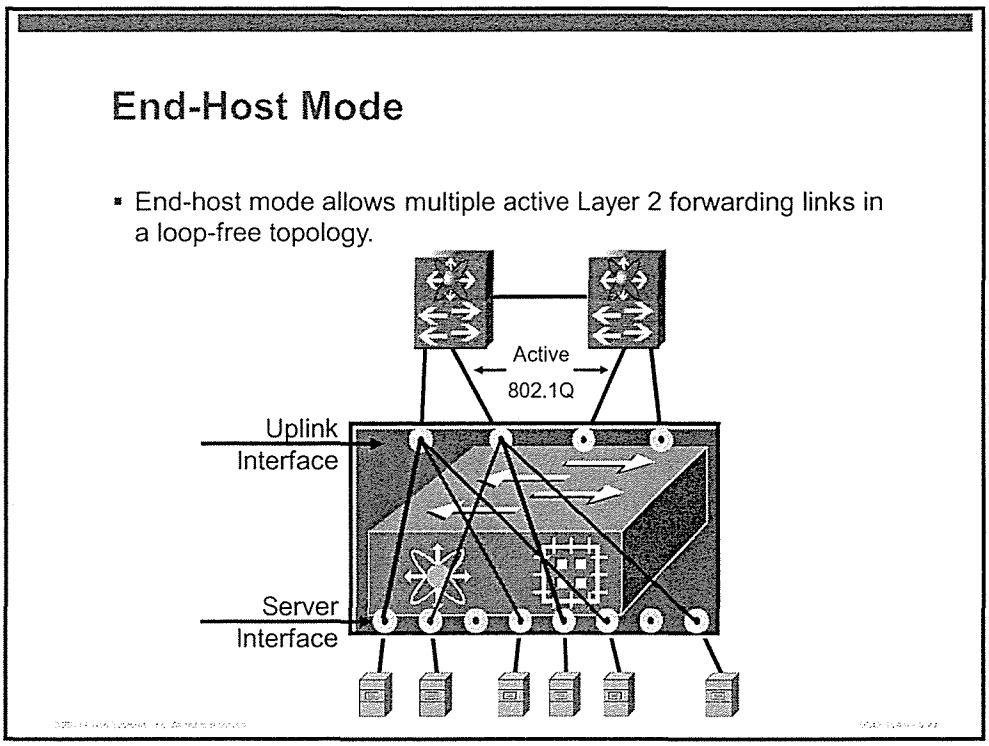


The port channel wizard includes logic to prevent duplicate port channel IDs. It also warns you that server links will be converted to uplinks before they can become members of a port channel.

End-Host Mode

This topic describes the features of end-host mode and its importance in forwarding over multiple Layer 2 links and maintaining a loop-free topology.

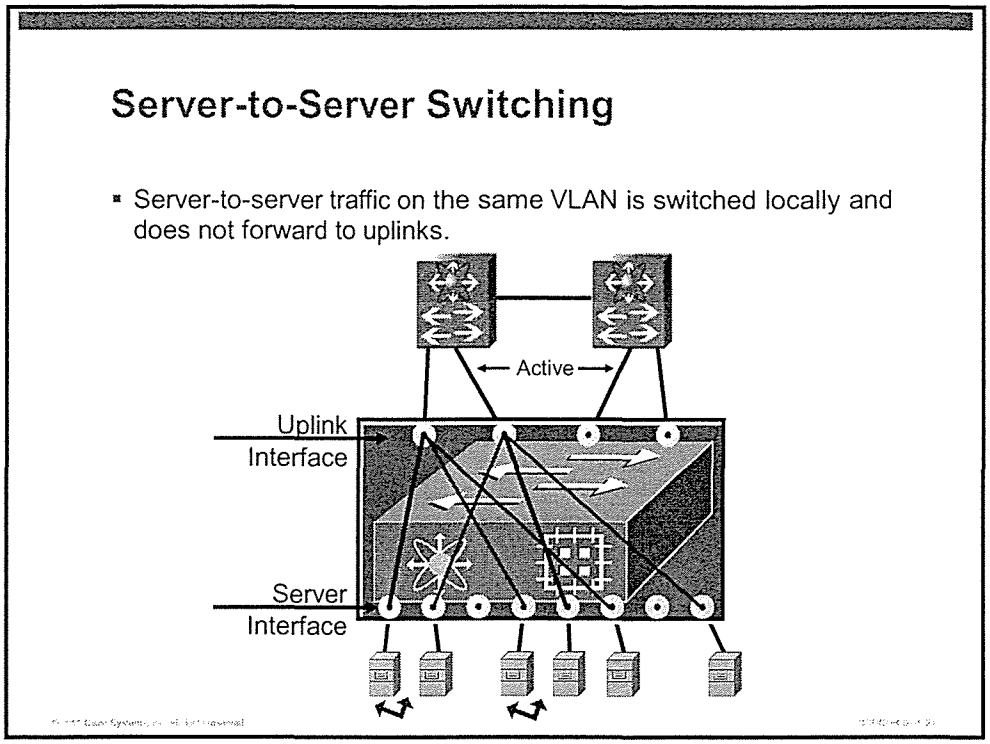
End-Host Mode



End-host mode, or end-host virtualizer (EHV), presents a link to a northbound uplink switch as a host trunk. Because it is a host port, it is not subject to spanning tree blocking on the port. Server MAC addresses are pinned to an uplink and are persistent, except in the case of uplink failure. After a MAC address has been learned on the uplink ports of the northbound switch, the return path is always maintained. In this way, multiple active Layer 2 links can forward without creating a loop.

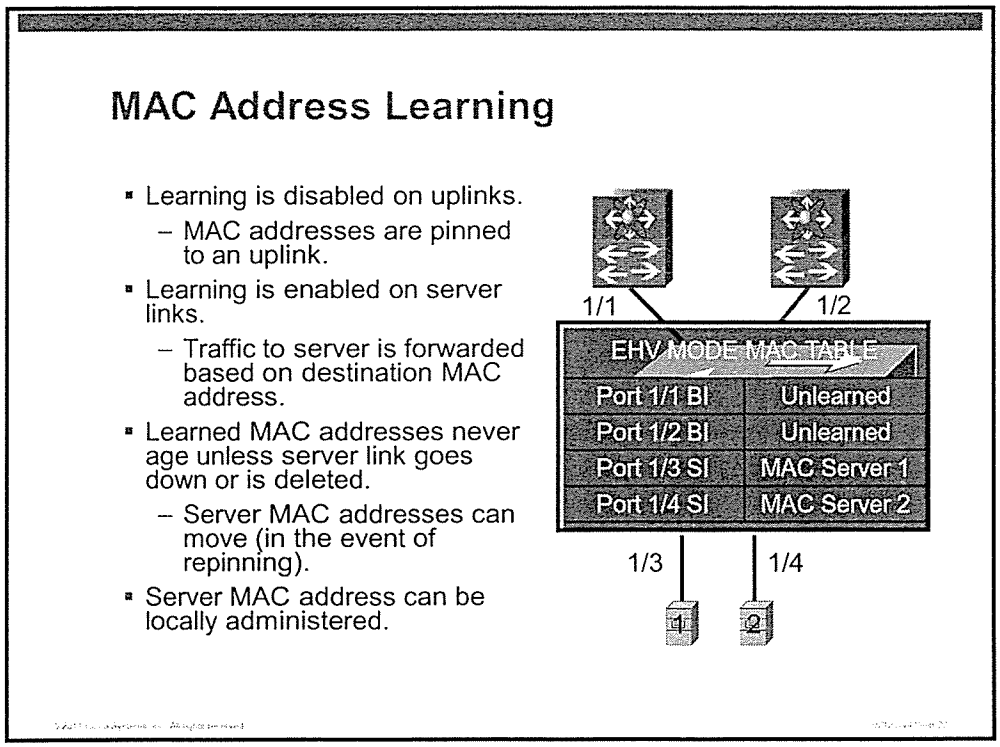
A port in EHV mode appears to the uplink switch as a host with many MAC addresses.

Server-to-Server Switching



Server-to-server communications on a common VLAN are locally switched by the fabric interconnect. Server-to-server communications across Layer 3 boundaries must be sent up an uplink port to a northbound switch to be routed to the correct VLAN.

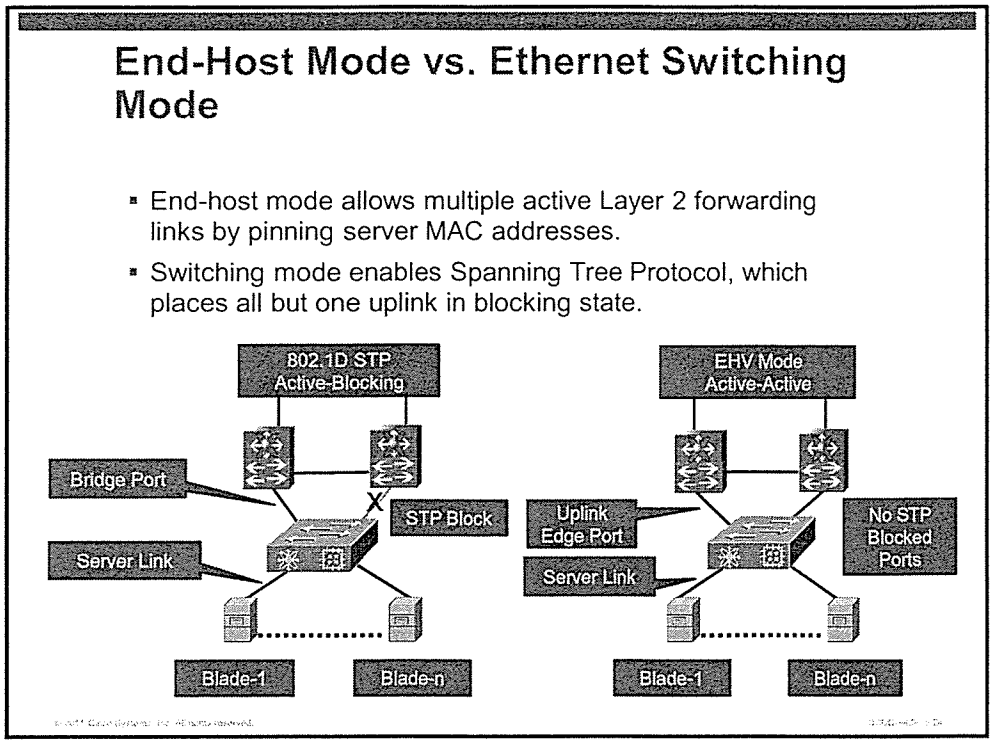
MAC Address Learning



A key concept in EHV mode is that a MAC forwarding table (in the traditional Ethernet switching sense) is not used to forward traffic to the uplink switch. Instead, a new server MAC address becomes associated with one uplink. All subsequent communications from that MAC address will be forwarded to the uplink to which it was pinned. A MAC address forwarding table is maintained only for server-to-server communications on the same VLAN.

End-Host Mode vs. Switched Mode

This topic compares the operation of the EHV mode and the Ethernet switching mode.

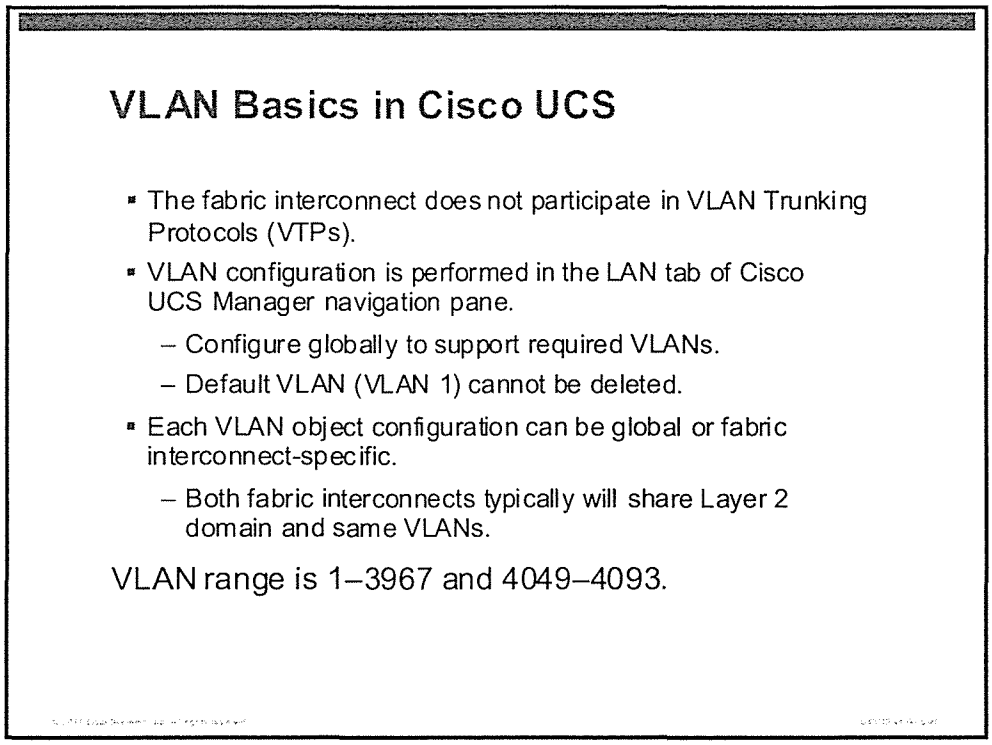


Although the fabric interconnects are capable of operating in Ethernet switching mode, default EHV mode is the preferred mode of operation. In Ethernet switching mode, the fabric interconnects must run Spanning Tree Protocol to maintain a loop-free topology. Spanning Tree Protocol will place all but one redundant uplink into blocking mode, which places constraints on uplink bandwidth and delays recovery from path failures. In EHV mode, a loop-free topology is maintained by pinning server MAC addresses to one particular uplink. In this way, all uplinks are actively forwarding traffic.

Requirements for Configuring VLANs in Cisco UCS Manager

This topic discusses the configuration of VLANs in Cisco UCS Manager.

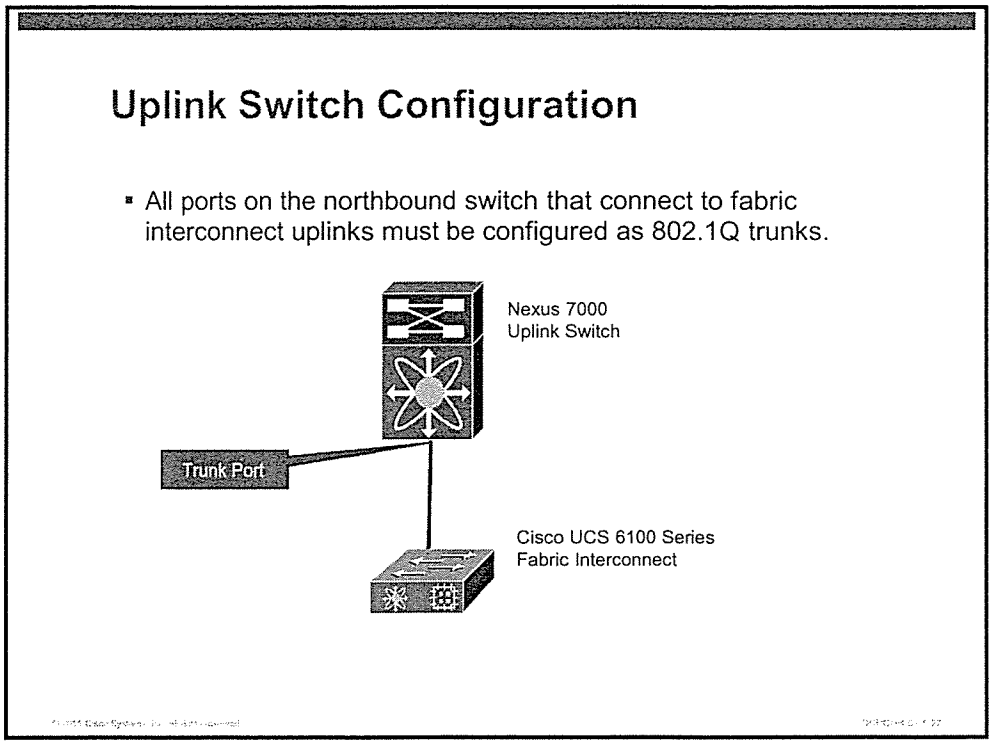
VLAN Basics in Cisco UCS



Although all uplinks from the fabric interconnect to the northbound switch are 802.1Q trunks, no virtual trunking protocol is employed. Therefore, the fabric interconnect requires manual configuration of VLANs.

Note	Cisco UCS Manager reserves VLANs 3968 to 4048 and 4094 for system use.

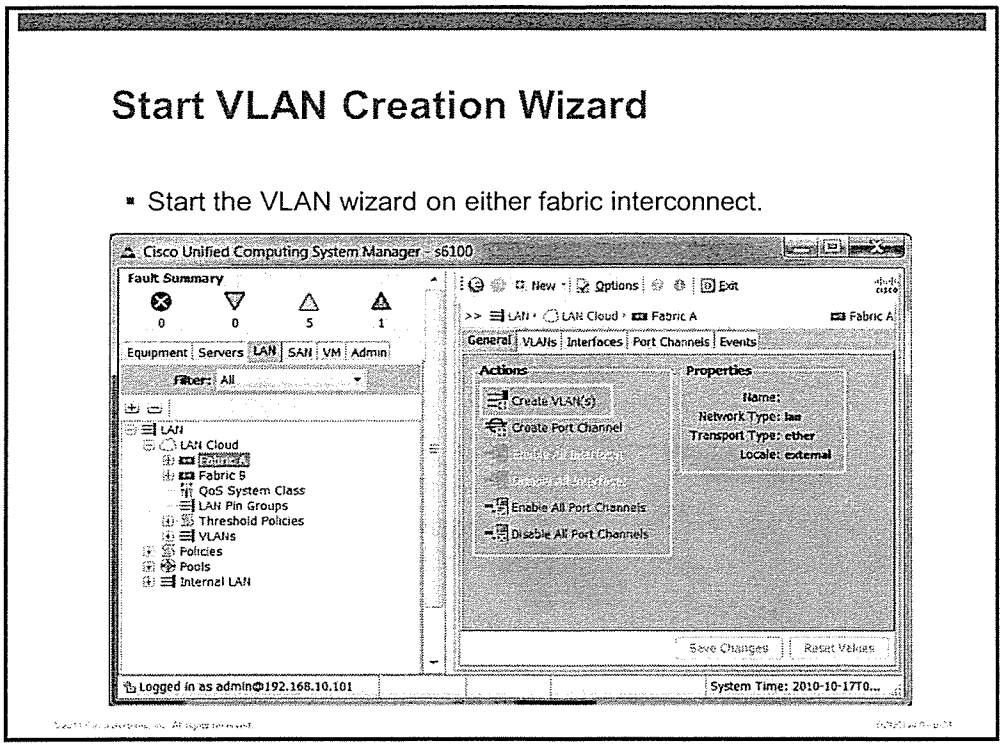
Uplink Switch Configuration



Because uplink ports on the fabric interconnects are always trunk ports, the northbound port on the uplink switch must also be configured as a trunk port. It is considered a best practice to limit the allowed VLANs on the northbound switch to the VLANs that are required by Cisco UCS.

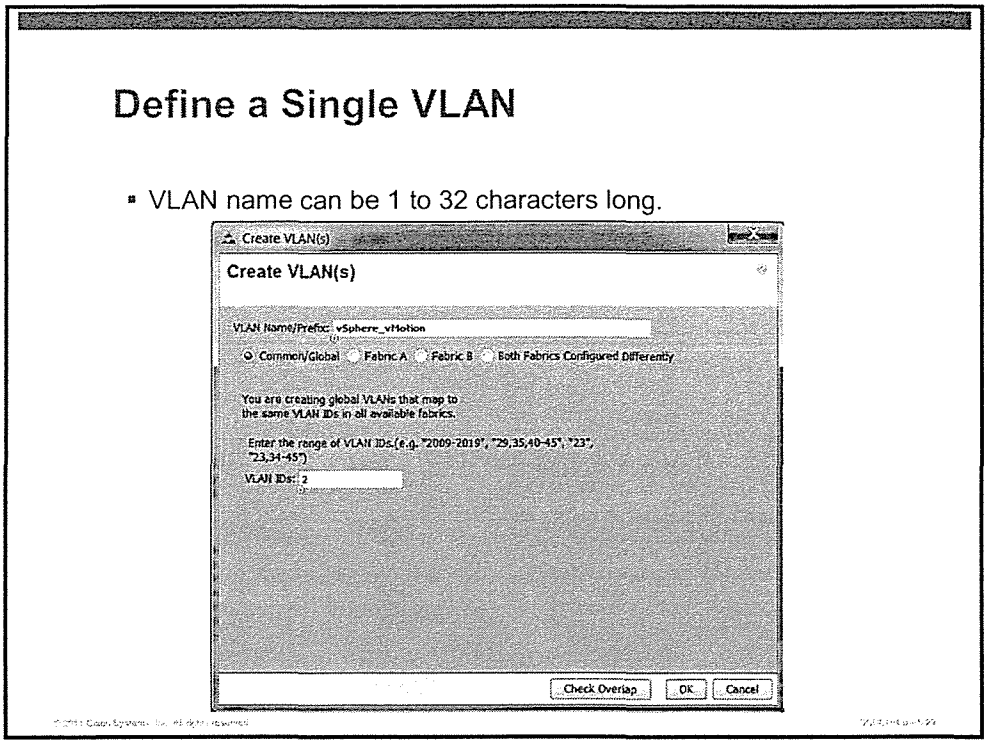
Cisco UCS Manager dynamically updates the allowed VLAN list on fabric interconnect uplinks anytime that a VLAN is created, modified, or deleted.

Start VLAN Creation Wizard



To start the VLAN creation wizard, click either of the fabric interconnects in the LAN tab of the navigation pane. Then, click the **Create VLANs** link in the content pane.

Define a Single VLAN

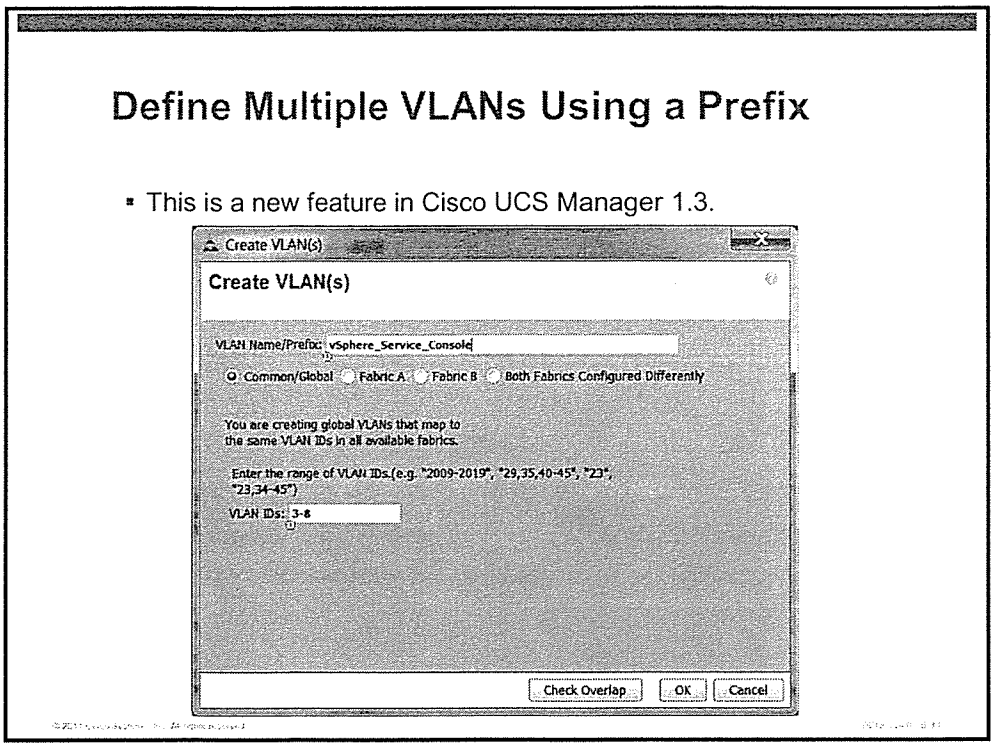


In Cisco UCS, VLANs require a name and a VLAN number. VLAN names are always used in the creation of vNIC profiles. This abstraction of the VLAN number allows you to change a VLAN associated with the VLAN names without requiring configuration changes to the server.

Click the **Check Overlap** button to verify that the VLAN number is not already defined.

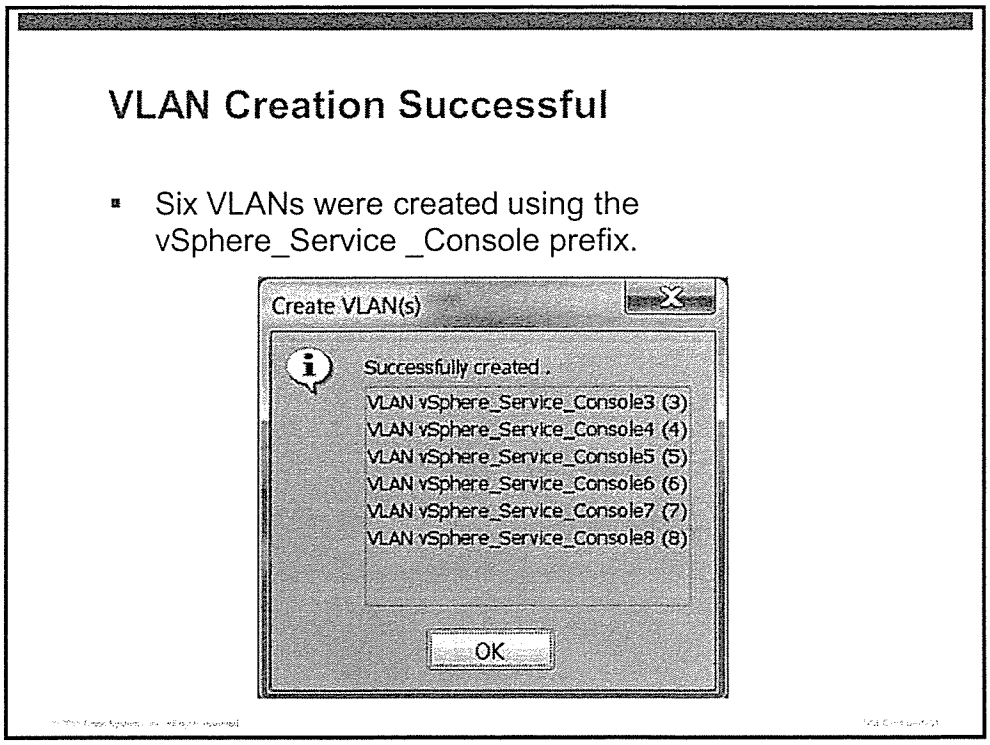
When you click the **Common/Global** radio button for VLAN creation, the VLAN name and number will be created on both fabric interconnects. This is the most common selection.

Define Multiple VLANs Using a Prefix



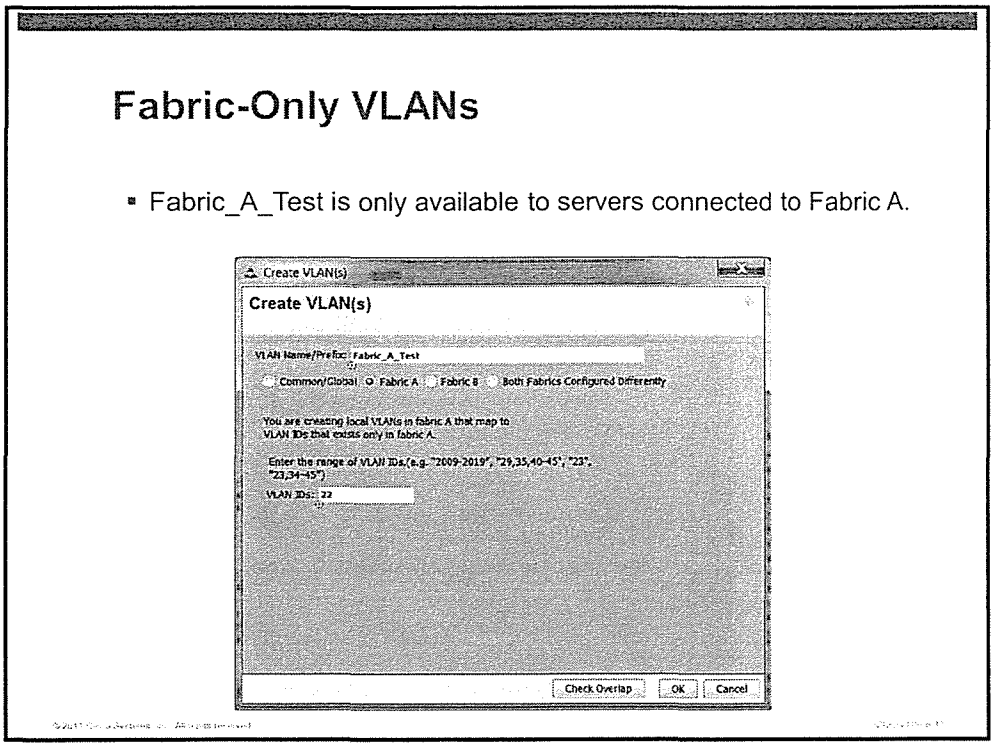
Beginning in Cisco UCS Manager version 1.3, you can automate the creation of VLANs by supplying a name prefix and a range of VLAN numbers. In the example, six VLANs will be created.

VLAN Creation Successful



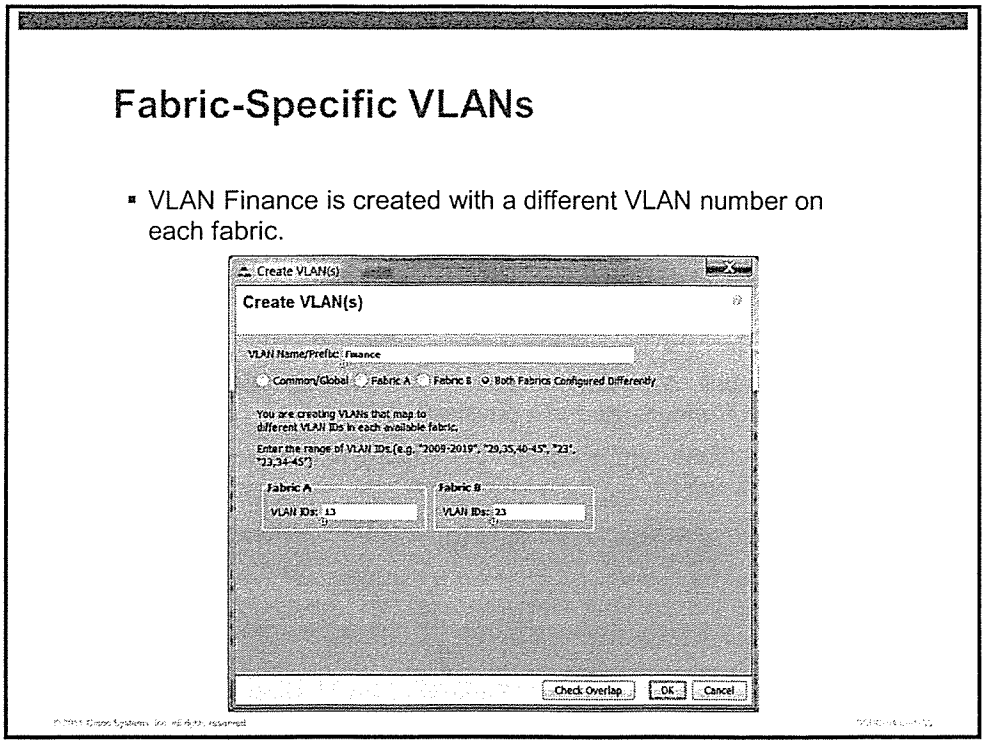
The dialog box in the figure indicates that the VLAN creation wizard successfully created six new VLANs based on the supplied prefix.

Fabric-Only VLANs



Fabric-only VLANs can be created if desired. In the example, VLAN 22 will be created only on fabric interconnect A. Because this VLAN exists on only one fabric, fabric failover will not be available for this VLAN.

Fabric-Specific VLANs

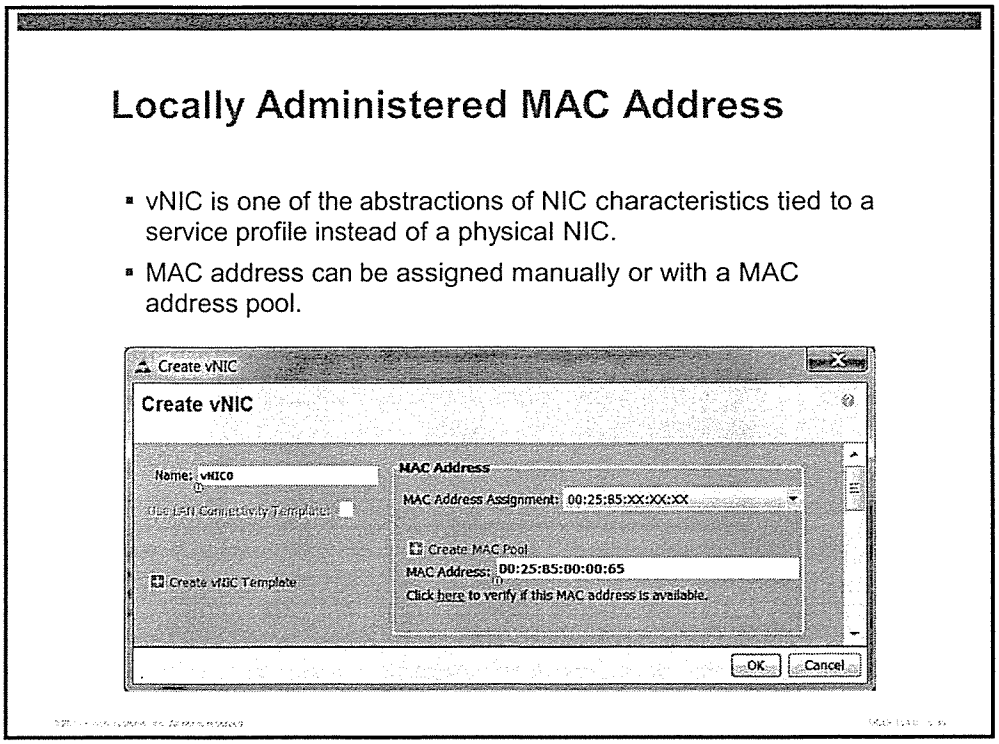


Fabric-specific VLANs can also be created if desired. In the example, the Finance VLAN will be bound to VLAN 13 on fabric A. It also will be bound to VLAN 23 and fabric B. This configuration might be required if an IP subnet was configured in different VLANs on the two uplink switches. Fabric failover is supported in this configuration.

Role of the vNIC in Abstracting MAC Addresses

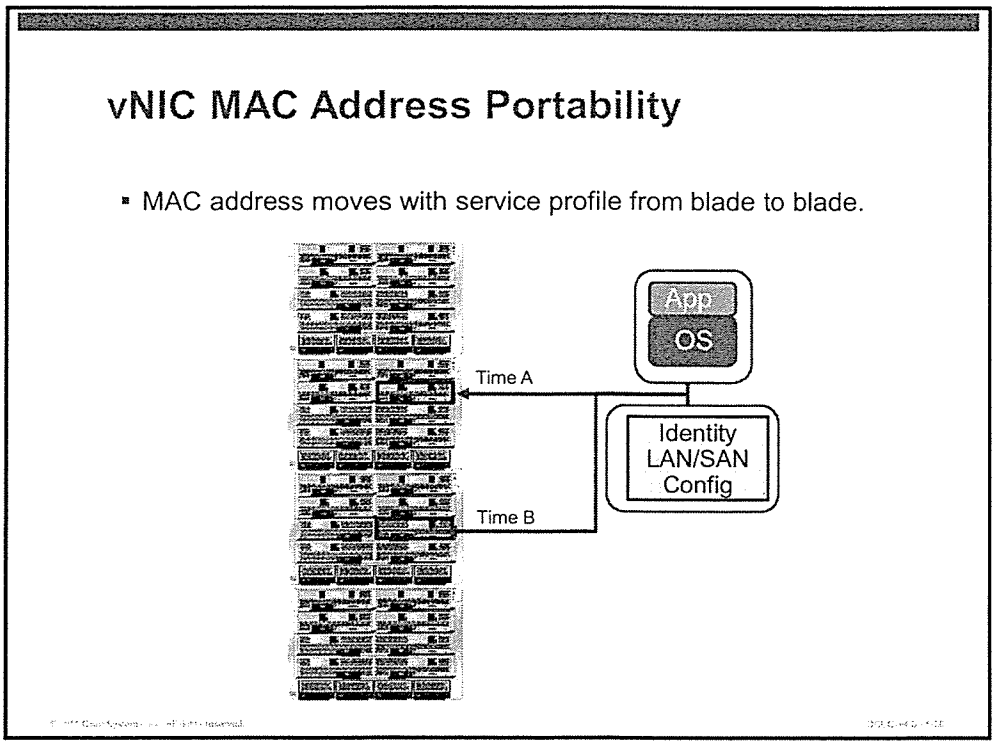
This topic discusses the role of the vNIC in the abstraction of MAC addresses from the hardware into a service profile.

Locally Administered MAC Address



Locally administered MAC addresses are identity resources that can be virtualized and abstracted from hardware into a Cisco UCS service profile. Stateless computing is a cornerstone value of Cisco UCS. Cisco UCS administrators have the option of manually configuring the MAC address based on the Cisco-supplied prefix, using an identity pool or the burned-in address.

vNIC MAC Address Portability

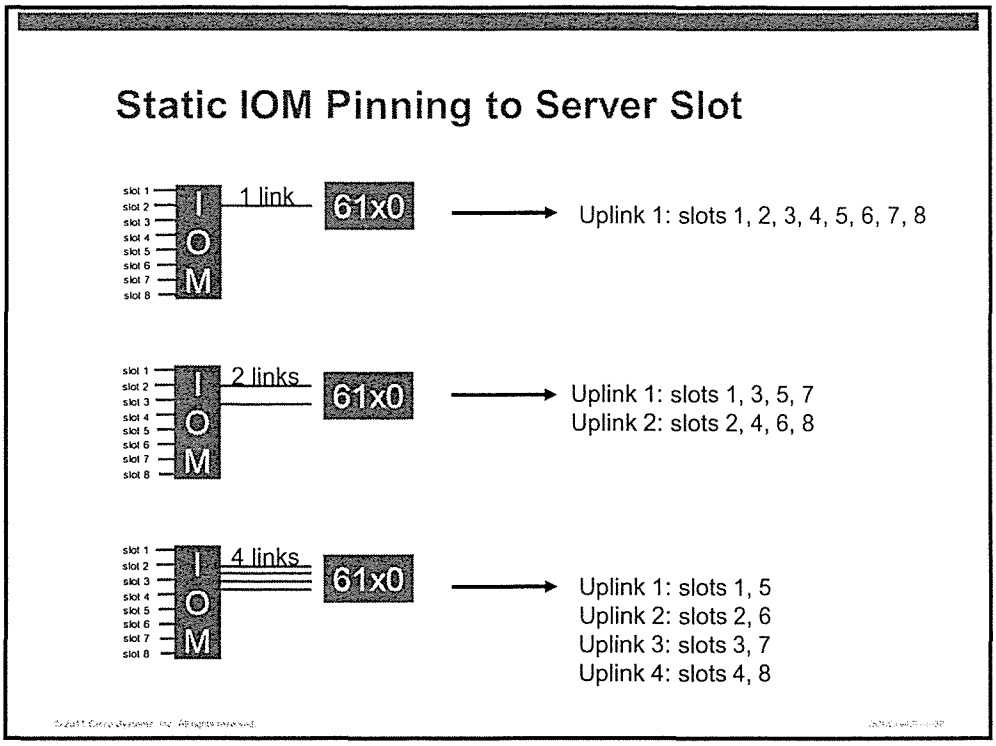


The main benefit of virtualizing the MAC address is that if the underlying server hardware fails, a service profile is simply moved to a replacement server. When the operating system boots on the new server, the MAC address is unchanged. From the perspective of the operating system or hypervisor running on the blade server, it is on the same hardware from which it booted the last time.

Static IOM Pinning and Recovery from Failure

This topic discusses static IOM pinning and recovery from link failure.

Static IOM Pinning to Server Slot

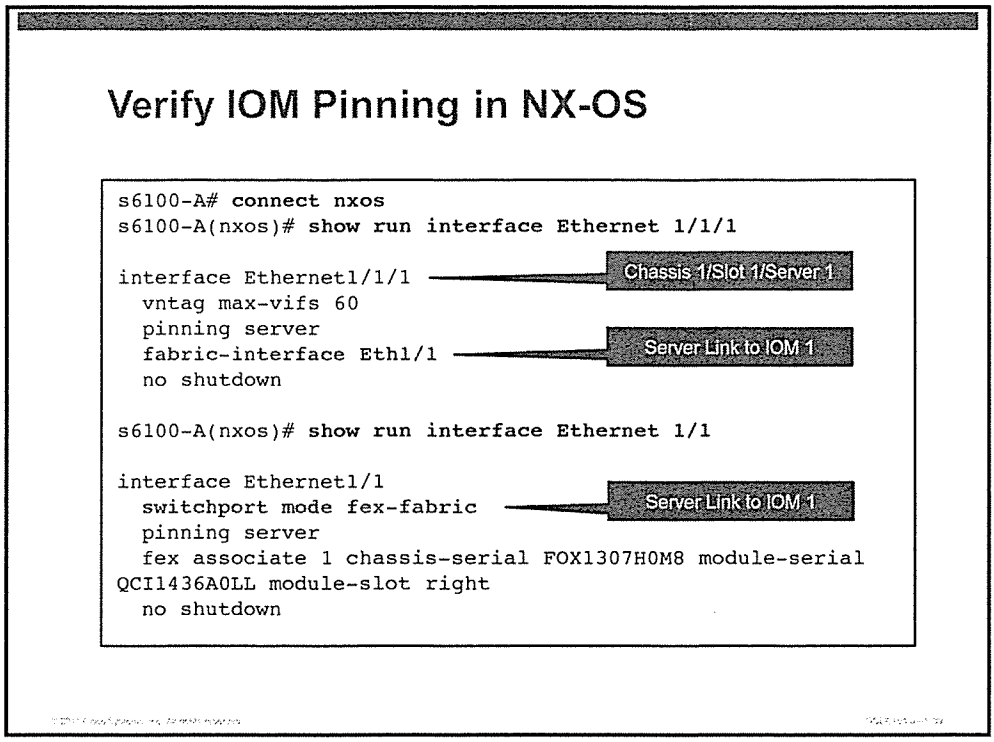


Cisco UCS Manager supports three IOM link topologies: 1 link, 2 links, and 4 links.

Each mezzanine card has one 10-Gb connection to the I/O multiplexer on fabric A and fabric B. A connection on each fabric is statically pinned to one of the four IOM server links to the fabric interconnect.

Number of Links	Server Pinning
1 link	Servers 1–8 are pinned to link 1.
2 links	Odd-numbered servers are pinned to link 1, and even-numbered servers are pinned to link 2.
4 links	Link 1: Servers 1 and 5 Link 2: Servers 2 and 6 Link 3: Servers 3 and 7 Link 4: Servers 4 and 8

Verify IOM Pinning in Cisco NX-OS

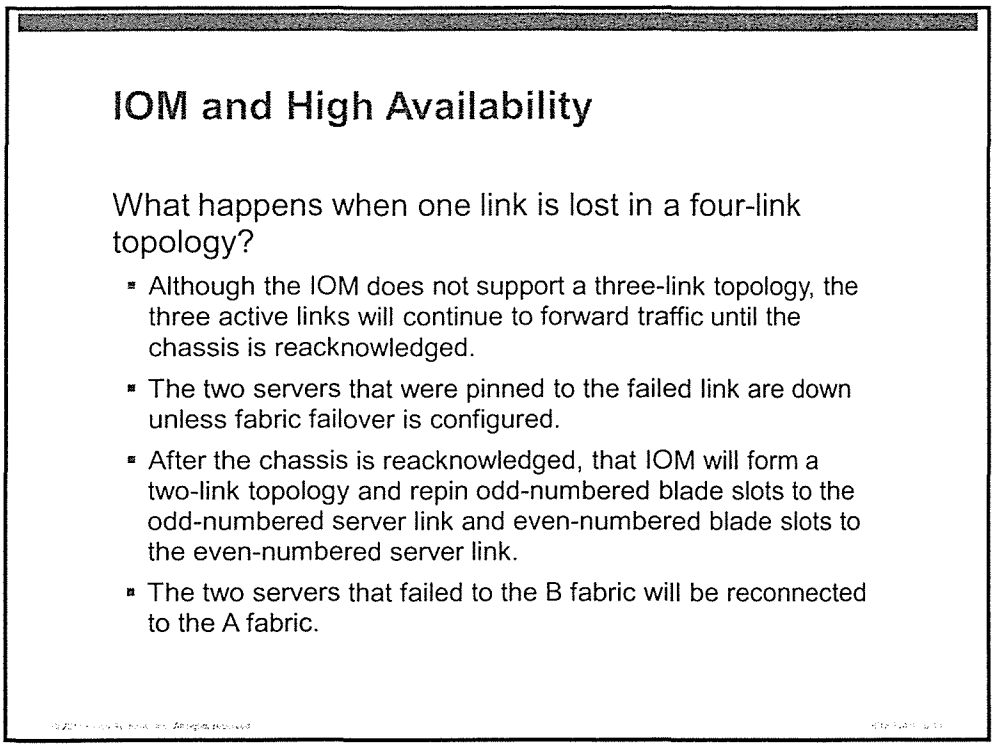


To validate static pinning from server blades to the IOM link, open the command-line interface (CLI) connection to one of the fabric interconnects and connect to the Cisco NX-OS shell. Fabric ports (server and uplink ports fixed in the chassis and expansion module) are numbered by slot number and port number. Port Ethernet 1/1 refers to port number one in the chassis. Ports and the expansion module are in slot 2, so port Ethernet 2/1 refers to the first port in the expansion module.

Each IOM has eight host ports. These are numbered in the format of chassis number/slot number/server number. The slot number refers to whether the port in question is a fixed configuration port (slot 1) or an expansion module port (slot 2). The server number is determined by which slot and Cisco UCS 5108 server chassis the server happens to occupy.

In the example, server 1 is in slot 1 of chassis 1 and the IOM is connected to slot 1 of the fabric interconnect (fixed port). Its fabric interface is indicated as Ethernet 1/1. That is the IOM link to which server 1 is pinned.

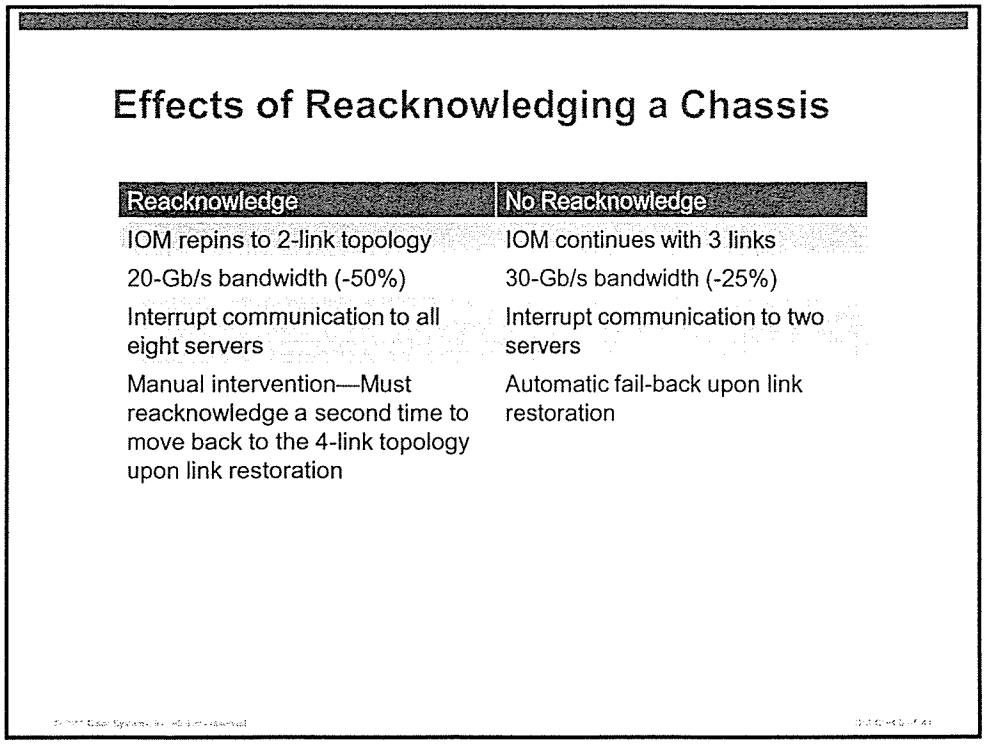
IOM and High Availability



When there is more than one IOM link to the fabric interconnect, failure of a link causes a loss of connectivity for servers that are associated with that link. If network interface card (NIC) teaming is configured in the operating system, or hardware-based failover is configured in the service profile, the affected servers will failover to their fabric B connection.

If no failover mechanism is configured for an impacted server, the server loses all connectivity. Upon link loss, the IOM does not automatically repin to a supported topology. You must manually reacknowledge the chassis for the IOM to repin.

Effects of Reacknowledging a Chassis

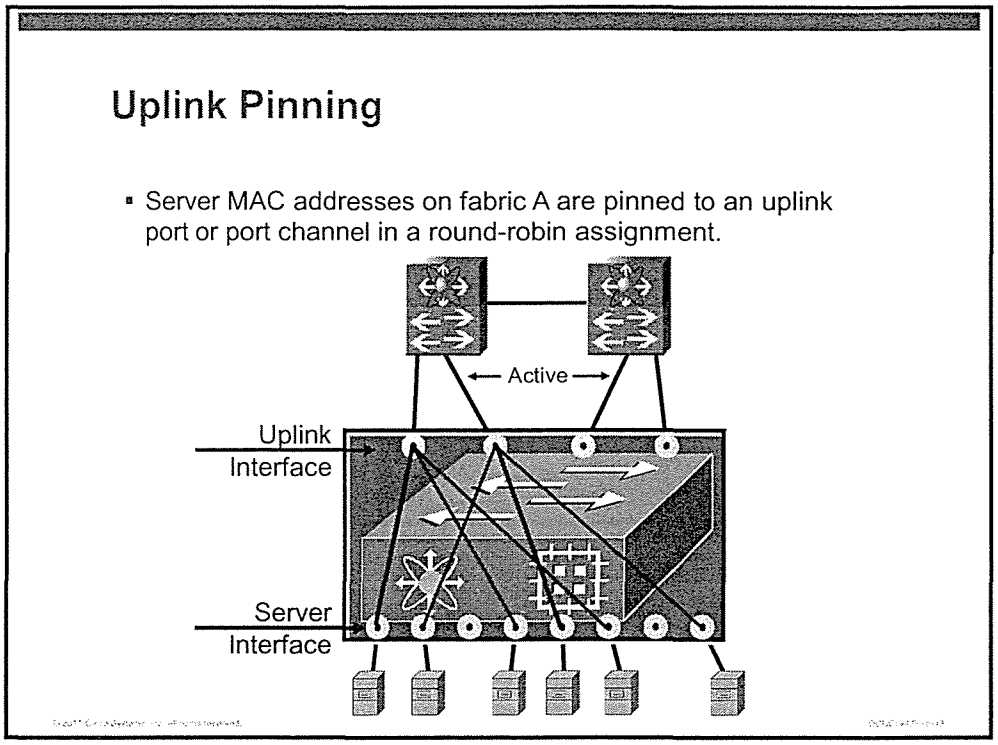


When an IOM link fails, it is important to consider carefully how to proceed. The general rule is if an IOM link goes down and the affected servers are not configured for fabric failover at the hardware or operating system level, the chassis should be reacknowledged. If the affected servers are configured for fabric failover, the chassis should not be reacknowledged. When the IOM link connectivity is restored, the servers that were impacted by the failure will fail back to their primary fabric.

Automatic Uplink Pinning and Recovery from Failure

This topic discusses the process of automatic pinning on uplink ports.

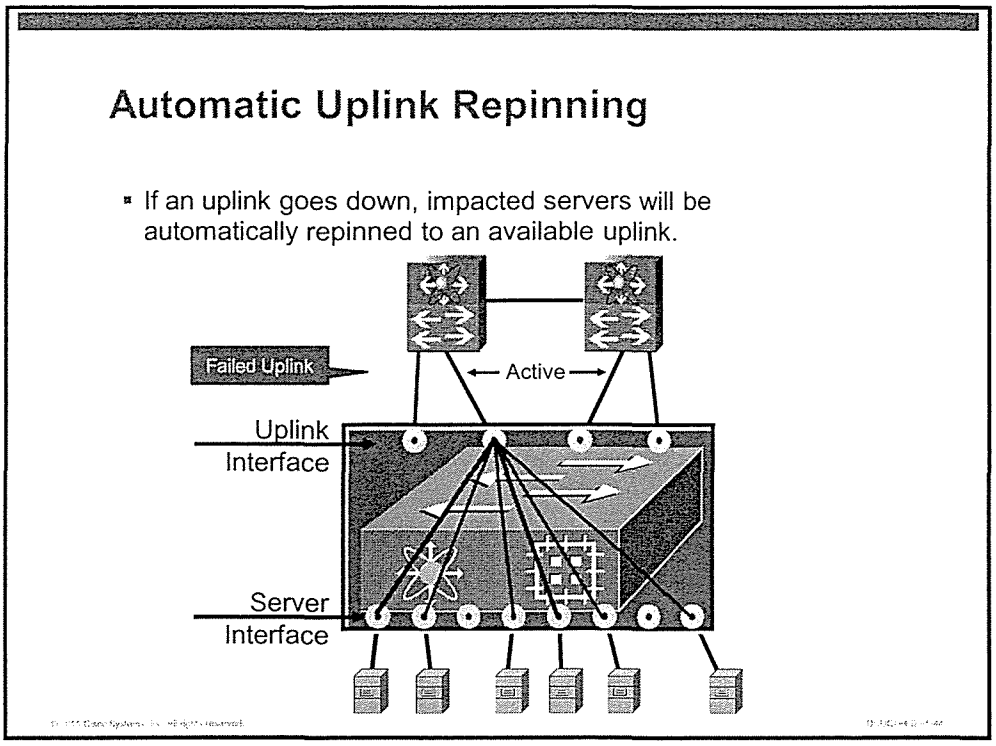
Uplink Pinning



It is important to understand the difference between IOM pinning and uplink pinning. IOM pinning is static and based on the number of links from the I/O module to the fabric interconnect.

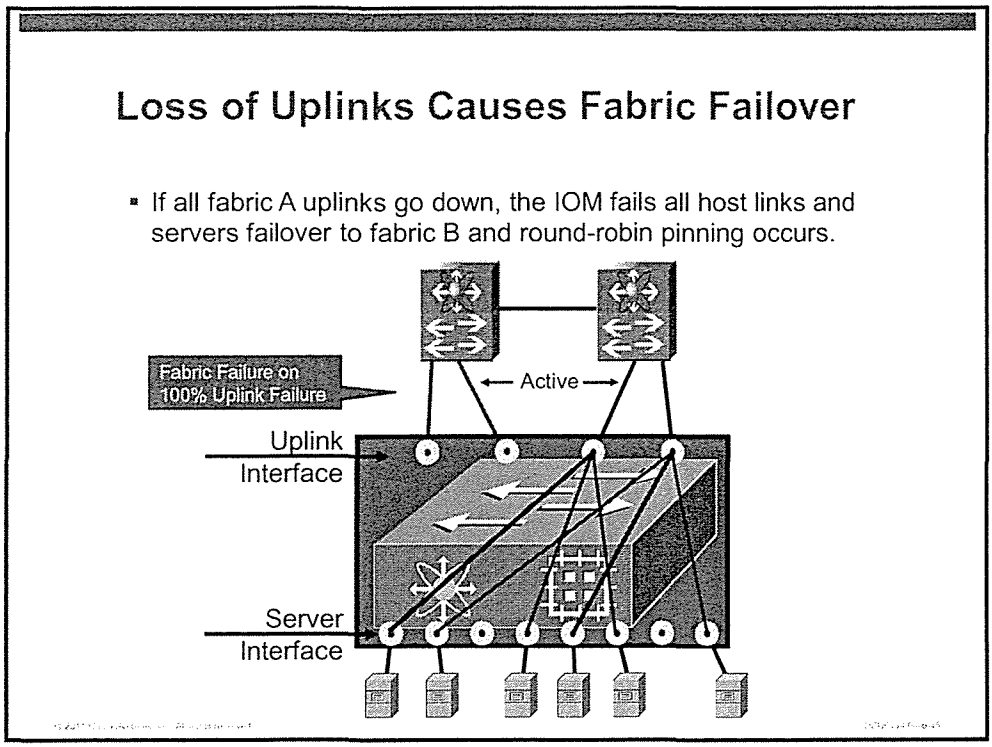
Recall from the discussion of end-host virtualization mode that a loop-free topology is assured by pinning MAC addresses to uplink ports. This pinning process can be either automatic or statically configured. By default, server MAC addresses are pinned to uplink interfaces in a round-robin process.

Automatic Uplink Repinning



With automatic uplink pinning, a link failure will cause all servers to be repinned to remaining uplinks. In the example, there are two uplinks on fabric A. When one of the links goes down, the server is simply repinned to the remaining uplink. The fabric interconnect will send a Gratuitous Address Resolution Protocol (GARP) to the northbound switch on behalf of the servers to announce them on the new port. The switch will update its MAC forwarding table to reflect the new interface.

Loss of Uplinks Causes Fabric Failover

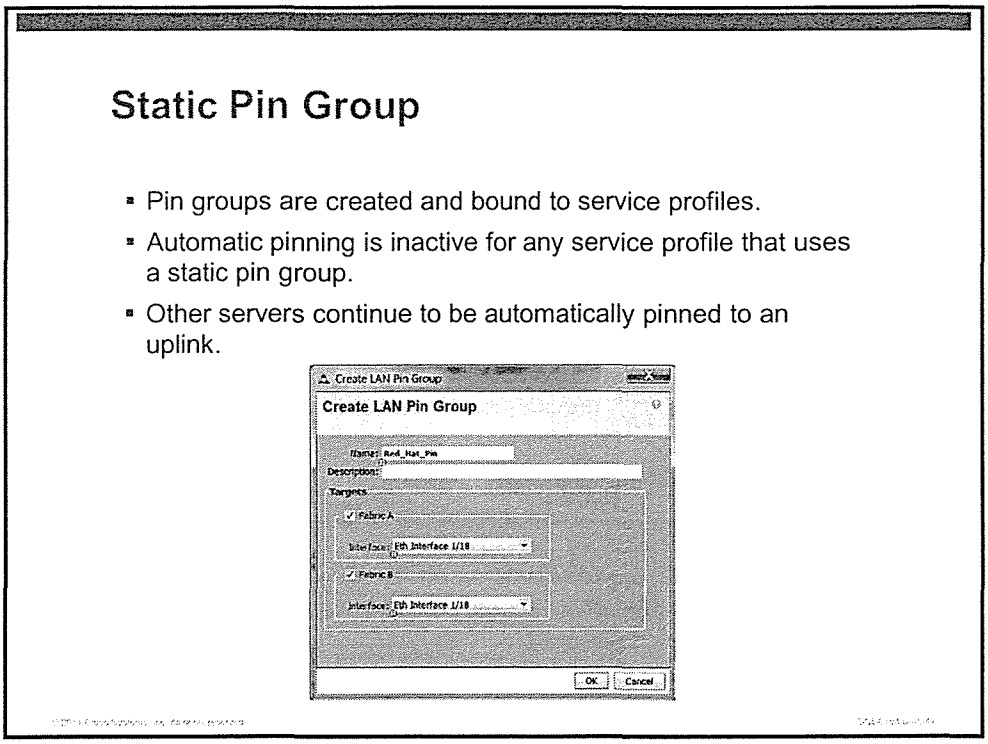


In the event all uplink ports on the fabric interconnect lose connectivity, the IOM instructs the I/O multiplexer (MUX) to shut down all eight of the host ports. The impacted servers will use either NIC teaming or hardware failover to re-establish connectivity on fabric B. If the servers are not configured for high availability in the operating system or service profile, they will be down until at least one uplink is restored on fabric A.

Configuration of Manual Uplink Pinning and Recovery from Failure

This topic discusses the configuration of static (manual) pinning.

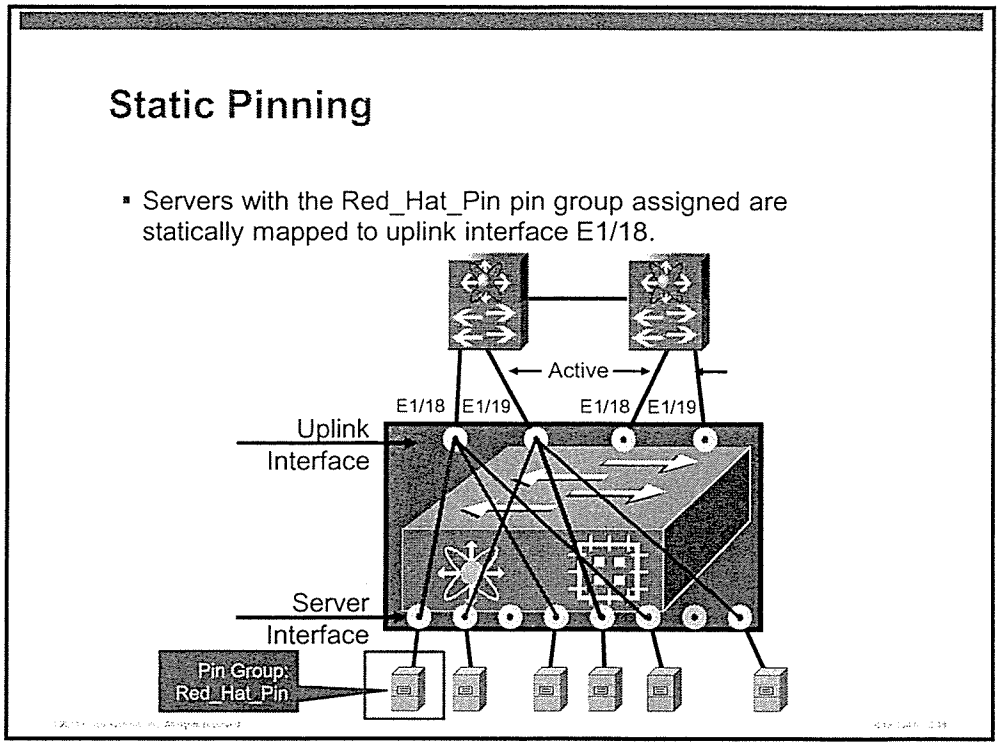
Static Pin Group



Pin groups are created under the LAN tab of the navigation pane. Pin groups are global policy elements and are replicated to the secondary management node.

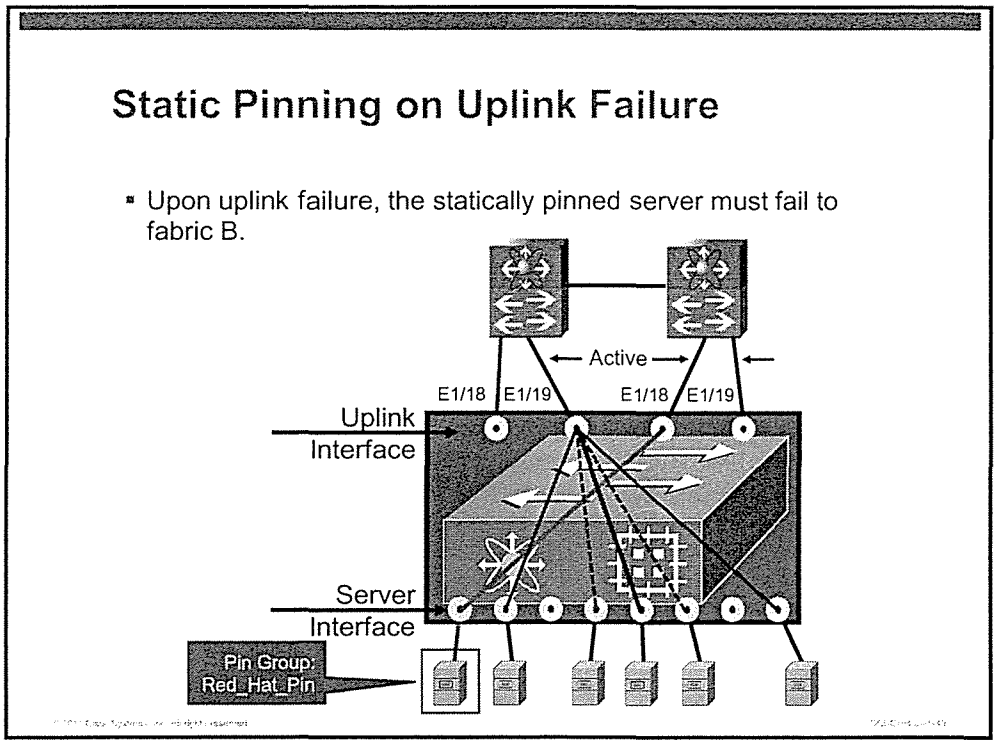
In this example, any service profile that includes this pin group policy will only use uplink Ethernet 1/18 on fabric A. If that uplink goes down, automatic repinning will not occur and the server will have to use fabric failover to re-establish connectivity on fabric B.

Static Pinning



In the illustration, the highlighted server is configured to use the static pin group called Red_Hat_Pin, which was just created. This server will always pin to uplink Ethernet 1/18 on fabric A, or Ethernet 1/18 on fabric B.

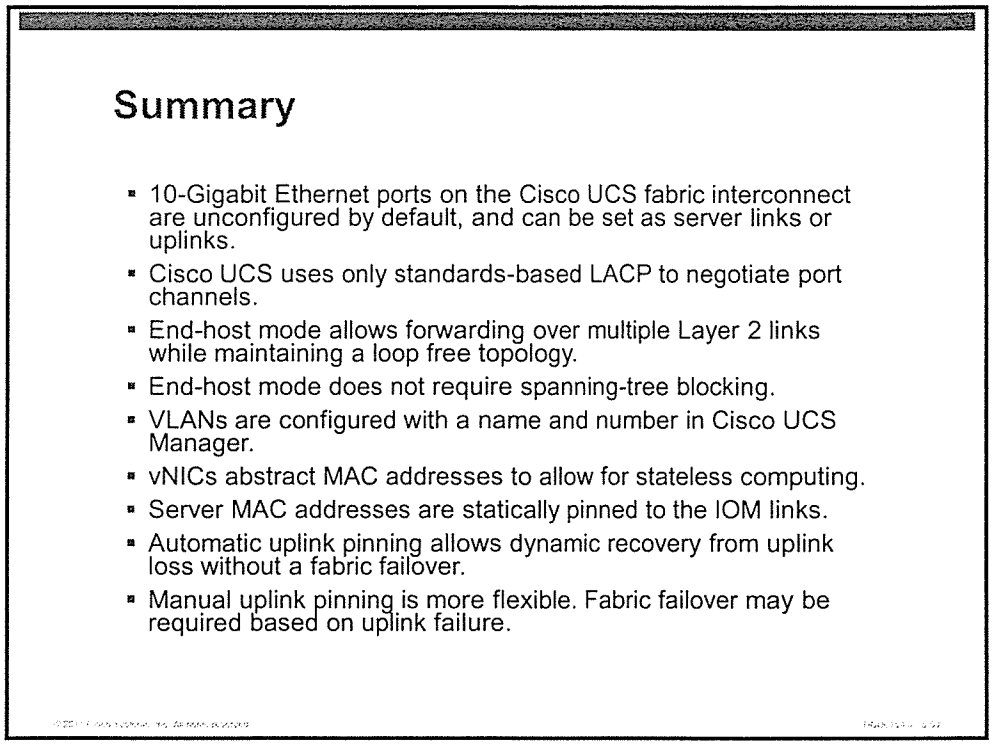
Static Pinning on Uplink Failure



When uplink Ethernet 1/18 fails, the server fails over to uplink Ethernet 1/18 on fabric B.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 4

Configuring Compute Node SAN Connectivity

Overview

Unified fabric is a major benefit of Cisco UCS, so you should understand how to integrate Fibre Channel SAN in the context of Fibre Channel over Ethernet (FCoE). After the virtual network interface card (vNIC) is configured and virtual LANs (VLANs) are established, the virtual host bus adapter (vHBA) is the second half of the FCoE solution.

Objectives

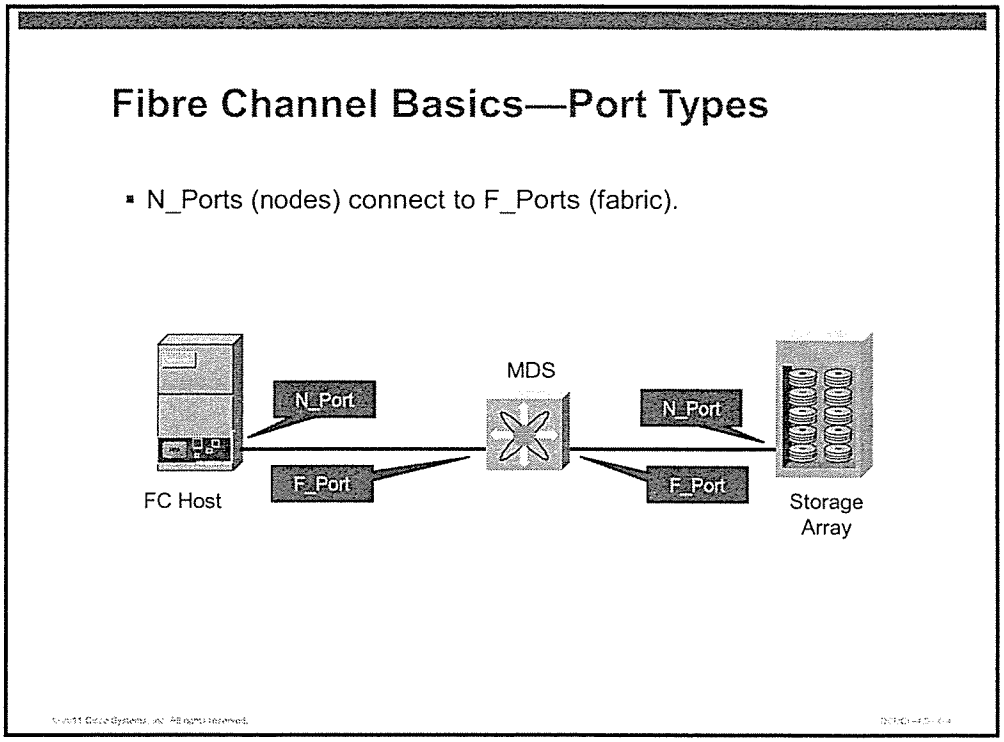
Upon completing this lesson, you will be able to describe the advantages of the Cisco N_Port Virtualization (NPV), describe basic Fibre Channel operation, and differentiate between automatic and static Fibre Channel uplink pinning. You also will understand how to configure VLANs and port channels. This ability includes being able to meet these objectives:

- Describe Fibre Channel switching
- Describe N_Port Virtualization
- Differentiate between benefits and drawbacks of Fibre Channel switching and NPV
- Describe how NPIV allows a single N_Port to be associated with multiple FC-IDs
- Describe the requirements and configuration of VSANs in Cisco UCS Manager
- Describe the role of the vHBAs to abstract WWNNs and WWPNs into a service profile
- Describe automatic uplink pinning and recovery from failure
- Describe the configuration of manual uplink pinning and recovery from failure

Fibre Channel Switching

This topic describes Fibre Channel basics.

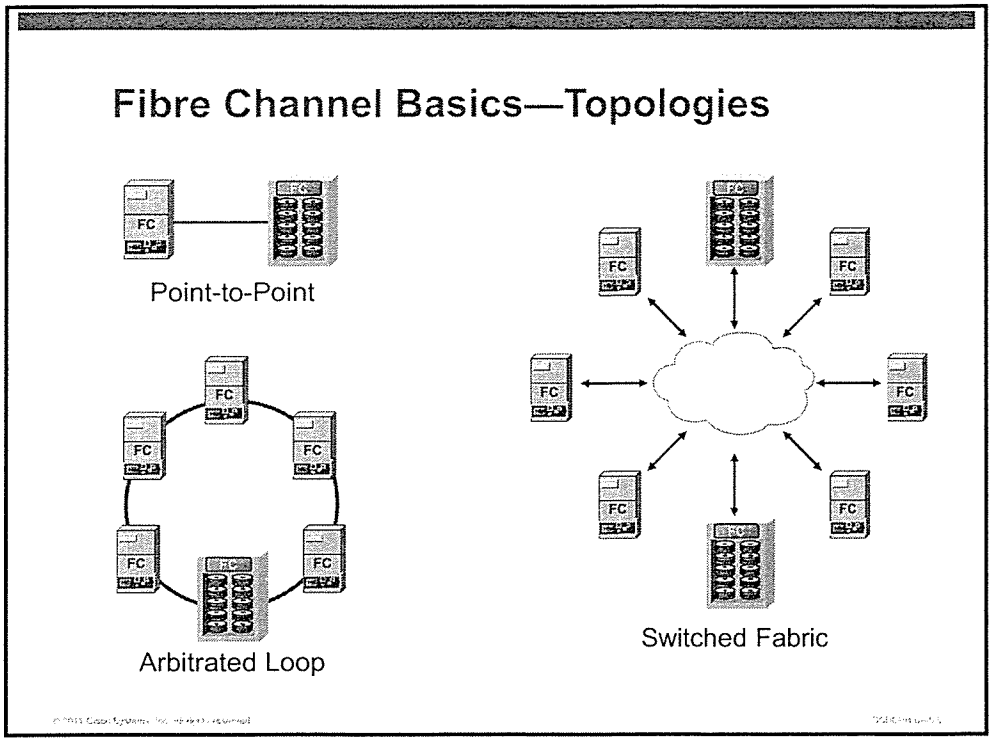
Fibre Channel Basics—Port Types



The Fibre Channel Protocol (FCP) defines a number of specialized port types. There are rules concerning which port types can connect to other port types.

FCP Port Type	Description	Connects to Which Type
N_Port	node (host) port	F_Port
NP_Port	node proxy (NPV Mode)	F_Port
F_Port	fabric port on Fibre Channel switch	N_Port, NP_Port
E_Port	expansion port (interswitch)	E_Port
TE_Port	trunking E_Port (Cisco only)	TE_Port

Fibre Channel Basics—Topologies



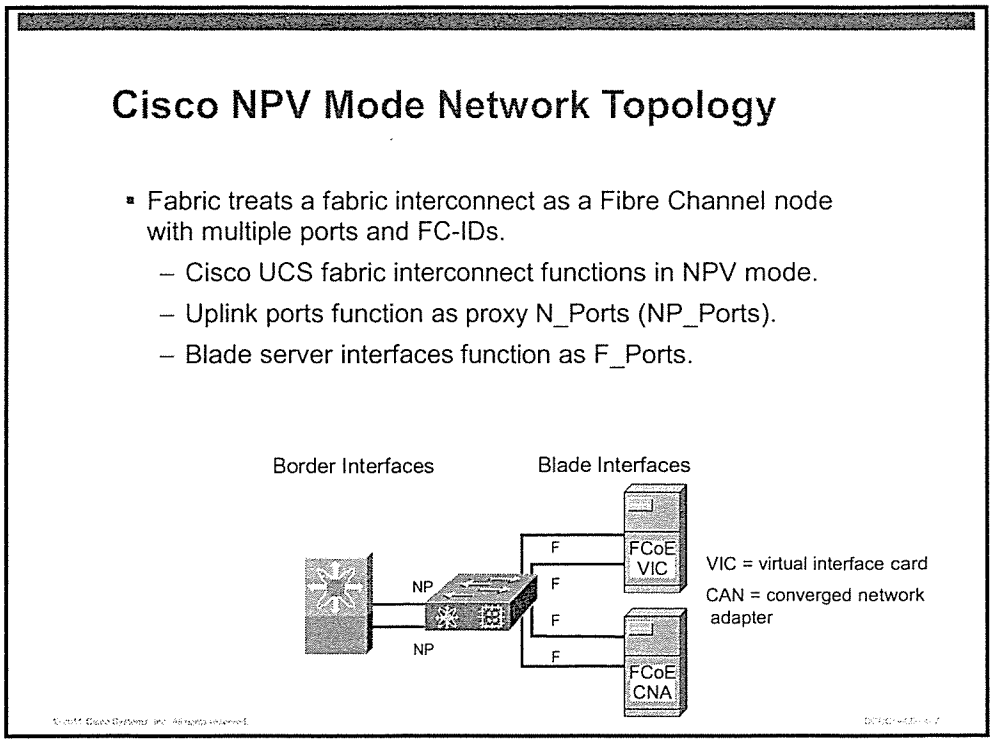
There are three basic topologies in Fibre Channel networks:

- Point-to-point connections are simple but do not scale.
- Arbitrated loop topologies are most commonly used to connect shelves of disks to a Fibre Channel storage controller.
- Switched topologies are the most common method of host attachment to Fibre Channel storage. Switched topologies can theoretically scale to millions of nodes. A Fibre Channel switch is required for FCoE to function.

Cisco NPV

This topic describes Cisco N_Port Virtualization.

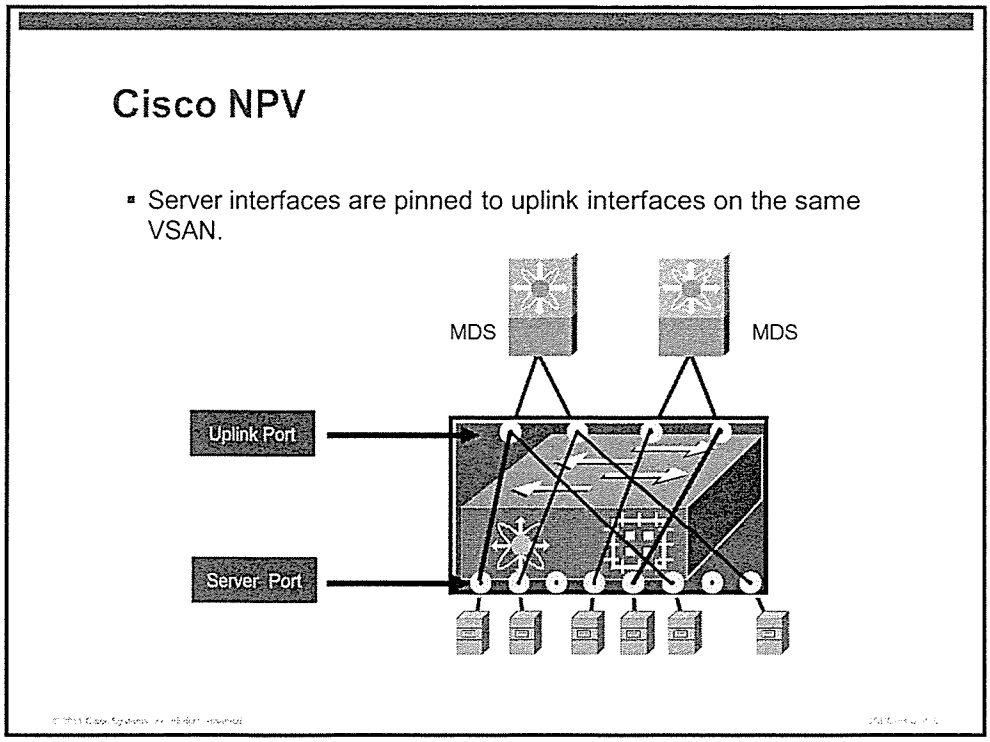
Cisco NPV Mode Network Topology



There are two types of interfaces in N-Port ID Virtualization (NPIV) topologies.

- **Server Interfaces:** Server-facing interfaces are either physical Fibre Channels or virtual Fibre Channel interfaces with F_Port modes.
  - There is no local switching.
  - All packets are forwarded.
  - Fabric login (FLOGI)-related processing is relayed in software (FLOGI, fabric discovery [FDISC], and corresponding Link Service Accept [LS_ACC], Link Service Reject [LS_RJT], and so on) to the same uplink interface.
  - NPIV is supported on F_Ports
- **Border Interfaces:** Border interfaces are network-facing and will always be N-Port types.
  - Internal FLOGI is sent to the core Fibre Channel switches.
  - Register with name servers on the successful internal FLOGI.
  - Every uplink can be connected to different Fibre Channel switches and VSANs.

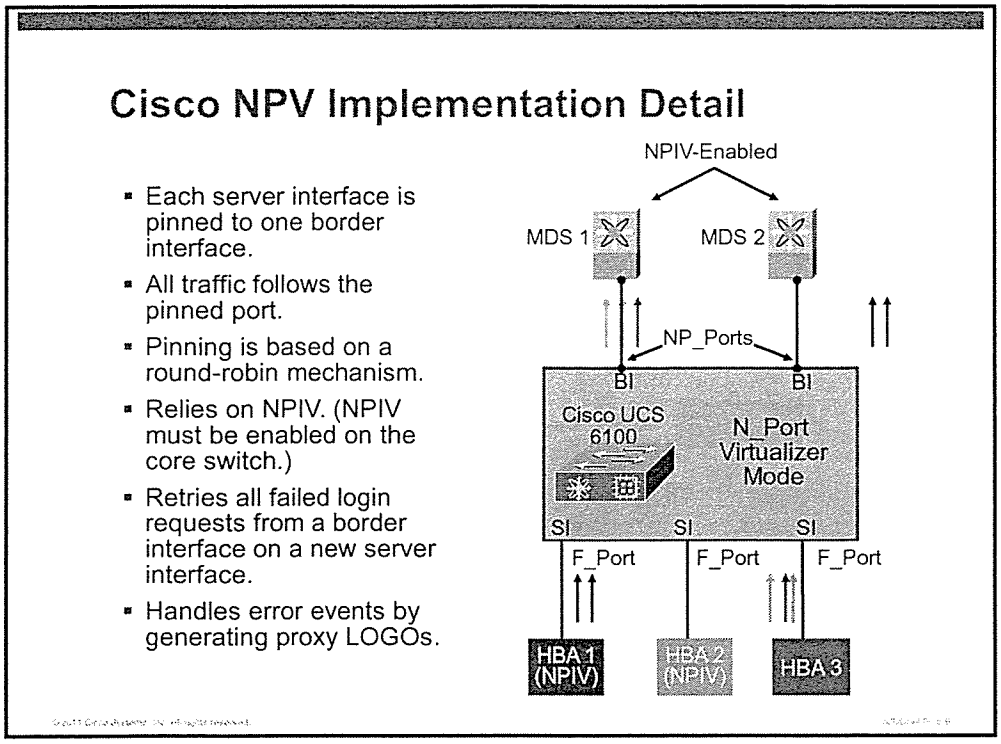
Cisco NPV



Each server link is pinned to exactly one uplink.

- Pinning logic distributes server links to various uplinks.
- All traffic is passed upstream for switching.

Cisco NPV Implementation Detail

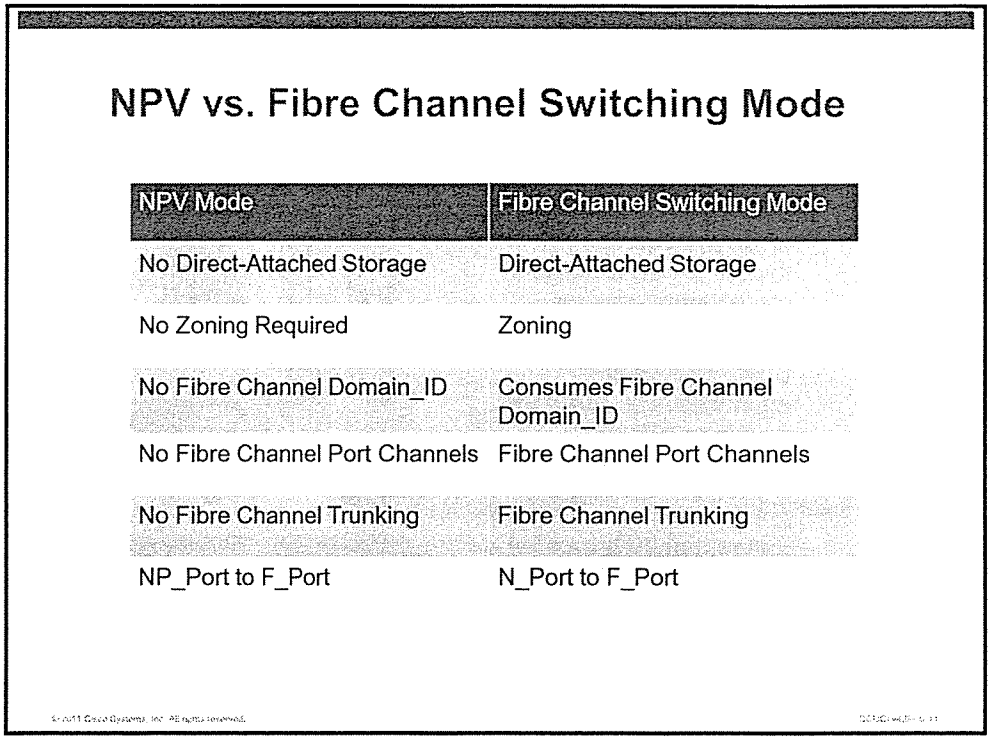


NPIV proxy modules in the Cisco Nexus Operating System (NX-OS) provide the proxy function of distributing FLOGI requests from servers over the available border interfaces. The Fibre Channel host bus adapters (HBAs) in servers and Fibre Channel switches assume that they are connected directly to each other by using a physical cable.

Note	The NPIV proxy function allows the NPIV to be used between the Cisco UCS fabric interconnect and the Fibre Channel switch. This applies even if some or all HBAs implement only the basics of N_Port functionality.

Benefits and Drawbacks of NPV and Fibre Channel Switching

This topic discusses the differences between NPV mode and Fibre Channel switching mode.

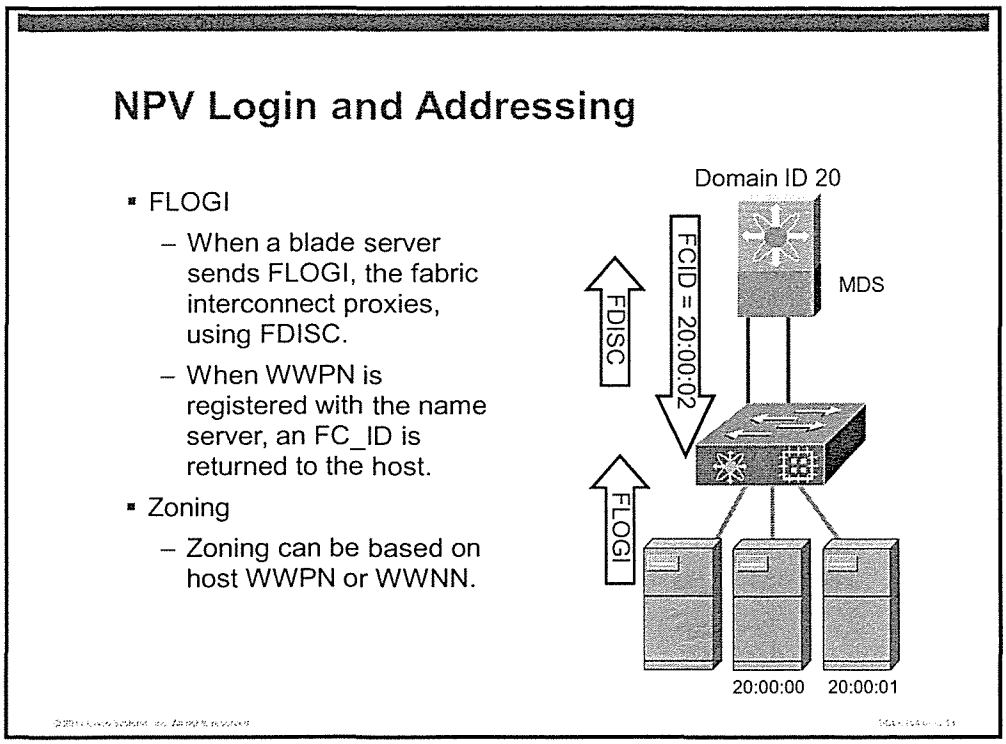


For large enterprise SANs, scalability is a critical concern. If the fabric interconnect operates in Fibre Channel switching mode, a Fibre Channel Domain_ID is consumed. Because there are only 239 possible Domain_IDs available within the Fibre Channel addressing schema, introducing a six- or eight-port Fibre Channel switch can severely limit how large a SAN can grow.

In NPV mode, the fabric interconnect appears to the Fibre Channel switch as a node. As such, no Domain_ID is required on behalf of the fabric interconnect.

How NPIV Allows a Single N_Port to Be Associated with Multiple FC_IDs

This topic discusses Fibre Channel addressing in NPV mode.

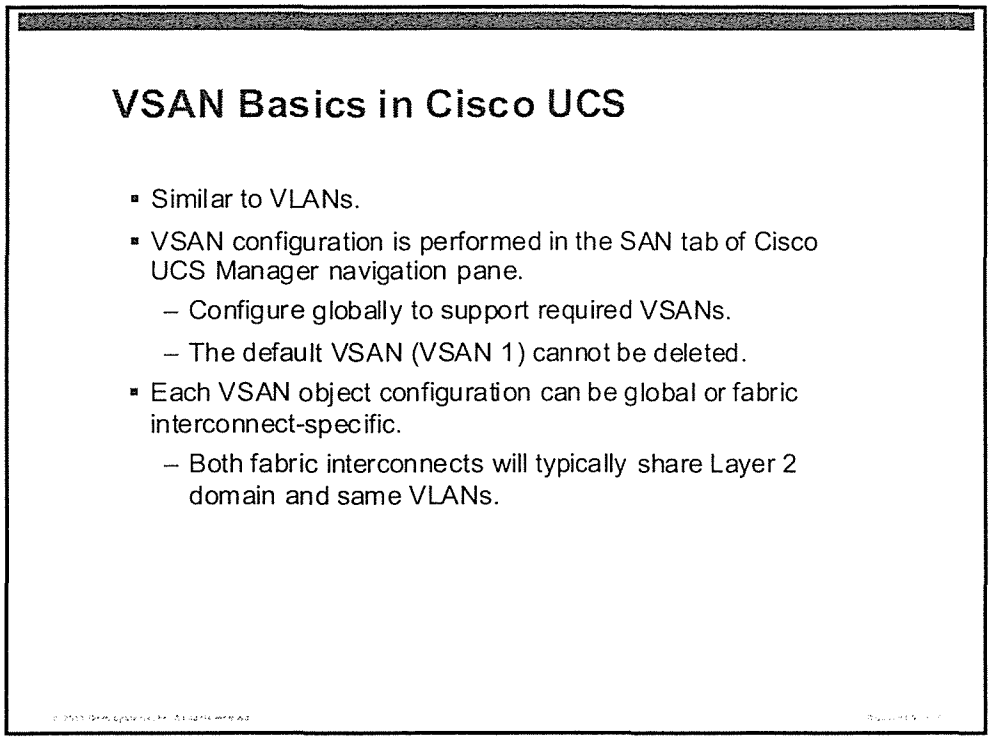


Using NPV, each downstream device (server or blade server) will be pinned to an uplink port based on a round-robin algorithm. The NPV mode switch will no longer service FLOGI login requests, operate the name service, perform zoning, or make routing decisions using Fabric Shortest Path First (FSPF). Instead, these operations are passed to the upstream switch, which is known as the NPV core switch. The NPV core switch will use NPIV to interpret multiple logins from the same port.

Requirements and Configuration of VSANs in Cisco UCS Manager

This topic discusses the creation of VSANs.

VSAN Basics in Cisco UCS

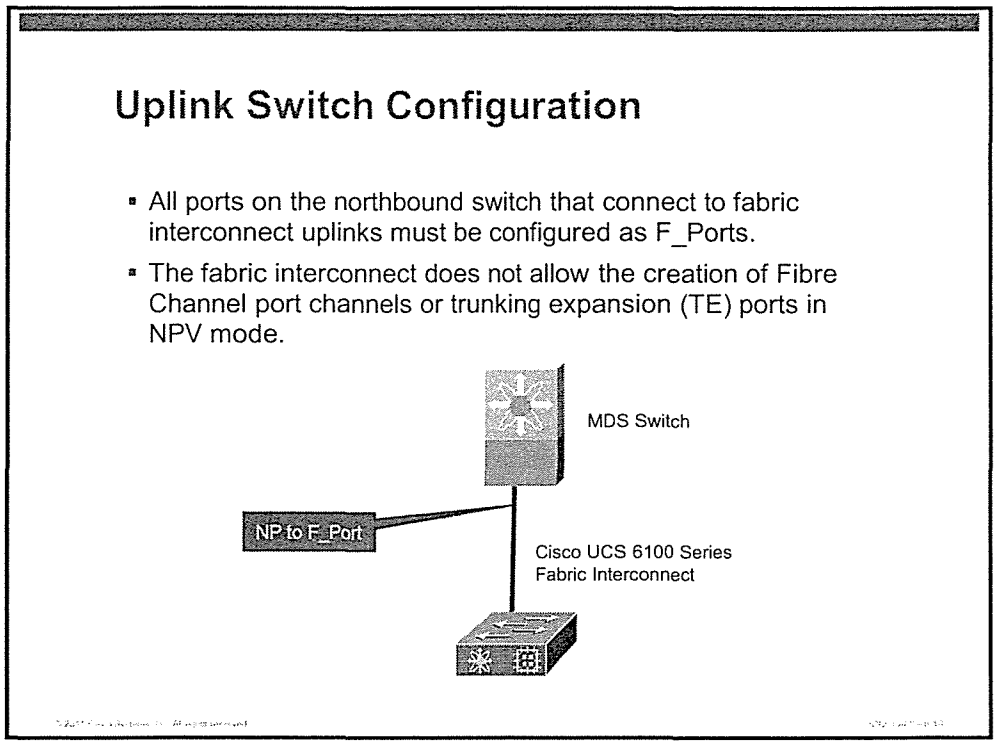


The VSAN and vHBA logic is similar to the VLAN and virtual network interface card (vNIC) logic.

You must have a Cisco UCS Manager vHBA object in a service profile to configure connectivity for a Fibre Channel adapter on a compute node.

To support any VSAN, that VSAN must be configured globally into Cisco UCS Manager and then associated with a particular vHBA. The default VSAN is preconfigured into Cisco UCS Manager and is chosen automatically as the default connectivity for each vHBA.

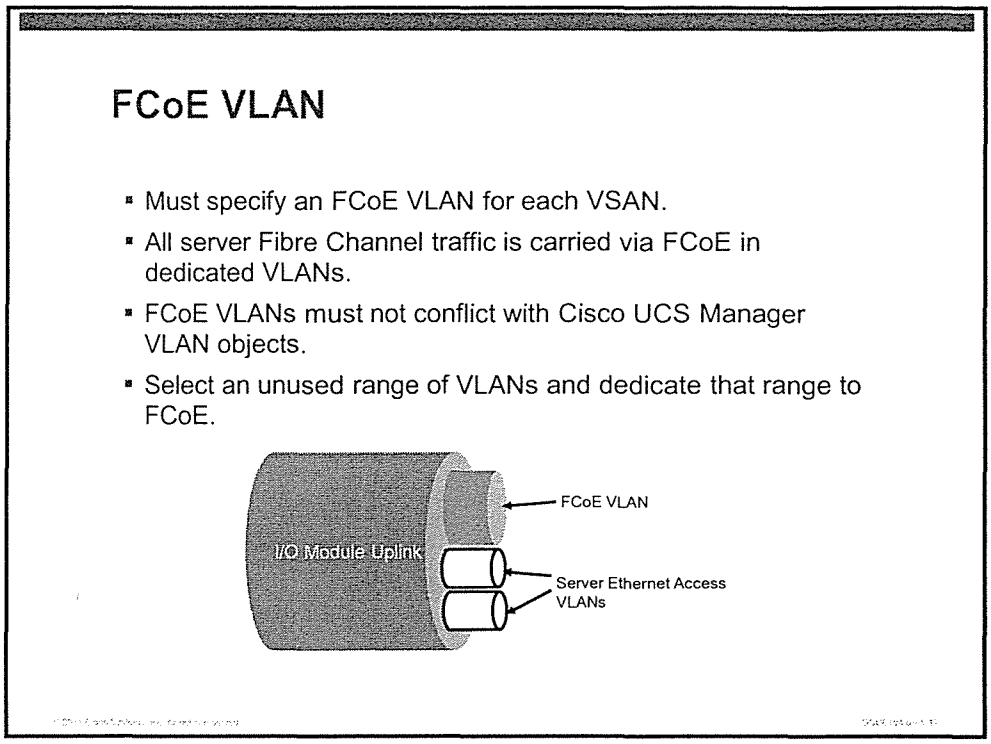
Uplink Switch Configuration



The Fibre Channel uplink on the northbound Fibre Channel switch must be configured as an F_Port on the same VSAN as the other end of the link on the fabric interconnect. There is a limit of one VSAN per Fibre Channel uplink.

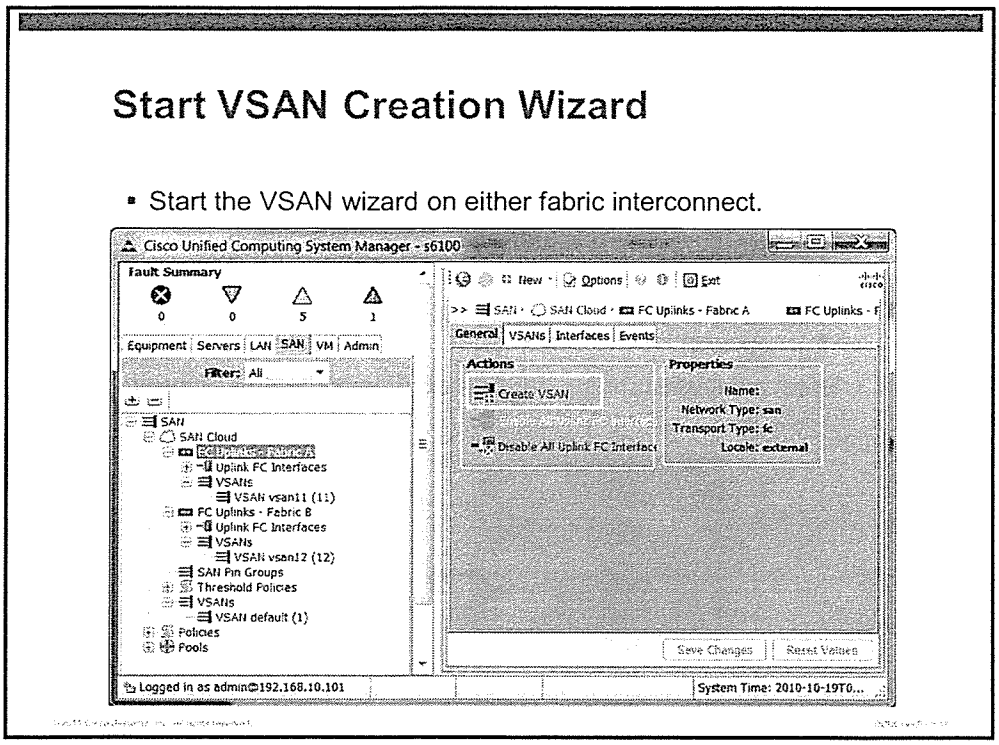
Although the Fibre Channel switching hardware is physically capable of forming Fibre Channel port channels in the same trunking, it currently is not supported in NPV mode.

FCoE VLAN



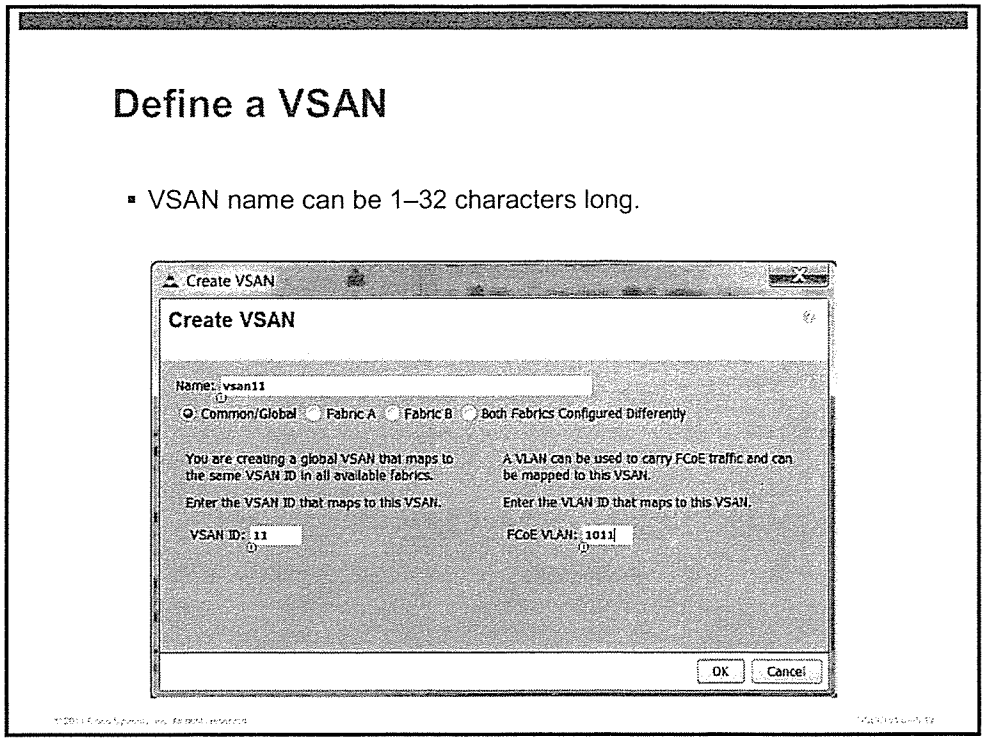
Because of the internal FCoE architecture of Cisco UCS, each VSAN supported within the architecture requires a dedicated VLAN to carry the FCoE traffic. FCoE VLANs are designated during VSAN configuration and are not created like Ethernet VLANs. The FCoE VLANs must not conflict with Ethernet VLAN objects. It is a best practice to dedicate an unused range of VLANs to FCoE traffic.

Start VSAN Creation Wizard



To start the VSAN creation wizard, click either of the fabric interconnects in the SAN tab of the navigation pane. Then, click the **Create VSAN** link in the content pane.

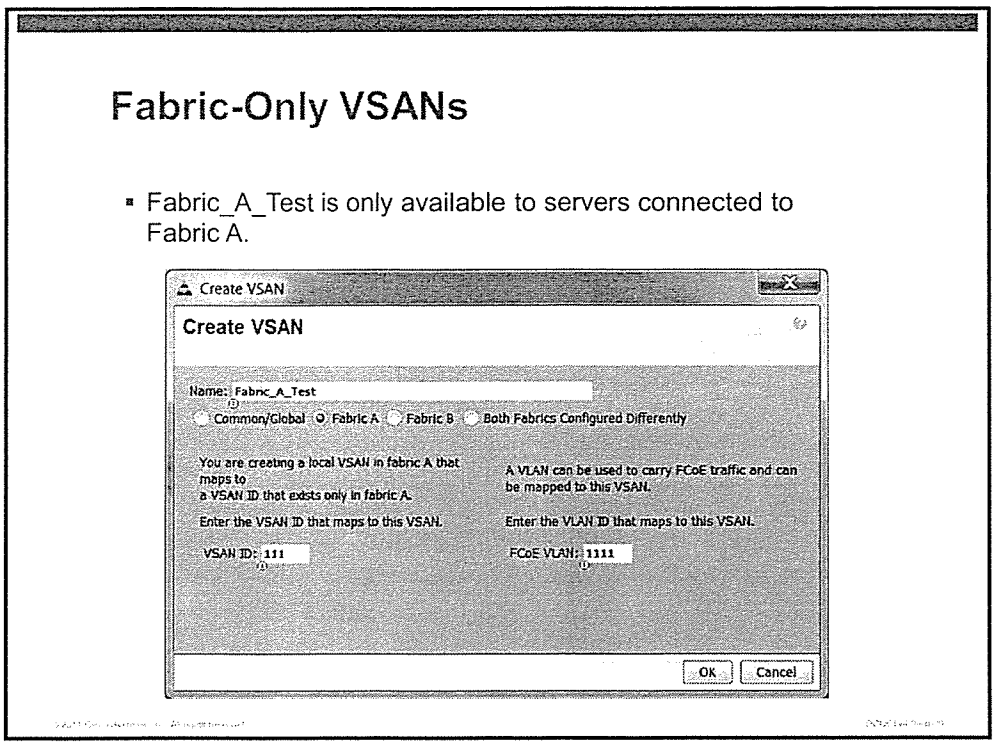
Define a VSAN



In Cisco UCS, VSANs require a name in a VSAN number. VSAN names are always used in the creation of vHBA profiles. This abstraction of the VSAN number allows a change of VSAN associated with the VSAN names without requiring configuration changes to the server.

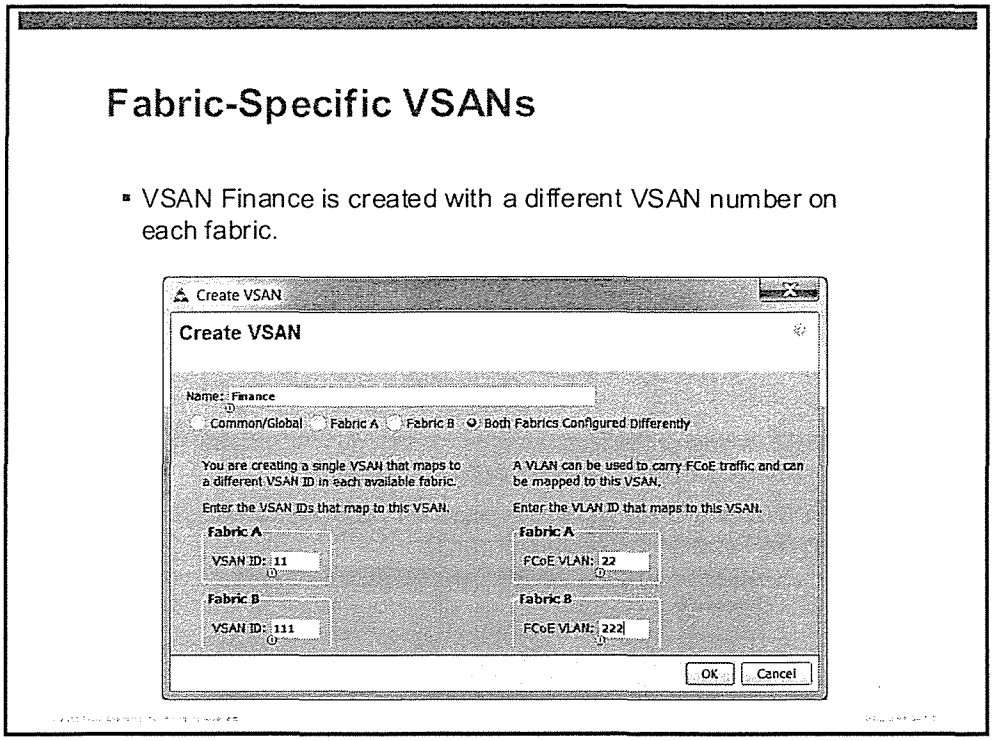
Common or global VSANs are created on both fabric interconnects and will use the same VSAN ID and FCoE VLAN. This type of configuration requires both fabric interconnects to be connected to the same physical Fibre Channel fabric. This configuration is not conducive to a high availability design because of the single point of failure.

Fabric-Only VSANs



Fabric-only VLANs can be created if desired. In the example, VSAN 111 will be created only on fabric interconnect A. In this configuration, each fabric interconnect would connect to a different upstream Fibre Channel switch. This configuration closely models traditional Fibre Channel designs and maintains the physical separation of the switch fabrics.

Fabric-Specific VSANs

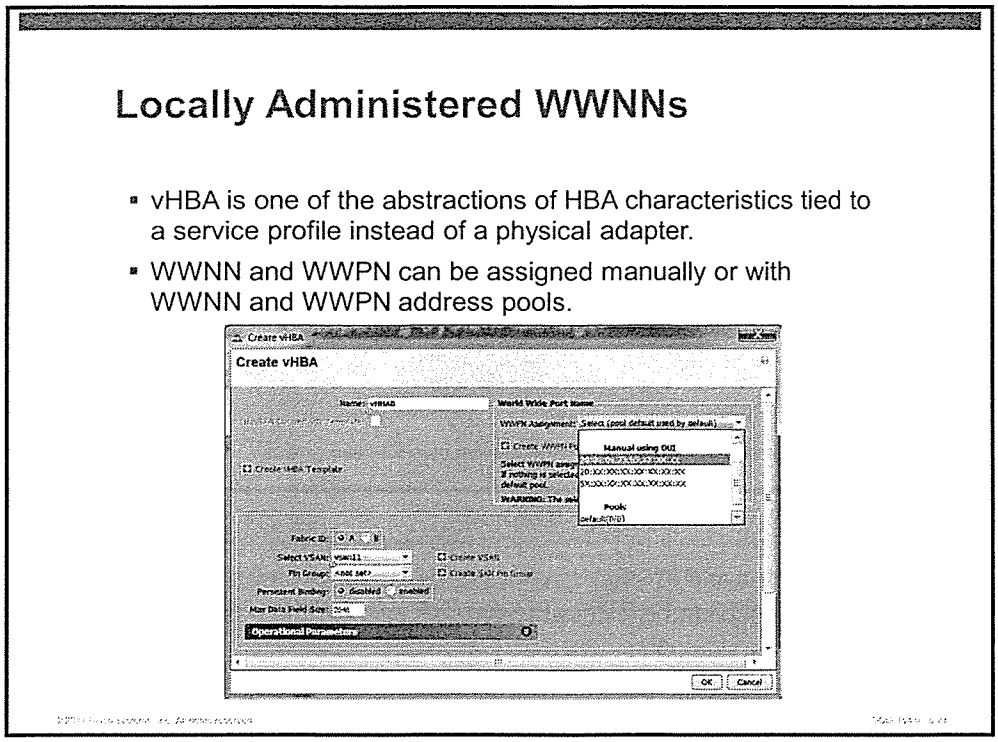


When using the Both Fabrics Configured Differently option, the same VSAN label is applied to two separate VSANs and FCoE VLANs. For this configuration to behave as expected, the same external resources need to be accessible through each of the upstream fabrics.

Role of vHBAs to Abstract WWNNs and WWPNs into a Service Profile

This topic discusses the benefits of configuring locally administered Fibre Channel world wide names (WWNs).

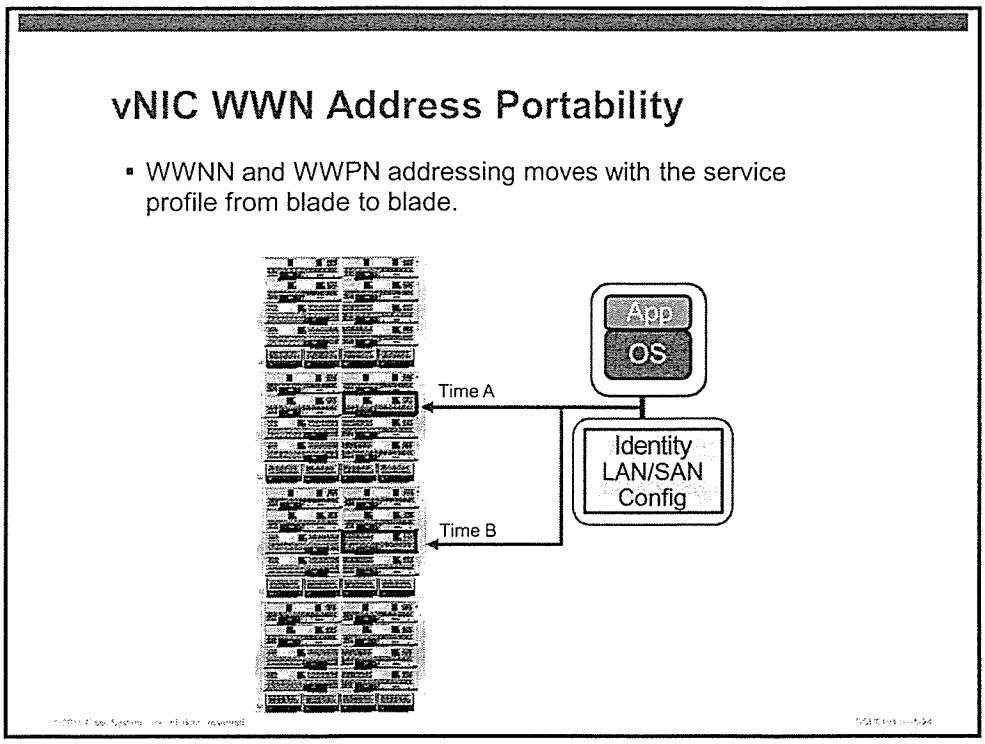
Locally Administered WWNs



Locally administered Fibre Channel WWNs are another identity resource that can be virtualized and abstracted from hardware in a Cisco UCS service profile. Stateless computing is one of the cornerstone values of Cisco UCS. Cisco UCS administrators have the option of manually configuring WWNs based on the Cisco-supplied prefix, using an identity pool, or the burned-in world wide node name (WWNN) or world wide port name (WWPN).

Abstracting WWNs in Fibre Channel networks is particularly important. If you use burned-in names and the service profile moves to a new blade server, it will not be able to find its boot logical unit number (LUN) until the SAN administrator rezones the fabric for the new WWNN or WWPN. Using local addressing allows Cisco UCS administrators to move a service profile to a replacement blade server. When the operating system or hypervisor boots, its old WWNN or WWPN will be preserved.

vNIC WWN Address Portability

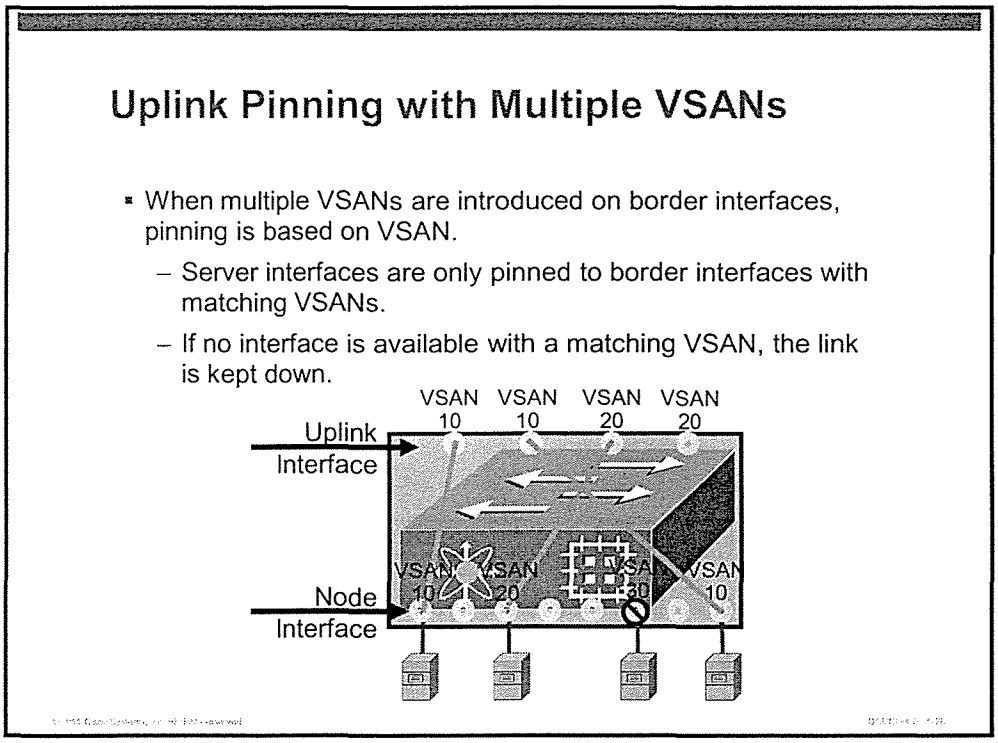


The main benefit of virtualizing Fibre Channel WWNs is that if the underlying server hardware fails, a service profile is simply moved to a replacement server. When the operating system boots on the new server, the WWNs are unchanged. From the perspective of the operating system or hypervisor running on the blade server, the service profile is on the same hardware from which it was last booted.

Automatic Uplink Pinning and Recovery from Failure

This topic discusses automatic uplink pinning.

Uplink Pinning with Multiple VSANs

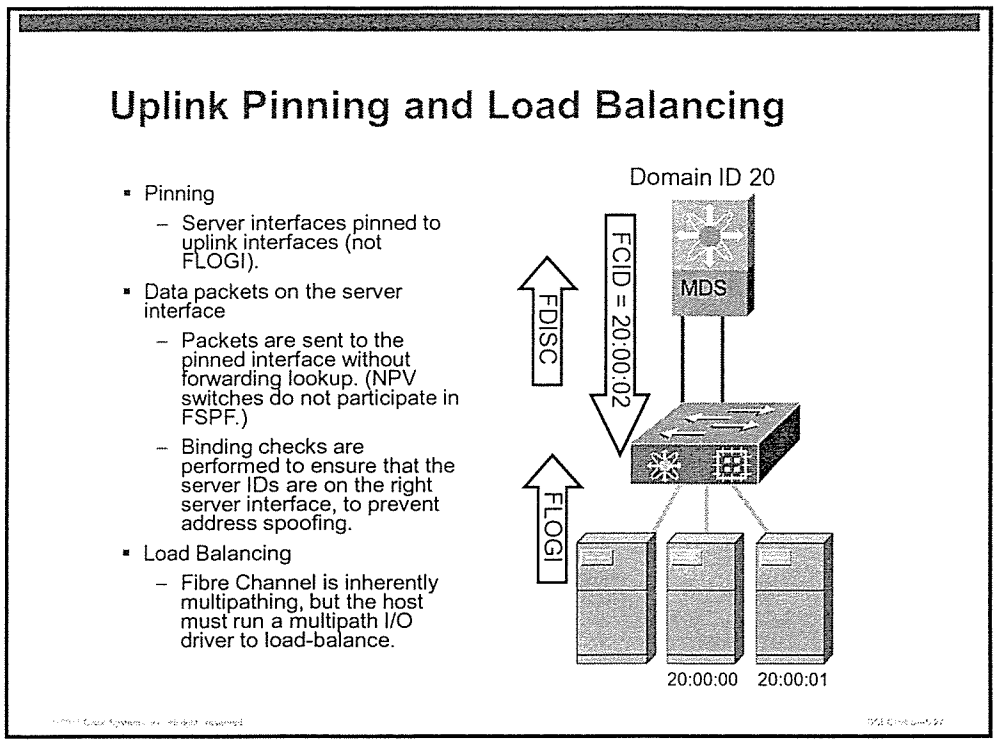


Uplink interfaces and node interfaces can only be configured for a single VSAN. Node interfaces will only be pinned to a port of the correct VSAN.

The example in the figure shows the following:

- Two uplink interfaces are configured for VSAN 10 and the other two are configured for VSAN 20.
- Two blade ports are configured for VSAN 10.
- One blade port is configured for VSAN 20.
- One server port is configured for VSAN 30.
- The blades that are configured for VSAN 10 will be pinned on one of the VSAN 10 border interfaces.
- The blade that is configured for VSAN 20 will be pinned to one of the VSAN 20 border interfaces.
- The blade interface that is configured for VSAN 30 will be kept down because there is no matching uplink interface.

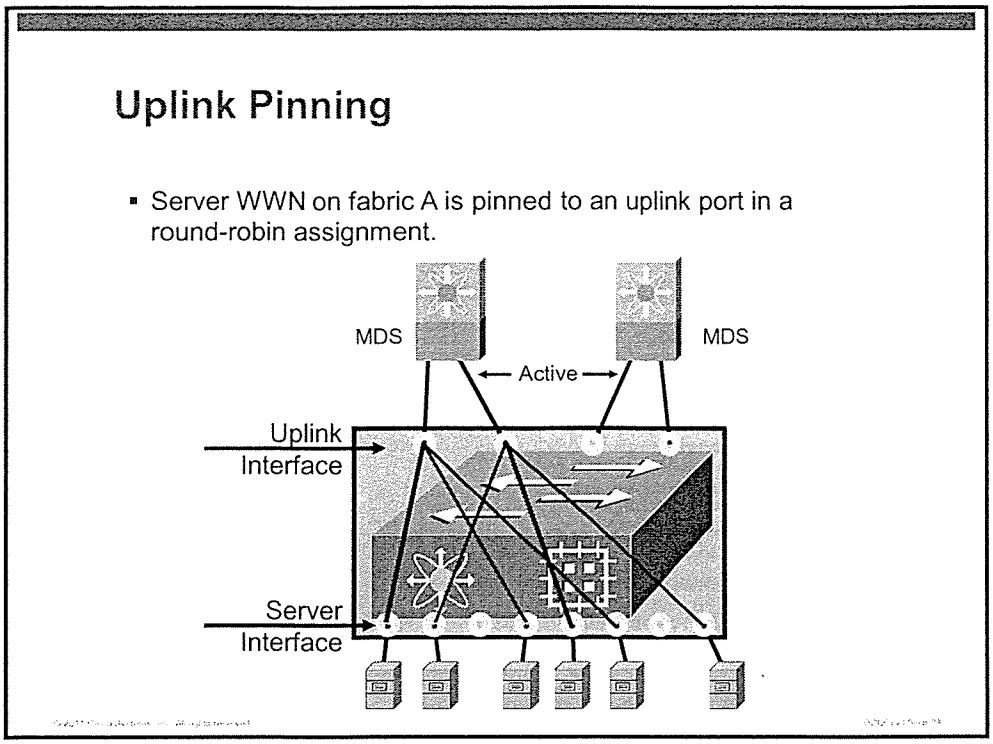
Uplink Pinning and Load Balancing



Using NPV, each downstream device (server or blade server) will be pinned to an uplink port based on a round-robin algorithm. These operations are passed to the upstream switch, which is known as the NPV core switch. The NPV core switch will use NPIV to interpret multiple logins from the same port.

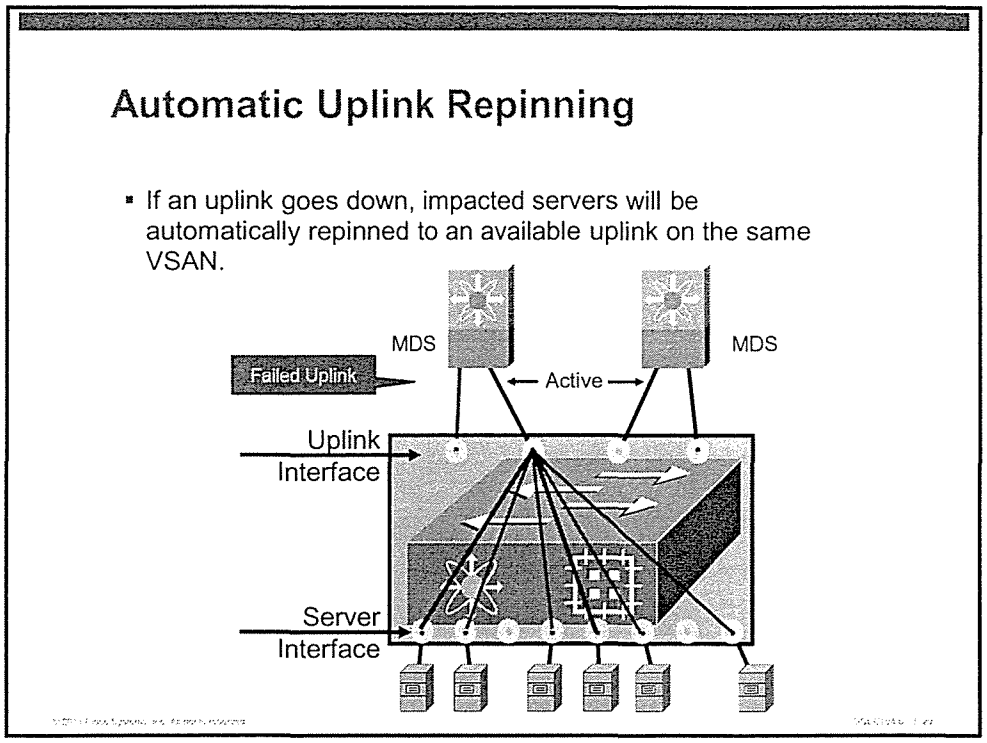
Although Fibre Channel is inherently multipathing, load-balancing and discovery of path failure is the responsibility of the multipath I/O driver in the operating system or hypervisor. The hardware failover option that is available for Ethernet does not affect Fibre Channel traffic.

Uplink Pinning



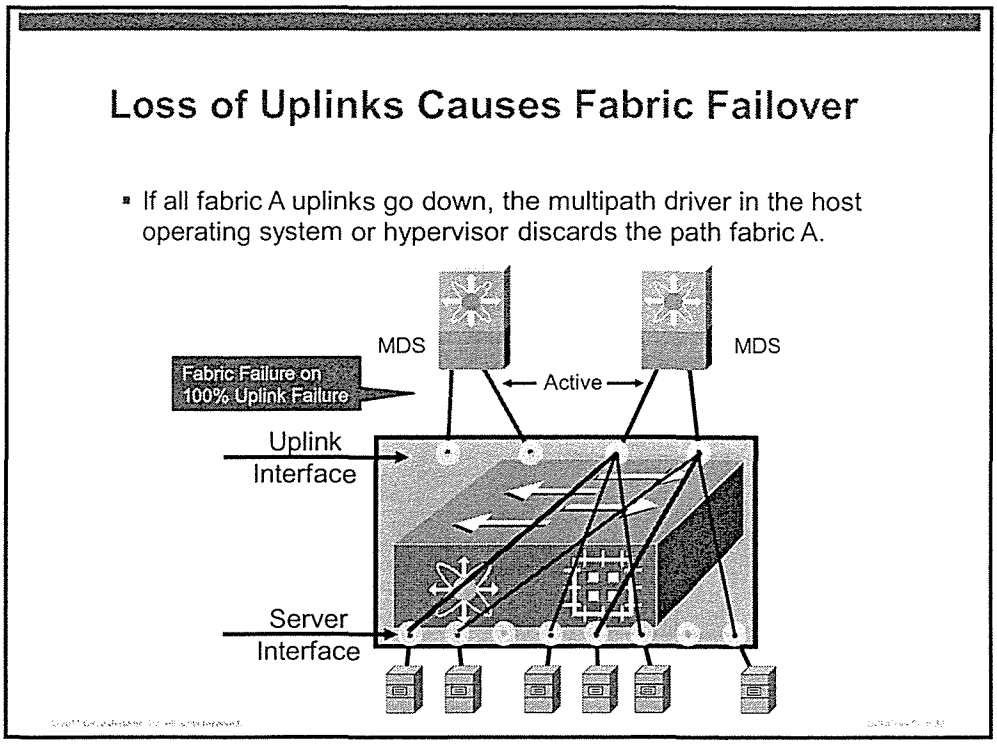
Recall from the discussion of end-host virtualization mode that a loop-free topology is assured by pinning MAC addresses to uplink ports. This pinning process can be either automatic or statically configured. By default, server MAC addresses are pinned to uplink interfaces in a round-robin process. The same process is followed with Fibre Channel traffic.

Automatic Uplink Repinning



With automatic uplink pinning, a link failure will cause all servers to be repinned to remaining uplinks. In the example, there are two uplinks on fabric A. When one of the links goes down, the server simply repins to the remaining uplink.

Loss of Uplinks Causes Fabric Failover

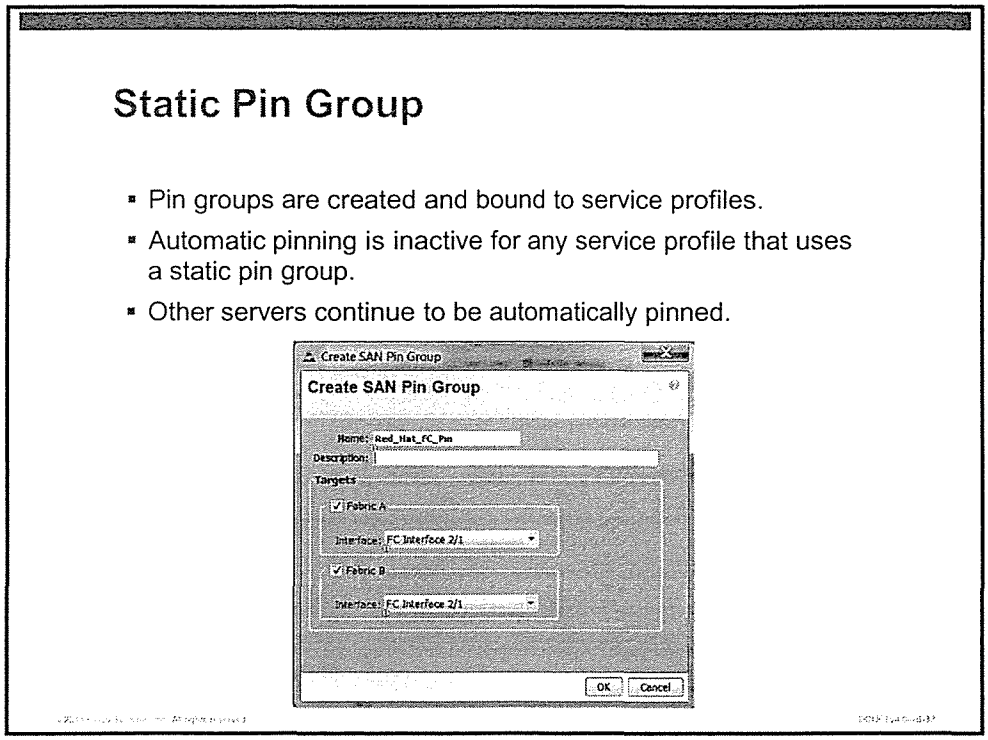


In the event that all uplink ports on the fabric interconnect lose connectivity, the operating system or hypervisor relies on its multipath I/O driver to discover the path loss and reroute. If the servers are not configured for high availability in the operating system or hypervisor, Fibre Channel communications will be down until at least one Fibre Channel uplink is restored on fabric A.

Configuration of Manual Uplink Pinning and Recovery from Failure

This topic discusses the creation of static pin groups to facilitate deterministic path selection.

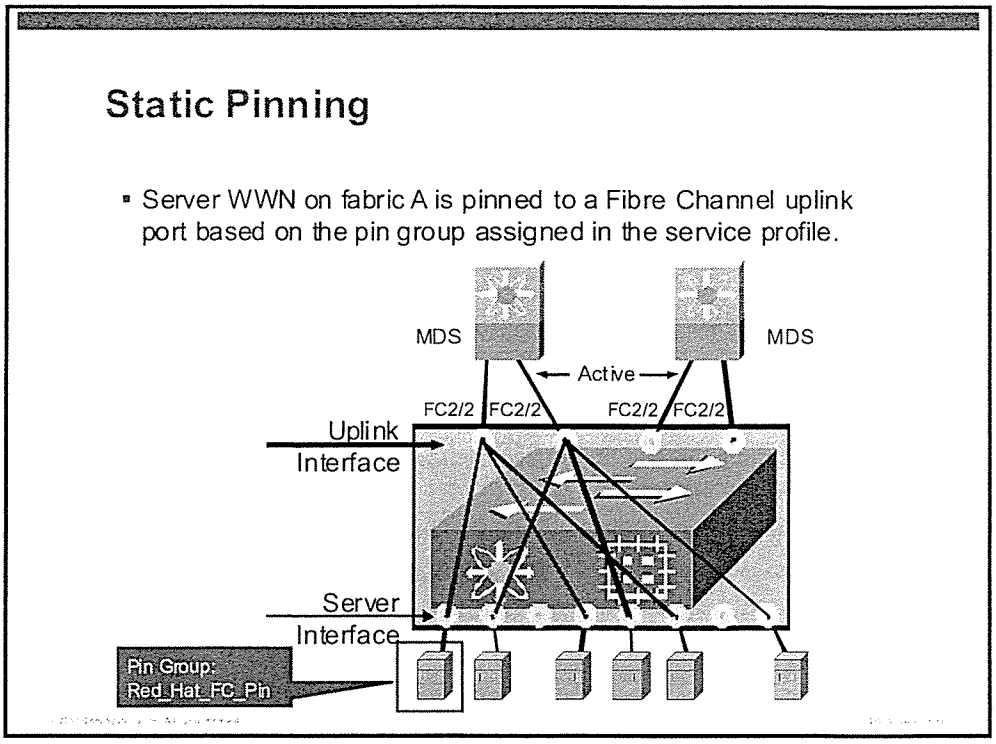
Static Pin Group



Pin groups are created under the LAN tab of the navigation pane. Pin groups are global policy elements and are replicated to the secondary management node.

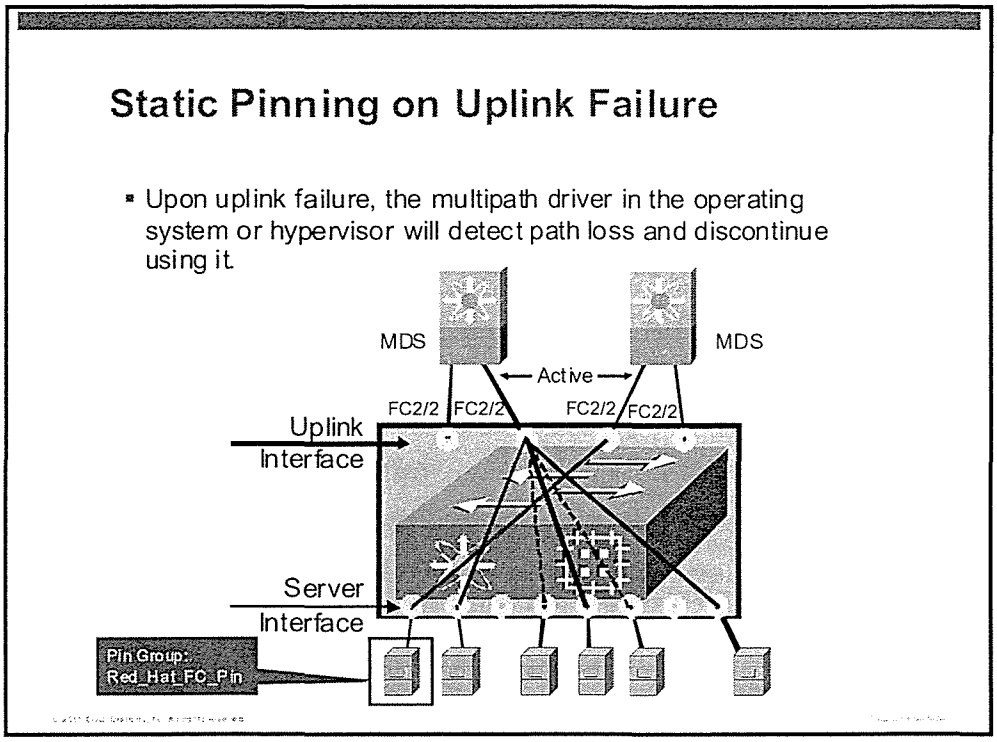
In this example, any service profile that includes this pin group policy will only use uplink FC 2/1 on fabric A. If that uplink goes down, automatic repinning will not occur and the server will rely on its multipath I/O driver to recognize the path failure and maintain connectivity on fabric B.

Static Pinning



In the example, the highlighted server is configured to use the static pin group called Red_Hat_FC_Pin that was just created. This server will always pin to uplink FC 2/1 on fabric A, or FC 2/1 on fabric B. If a multipath I/O driver is installed in the hypervisor or operating system, the HBA will operate over both fabric paths. If the pinned uplink fails on either fabric, the multipath driver is responsible for recognizing path failure.

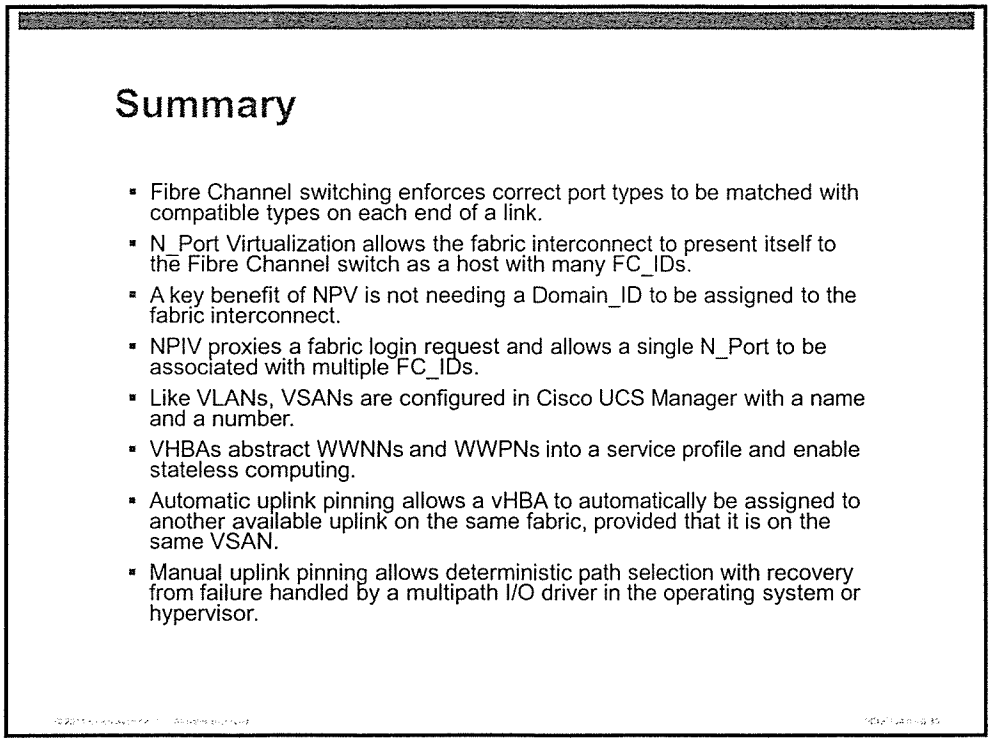
Static Pinning on Uplink Failure



In a static pinning environment, the operating system or hypervisor relies on its multipath I/O driver to detect path failure and discontinue using that path. If there is no multipath I/O driver, Fibre Channel communications will halt until the statically pinned uplink is restored.

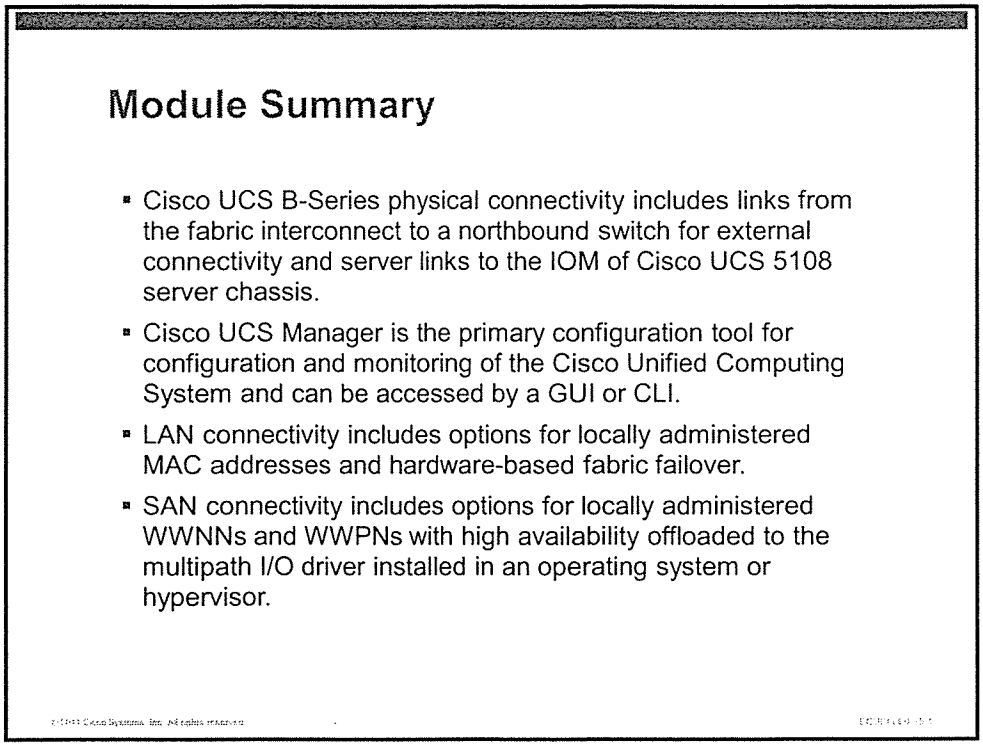
Summary

This topic summarizes the key points that were discussed in this lesson.



Module Summary

This topic summarizes the key points that were discussed in this module.



This module examines a broad range of physical and logical connectivity configuration requirements to implement Cisco UCS B-Series server chassis and components. High availability, navigating the Cisco UCS user interfaces, and LAN and SAN connectivity are the main themes.

The I/O module (IOM) provides external connectivity to Cisco UCS B-Series blade servers. Three levels of bandwidth oversubscription are available, based on the number of links from the IOM to the fabric interconnect. In addition to physical connectivity, the Chassis Management Controller (CMC) component of the IOM is responsible for chassis in component discovery, thermal management and monitoring, and cluster functions.

Many processes in Cisco UCS, such as chassis discovery and service profile association, are managed by finite state machines (FSMs). Monitoring FSM state for errors is a key troubleshooting activity.

There are two main user interfaces available to manage Cisco UCS, the Cisco UCS Manager GUI and a command-line interface (CLI). The CLI is available with multiple user shells for management, monitoring, and troubleshooting, and it is ideal for scripted operations.

To establish LAN connectivity for blade servers, a virtual NIC (vNIC) definition is created in a service profile. The vNIC definition includes the capability of locally administrating the MAC address to allow portability and stateless computing. To provide external LAN connectivity, the fabric interconnects are provisioned with uplinks to the northbound switches. These ports can exist as individual links or be aggregated into port channels.

By default, the fabric interconnects operate in end-host virtualization (EHV) mode for Ethernet LAN traffic. In EHV mode, the fabric interconnect does not maintain a MAC address forwarding table for traffic bound for an uplink. Instead, source MAC addresses are pinned to an uplink to maintain a loop-free topology.

To establish SAN connectivity for blade servers, a virtual HBA (vHBA) definition is created in a service profile. The vHBA definition includes the capability of locally administrating the world wide node names (WWNNs) and world wide port names (WWPNs) to allow portability and stateless computing. To provide external SAN connectivity, the fabric interconnects are provisioned with Fibre Channel uplinks to northbound Fibre Channel switches. These ports must exist as individual links with one VSAN per uplink. Fibre Channel port channels and VSAN trunking are not supported in N_Port Virtualization (NPV) mode.

References

- Gai, S., Salli, T., et al (2009). Project California: a Data Center Virtualization Server. Raleigh, NC: Lulu.com.
- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1)—Chassis Discovery*
- http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1_chapter1.html#concept_40AFE09861FA4D02A9879856A1411FAC Cisco Systems, Inc. *Cisco UCS SMASH Reference Guide*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/utilities/smash/reference/guide/ucs_smash_reference.html
- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1) – Uplink Ethernet Port Channels*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/1.3.1/CLI_Config_Guide_1_3_1_chapter5.html#concept_15B479F615A44205BB3851188C06F328
- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1)—Service Profiles that Override Server Identity*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/1.3.1/CLI_Config_Guide_1_3_1_chapter25.html#concept_472B3819CBB04CC9AC60044602D2C7CA
- Cisco Systems, Inc. *Cisco Fabric Manager Interfaces Configuration Guide—Configuring N Port Virtualization*

  http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/5_0/configuration/guides/int/fm/npv.html
- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1)—Configuring Named VSANs*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/CiscoUCSM_GUI_Configuration_Guide_1_3_1_chapter20.html

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) Which two choices are valid for blade server bandwidth oversubscription? (Choose two.) (Source: "Configuring Cisco UCS B-Series Physical Connectivity")

A) 16:1
B) 12:1
C) 10:1
D) 8:1
E) 6:1
F) 2:1
G) 1:1

Q2) Which three numbers indicate the number of supported links from the I/O module to the fabric interconnect? (Choose three.) (Source: "Configuring Cisco Unified Computing System B-Series Physical Connectivity")

A) 1
B) 2
C) 3
D) 4
E) 6
F) 8

Q3) If all chassis connect to their fabric interconnect with two links, which two statements are true about how many chassis can be supported in a Cisco UCS system? (Choose two.) (Source: "Configuring Cisco UCS B-Series Physical Connectivity")

A) Cisco UCS 6120 supports 20 chassis in this configuration.
B) Cisco UCS 6120 supports 10 chassis in this configuration.
C) Cisco UCS 6140 supports 20 chassis in this configuration.
D) Cisco UCS 6140 supports 10 chassis in this configuration.
E) Cisco UCS 6160 supports 20 chassis in this configuration.
F) Cisco UCS 6160 supports 10 chassis in this configuration.

Q4) Which three items are components of the I/O module? (Choose three.) (Source: "Configuring Cisco UCS B-Series Physical Connectivity")

A) chassis monitoring switch (CMS)
B) chassis switch monitor (CSM)
C) chassis management switch (CMS)
D) I/O MUX
E) chassis controller module (CCM)
F) chassis monitoring controller (CMC)
G) chassis management controller (CMC)

Q5) Where would you find information relevant to the discovery process while discovery is occurring? (Source: "Configuring Cisco UCS B-Series Physical Connectivity")

A) Intelligent Platform Management Interface (IPMI)
B) Serial over LAN (SoL)
C) LAN over Serial (LoS)
D) KVM over IP
E) finite state machine (FSM)
F) CIM XML
G) SMASH CLP

Q6) Which two items are major categories in the Equipment tab of the navigation pane? (Choose two.) (Source: "Exploring the Cisco UCS B-Series User Interfaces")

A) server
B) I/O module
C) chassis
D) fabric interconnects

Q7) Which two statements are true about the Cisco UCS Manager GUI? (Choose two.) (Source: "Exploring the Cisco UCS B-Series User Interfaces")

A) It is viewed in a browser window.
B) It is a Java application that opens in a separate window.
C) The GUI is divided into navigation, content, and context panes.
D) The GUI is divided into navigation and content panes.

Q8) In which Cisco UCS Manager CLI shell would you issue the **debug** command? (Source: "Exploring the Cisco UCS B-Series User Interfaces")

A) NX-OS
B) local-mgmt
C) IOM
D) adapter
E) CIMC
F) BMC

Q9) Which command would you use to access the Cisco UCS Manager CLI shell that provides the ping utility? (Source: "Exploring the Cisco UCS B-Series User Interfaces")

A) **connect nxos**
B) **context nxos**
C) **connect local-mgmt**
D) **context local-mgmt**
E) **connect iom**
F) **context iom**

Q10) Which two Cisco UCS Manager shells are read-only? (Choose two.) (Source: "Exploring the Cisco UCS B-Series User Interfaces")

A) IOM
B) NX-OS
C) adapter
D) UCS
E) local-mgmt

Q11) Which three options are valid port states on the Cisco UCS fabric interconnect? (Choose three.) (Source: "Configuring Compute Node LAN Connectivity")

A) fabric
B) unconfigured
C) local-mgmt
D) server
E) 1 Gb/s
F) uplink
G) 10 Gb/s

Q12) Which two types of interfaces can be configured for 1 Gb/s operation? (Choose two.) (Source: "Configuring Compute Node LAN Connectivity")

A) server
B) uplink
C) fabric
D) port channel
E) local-mgmt
F) NX-OS

Q13) How does end-host virtualization mode maintain a loop-free topology? (Source: "Configuring Compute Node LAN Connectivity")

A) STP
B) Rapid Spanning Tree (RST)
C) Multiple Spanning Tree (MST)
D) Per VLAN Rapid Spanning Tree (PVRST)
E) MAC pinning

Q14) Which statement about IOM pinning is true? (Source: "Configuring Compute Node LAN Connectivity")

A) If an IOM link fails, you must manually reacknowledge the chassis to repin servers.
B) If an IOM link fails, the IOM automatically repins all servers to the new topology.
C) If an IOM link fails, you must manually reacknowledge the chassis to repin servers.
D) If an IOM link fails, the IOM automatically shuts down the host ports to servers impacted by the failure.
E) If an IOM link fails, you must manually reacknowledge the IOM to repin servers.

Q15) Which two statements are true about static uplink pinning? (Choose two.) (Source: "Configuring Compute Node LAN Connectivity")

A) You can select one interface uplink on each fabric.
B) You can select two uplinks on each fabric.
C) You can select two port channels on each fabric.
D) You can select one uplink and one port channel on both fabrics.
E) You can select one port channel on each fabric.

Q16) Which statement is true about static uplink pinning? (Source: "Configuring Compute Node SAN Connectivity")

A) You can select one interface uplink on each fabric.
B) You can select two uplinks on each fabric.
C) You can select two port channels on each fabric.
D) You can select one uplink and one port channel on both fabrics.
E) You can select one port channel on each fabric.

Q17) Which two statements are true about automatic uplink pinning? (Choose two.) (Source: "Configuring Compute Node SAN Connectivity")

A) If a Fibre Channel uplink goes down, the server automatically gets pinned to the next available uplink on a new VSAN.
B) If a Fibre Channel uplink goes down, the server automatically gets pinned to the next available uplink on the same VSAN.
C) A multipath I/O driver is required for automatic repinning.
D) A multipath I/O driver is required for high availability.

Q18) Which statement is true about uplink pinning? (Source: "Configuring Compute Node SAN Connectivity")

A) You can configure 512 VSANs per uplink.
B) You can configure 256 VSANs per uplink.
C) You can configure 1 VSAN per uplink.
D) You can configure 512 VSANs per Fibre Channel port channel.
E) You can configure 256 VSANs per Fibre Channel port channel.
F) You can configure 1 VSAN per Fibre Channel port channel.

Q19) Which three statements are true about operating in NPV mode? (Choose three.) (Source: "Configuring Compute Node SAN Connectivity")

A) Single-initiator zoning is performed on the fabric interconnect.
B) No zoning can be configured on the fabric interconnect.
C) A Fibre Channel domain_ID is not consumed in NPV mode.
D) A Fibre Channel domain_ID is consumed in NPV mode.
E) Fibre Channel port channels can be configured from the fabric interconnect to the MDS switch.
F) Fibre Channel port channels cannot be configured from the fabric interconnect to the MDS switch.

Q20) Which three statements are true about Fibre Channel port combinations? (Choose three.) (Source: "Configuring Compute Node SAN Connectivity")

A) Connect N_Port to N_Port.
B) Connect N_Port to F_Port.
C) Connect E_Port to F_Port.
D) Connect E_Port to E_Port.
E) Connect TE_Port to N_Port.
F) Connect TE_Port to F_Port.
G) Connect NP_Port to F_Port.

Module Self-Check Answer Key

Q1) D, F

Q2) A, B, D

Q3) B, C

Q4) C, D, G

Q5) E

Q6) C, D

Q7) B, D

Q8) A

Q9) C

Q10) B, C

Q11) B, D, F

Q12) B, D

Q13) E

Q14) A

Q15) A, E

Q16) A

Q17) B, D

Q18) C

Q19) B, C, F

Q20) B, D, G