Getting Started Guide for Cisco UCS E-Series Servers, Release 2.x

First Published: August 09, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-29450-01

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Configuration Quick Reference	Provides a list of commands and steps to quickly setup and use the E-Series Server.
Chapter 2	Cisco UCS E-Series Servers Overview	Provides an overview of the E-Series Server, hardware and software requirements, and E-Series Server options.

Chapter	Title	Description
Chapter 3	Installing the E-Series Server into the Router	Describes how to install the E-Series Server into the router.
Chapter 4	Configuration Differences	Provides configuration differences between the Cisco SRE-V and the E-Series Server and between ISR G2 and the Cisco ISR 4451-X.
Chapter 5	Configuring CIMC Access	Provides options to configure CIMC access.
Chapter 6	Accessing CIMC	Provides an overview of CIMC and describes how to log into CIMC.
Chapter 7	Managing RAID	Describes RAID options and how to configure RAID.
Chapter 8	Installing the Operating System	Describes how to install an operating system.
Chapter 9	Configuring a Connection Between the Router and the E-Series Server	Describes how to configure a connection between the router and the E-Series Server.
Chapter 10	BIOS	Provides an overview of BIOS, how to install the BIOS firmware, and how to access the BIOS setup menu.
Chapter 11	Recovering from Corrupt CIMC Firmware	Describes how to recover from corrupt CIMC firmware.
Chapter 12	Diagnostic Tests	Describes how to run diagnostic tests.
Chapter 13	Cisco IOS Software Command Reference—ISR G2	Provides a list of Cisco IOS commands used to configure the ISR G2 and the E-Series Server.
Chapter 14	Cisco IOS Software Command Reference—Cisco ISR 4451-X	Provides a list of Cisco IOS commands used to configure the Cisco ISR 4451-X and the E-Series Server.

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
User input	Text the user should enter exactly as shown or keys a user should press appear in this font.
Document titles	Document titles appear in *this font*.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

The http://www.cisco.com/en/US/docs/unified_computing/ucs/e/1.0/roadmap/e_series_road_map.html provides links to all E-Series Server documentation:

- *Release Notes for Cisco UCS E-Series Servers*
- *Getting Started Guide for Cisco UCS E-Series Servers*
- *Hardware Installation Guide for Cisco UCS E-Series Servers*
- *Cisco Network Modules, Server Modules, and Interface Cards Regulatory Compliance and Safety Information*
- *Host Upgrade Utility Guide for Cisco UCS E-Series Servers*
- *GUI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller*
- *CLI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller*
- *CIMC XML API Programmer's Guide for Cisco UCS E-Series Servers*
- *Troubleshooting Guide for Cisco UCS E-Series Servers*
- *Open Source Used in Cisco UCS E-Series Servers*

New and Changed Information

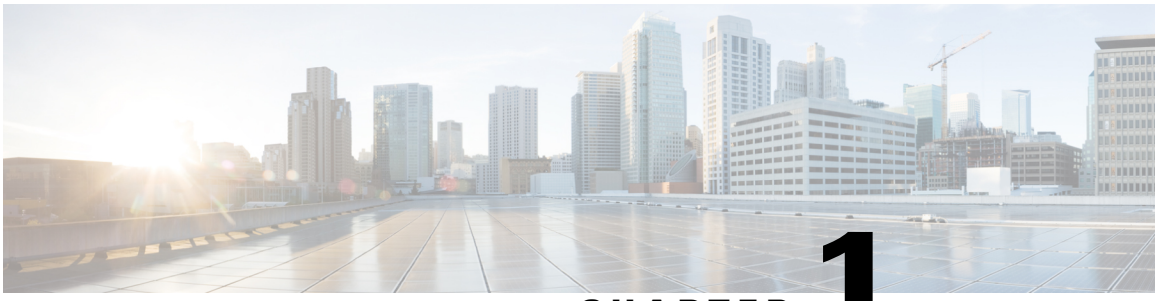
The following table provides an overview of the significant changes to this guide for the current release:

Table 1: New Features and Significant Changes in the Getting Started Guide for Cisco UCS E-Series Servers, Release 2.0

Feature	Description	Where Documented
Combined Getting Started Guide	One Getting Started Guide for all the platforms that the E-Series Server supports—Cisco 2900 and 3900 Integrated Services Routers (ISR G2) and the Cisco 4451-X Integrated Services Router (Cisco ISR 4451-X).	This guide.
Configuring CIMC Access	Provides the following information: • Configuring CIMC Access—ISR G2 • Configuring CIMC Access—Cisco ISR 4451-X	Configuring CIMC Access, on page 25
Configuring a Connection Between the Router and the E-Series Server	Provides the following information: • Configuring an Internal Connection Between the ISR G2 and the E-Series Server • Configuring an Internal Connection Between the Cisco ISR 4451-X and the E-Series Server	Configuring a Connection Between the Router and the E-Series Server, on page 87
RAID	Enhanced RAID feature.	Managing RAID, on page 61
Configuring the Server Boot Order	Support added for booting the server from specific devices within a device category.	Installing the Operating System or Hypervisor, on page 71
Host Image Mapping	Enhanced Host Image Mapping feature.	Installing the Operating System or Hypervisor, on page 71
Mapping the Diagnostics Image to the Host	Enhanced Diagnostics Image Mapping feature.	Diagnostic Tests, on page 119

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send an email to ucse_docfeedback@cisco.com. We appreciate your feedback.



CHAPTER 1

Configuration Quick Reference

Use this configuration quick reference chapter if you just need a list of commands and steps to quickly set up and use the Cisco UCS E-Series Server (E-Series Server). Detailed information about each of the configuration steps is provided in subsequent chapters.

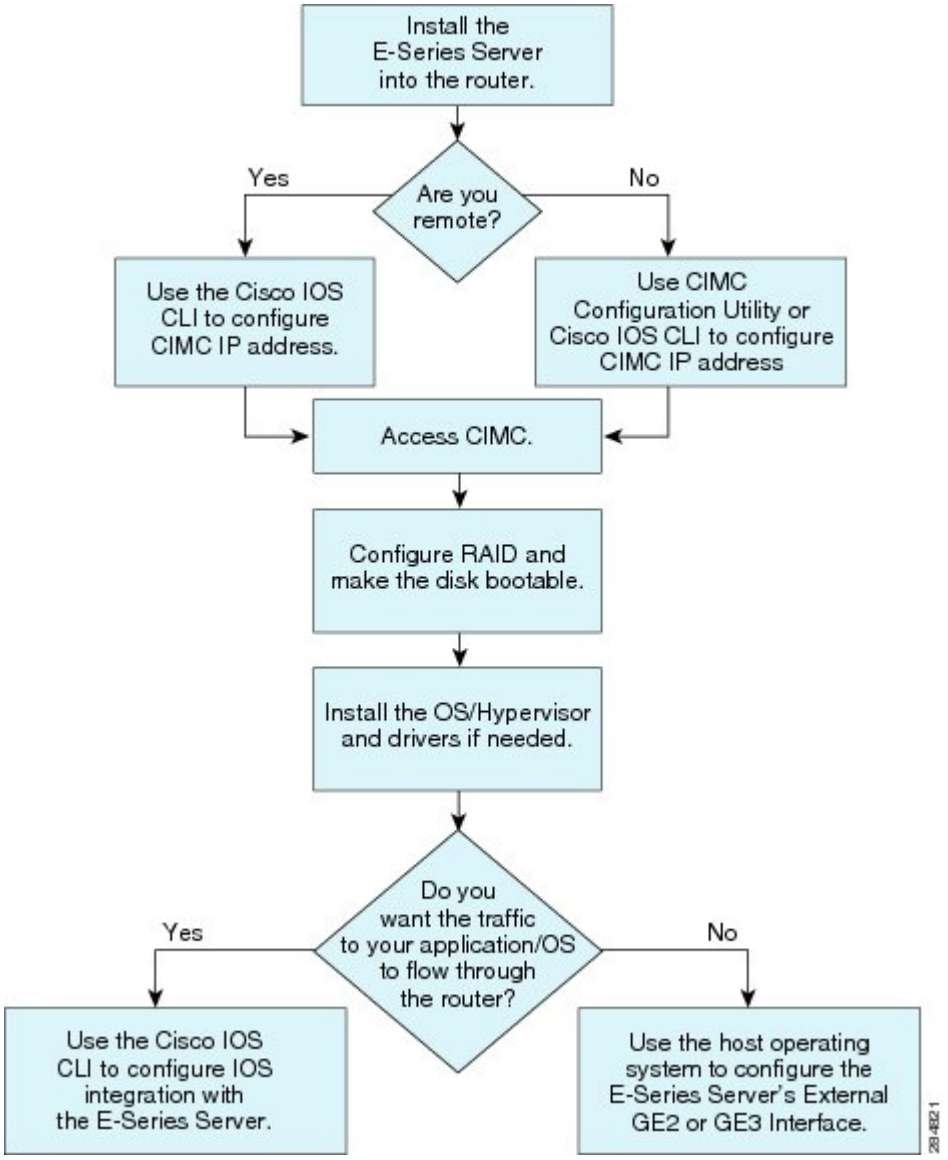
Note Use this configuration quick reference chapter if you purchased Option 1 (E-Series Server without preinstalled operating system or hypervisor). Some of the configuration steps are different if you purchased Option 2 (E-Series Server with preinstalled Microsoft Windows Server), or Option 3 (E-Series Server with preinstalled VMware vSphere Hypervisor™).

This chapter includes the following sections:

Configuration Quick Reference Tasks

The following figure shows the basic workflow for Option 1—E-Series Server without preinstalled operating system or hypervisor.

Figure 1: Basic Workflow—Option 1



Procedure

Step 1 Install the E-Series Server into the router.

Step 2 Configure the CIMC IP address for CIMC access. Use one of the following methods:

- If you are a remote user, use the Cisco IOS CLI to configure CIMC access. Enter the following commands:

  Note This configuration shows you how to configure CIMC access using the E-Series Server's Console interface (shared LOM). For details, see Configuring CIMC Access Using the Router's Internal PCIe Slot/0 Console Interface—ISR G2, on page 30.

  Note To use another interface, see Configuring CIMC Access, on page 25.

  - **enable**
  - **configure terminal**
  - **interface ucse** *slot/port*
  - **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*
  - **imc access-port shared-lom console**
  - **no shut**
  - **end**

- If you are a local user, use one of the following methods:
  - Connect a keyboard and monitor to the front panel of the E-Series Server, and then use the CIMC Configuration Utility to configure CIMC access. See Configuring CIMC Access Using the CIMC Configuration Utility, on page 51.
  - Use the Cisco IOS CLI to configure CIMC access (see the configuration for a remote user above).

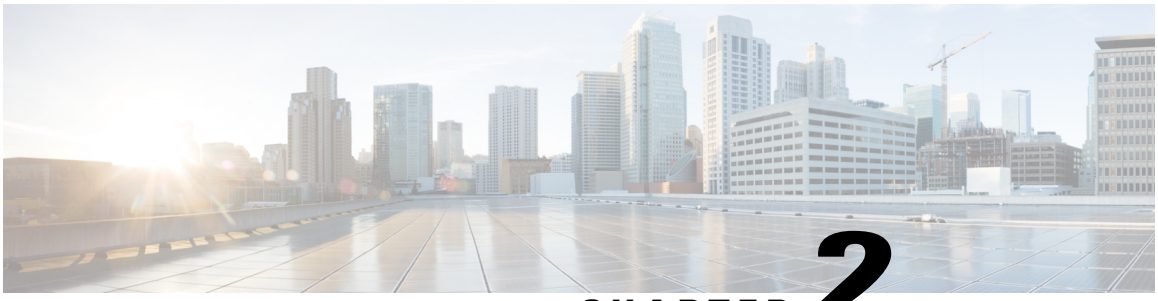
Step 3 In your web browser, enter the IP address that you configured in Step 2 to access CIMC.

Step 4 Configure RAID and make the disk drive bootable. See Managing RAID, on page 61.

Step 5 Install the operating system or Hypervisor and if needed, install drivers. See Installing the Operating System or Hypervisor, on page 71.

Step 6 Do one of the following:

- If you do not want the traffic to your application or operating system to flow through the router, use the server's host operating system to configure the E-Series Server's external GE2 or GE3 interface.
- If you want the traffic to your application or operating system to flow through the router, use the Cisco IOS CLI to configure an internal connection between the router and the E-Series Server. See Configuring a Connection Between the Router and the E-Series Server, on page 87.



CHAPTER 2

Cisco UCS E-Series Servers Overview

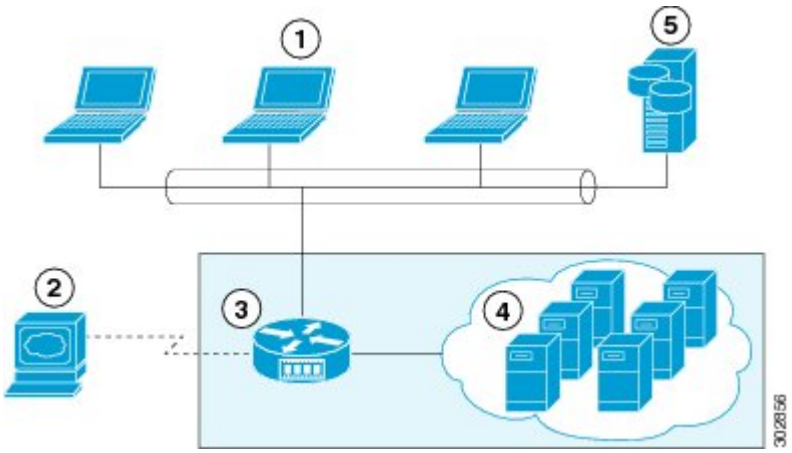
This chapter includes the following sections:

Cisco UCS E-Series Servers Overview

The Cisco UCS E-Series Servers (E-Series Servers) are the next generation of Cisco UCS Express servers. E-Series Servers are a family of size, weight, and power-efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (ISR G2) and the Cisco 4451-X Integrated Services Router (Cisco ISR 4451-X). These servers provide a general purpose compute platform for branch-office applications deployed either as bare-metal on operating systems, such as Microsoft Windows or Linux, or as virtual machines on hypervisors, such as VMware vSphere Hypervisor™, Microsoft Hyper-V, or Citrix XenServer.

The following figure shows an example of an E-Series Server Hypervisor deployment.

Figure 2: Example of an E-Series Server Hypervisor Deployment



1	Client Devices	4	Virtual Machines Hosted on the E-Series Server (applicable only if Hypervisor is running on the E-Series Server)
2	E-Series Server Management Console	5	Enterprise Storage Device
3	Cisco ISR G2 Router with E-Series Server running a Hypervisor or Bare-Metal Operating System		

Note For information about the supported E-Series Servers and the maximum number of E-Series Servers that can be installed per ISR, see the "Hardware Requirements" section in the *Release Notes for Cisco UCS E-Series Servers*.

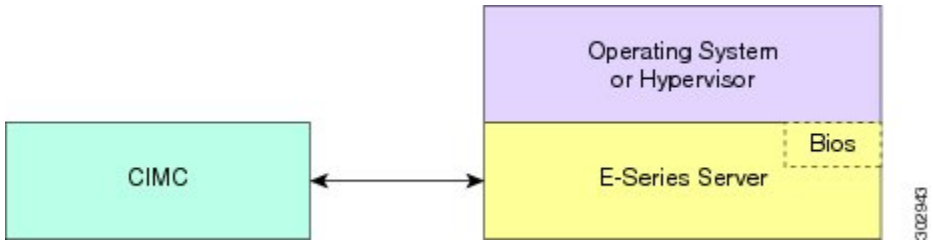
Server Software

E-Series Servers require three major software systems:

- CIMC Firmware
- BIOS Firmware
- Operating System or Hypervisor

The following figure shows how the software interacts with the E-Series Server.

Figure 3: Server Software



CIMC Firmware

Cisco Integrated Management Controller (CIMC) is a separate management module built into the motherboard of the E-Series Server. A dedicated ARM-based processor, separate from the main server CPU, runs the CIMC firmware. The system ships with a running version of the CIMC firmware. You can update the CIMC firmware, but no initial installation is needed.

CIMC is the management service for the E-Series Servers. You can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server.

BIOS Firmware

BIOS initializes the hardware in the system, discovers bootable devices, and boots them in the provided sequence. It boots the operating system and configures the hardware for the operating system to use. BIOS manageability features allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, manage firmware, and create BIOS error reports.

The system ships with a running version of the BIOS firmware. You can update the BIOS firmware, but no initial installation is needed.

Operating System or Hypervisor

The main server CPU runs on an operating system, such as Microsoft Windows or Linux; or on a Hypervisor. You can purchase an E-Series Server with pre-installed Microsoft Windows Server or VMware vSphere Hypervisor™, or you can install your own platform.

Note For information about the platforms that have been tested on the E-Series Servers, see the "Software Requirements" section in the *Release Notes for Cisco UCS E-Series Servers*.

Managing E-Series Servers

The following table lists the management interfaces used by the E-Series Server.

Table 2: E-Series Server Management Interfaces

Management Interface	Description
Cisco IOS CLI	Configures the host router and the E-Series Server.
CIMC GUI	Web-based GUI used to access, configure, administer, and monitor the E-Series Server.
CIMC CLI	SSH-based CLI used to access, configure, administer, and monitor the E-Series Server.
SNMP	Allows you to view server configuration and status, and send fault and alert information through Simple Network Management Protocol (SNMP) traps.

E-Series Server Options

E-Series Servers are available in the following options:

- Option 1—E-Series Server without a preinstalled operating system or hypervisor
- Option 2—E-Series Server with a preinstalled Microsoft Windows Server

  At the time of purchase, you can choose the appropriate RAID option that you want enabled on the E-Series Server.

  Note If you purchase this option, the Microsoft Windows Server license is preactivated.

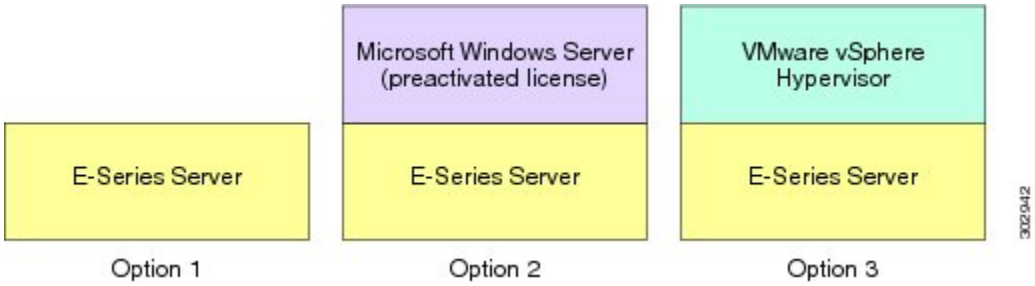
- Option 3—E-Series Server with a preinstalled VMware vSphere Hypervisor™

  At the time of purchase, you can choose the appropriate RAID option that you want enabled on the E-Series Server.

  Note The default username for the preinstalled VMware vSphere Hypervisor™ is **root**, which cannot be changed, and the default password is **password**. After you log in, we recommend that you change the password.

The following figure shows the E-Series Server options.

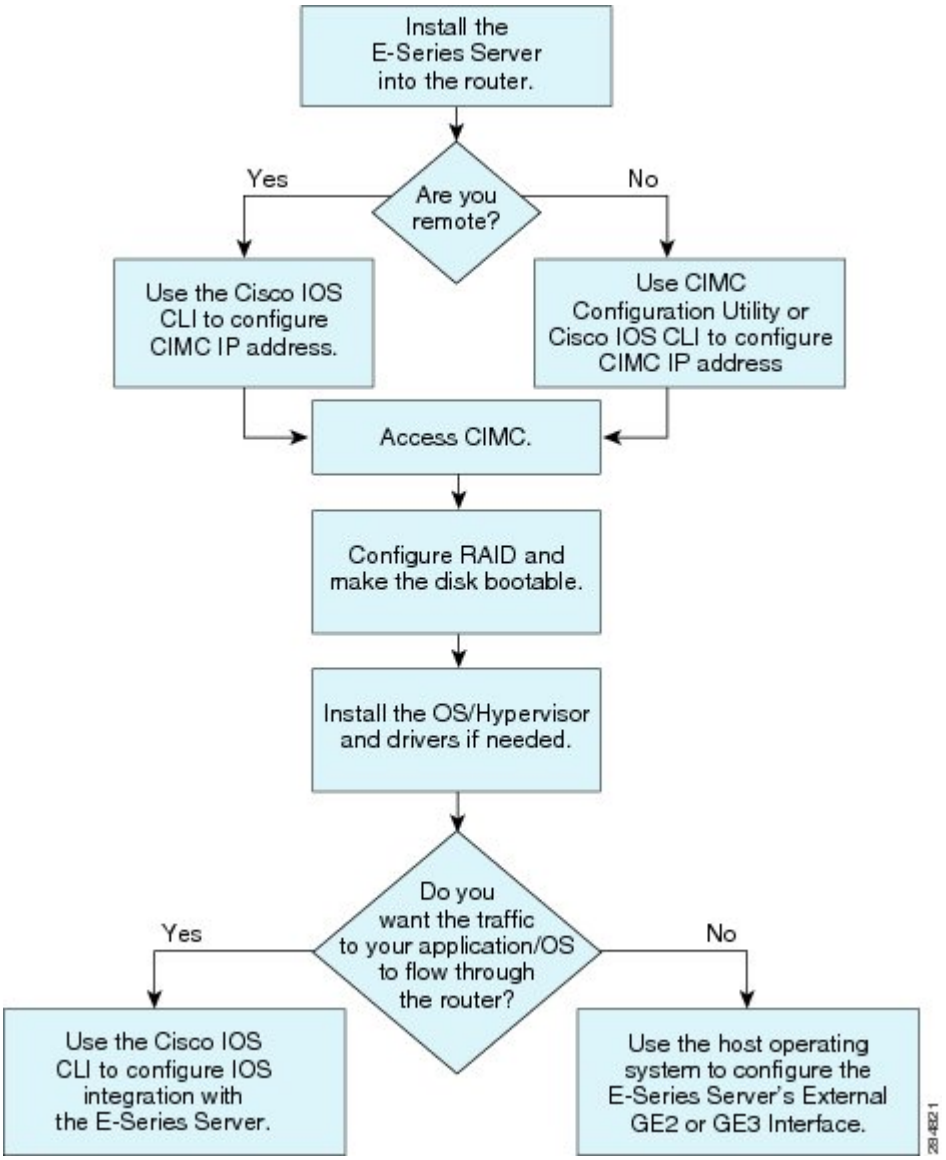
Figure 4: E-Series Server Options



Basic Workflow for Option 1—E-Series Server without a Preinstalled Operating System or Hypervisor

The following figure shows the basic workflow for Option 1—E-Series Server without a preinstalled operating system or hypervisor.

Figure 5: Basic Workflow—Option 1



The following procedure provides the references for the tasks that you must perform when you purchase Option 1—hardware only (E-Series Server without a preinstalled operating system or hypervisor).

Procedure

	Command or Action	Purpose
Step 1	Install the E-Series Server into the router.	See Installing the E-Series Server into the Router, on page 15.
Step 2	Configure the CIMC IP address for CIMC access.	See Configuring CIMC Access, on page 25.
Step 3	Access CIMC.	See Accessing CIMC, on page 55.
Step 4	Configure RAID and make the disk drive bootable.	See Managing RAID, on page 61.
Step 5	Install the operating system and if needed, install the drivers.	See Installing the Operating System or Hypervisor, on page 71.
Step 6	Configure an internal connection between the router and the E-Series Server.	Depending on whether you want the traffic to flow through the router or not, do one of the following: • If you *do not want* the traffic to your application or operating system to flow through the router, use the server's host operating system to configure the E-Series Server's external GE2 or GE3 interface. • If you *want* the traffic to your application or operating system to flow through the router, use the Cisco IOS CLI to configure an internal connection between the router and the E-Series Server. See Configuring a Connection Between the Router and the E-Series Server, on page 87.

Basic Workflow for Option 2—E-Series Server with a Preinstalled Microsoft Windows Server

The following procedure provides the references for the tasks that you must perform when you purchase Option 2—E-Series Server with a preinstalled Microsoft Windows Server.

Procedure

	Command or Action	Purpose
Step 1	Install the E-Series Server into the router.	See Installing the E-Series Server into the Router, on page 15.
Step 2	Configure the CIMC IP address for CIMC access.	See Configuring CIMC Access, on page 25.

	Command or Action	Purpose
Step 3	Configure an internal connection between the router and the E-Series Server.	Depending on whether you want the traffic to flow through the router or not, do one of the following: • If you *do not want* the traffic to your application or operating system to flow through the router, use the server's host operating system to configure the E-Series Server's external GE2 or GE3 interface. • If you *want* the traffic to your application or operating system to flow through the router, use the Cisco IOS CLI to configure an internal connection between the router and the E-Series Server. See Configuring a Connection Between the Router and the E-Series Server, on page 87.
Step 4	Access CIMC, and then access the Microsoft Windows Server from CIMC.	See Accessing CIMC, on page 55.

Basic Workflow for Option 3—E-Series Server with a Preinstalled VMware vSphere Hypervisor

The following procedure provides the references for the tasks that you must perform when you purchase Option 3—E-Series Server with a preinstalled VMware vSphere Hypervisor™.

Procedure

	Command or Action	Purpose
Step 1	Install the E-Series Server into the router.	See Installing the E-Series Server into the Router, on page 15.
Step 2	Configure the CIMC IP address for CIMC access.	See Configuring CIMC Access, on page 25.
Step 3	Configure an internal connection between the router and the E-Series Server.	Depending on whether you want the traffic to flow through the router or not, do one of the following: • If you *do not want* the traffic to your application or operating system to flow through the router, use the server's host operating system to configure the E-Series Server's external GE2 or GE3 interface. • If you *want* the traffic to your application or operating system to flow through the router, use the Cisco IOS CLI to configure an internal connection between the router and the E-Series Server. See Configuring a

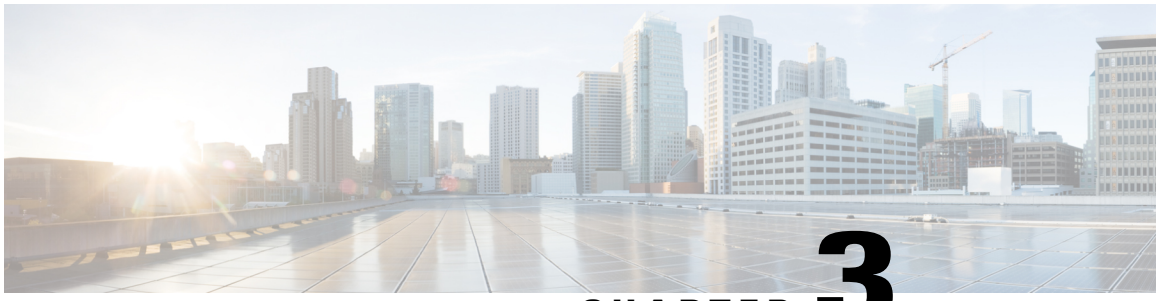
	Command or Action	Purpose
		Connection Between the Router and the E-Series Server, on page 87.
Step 4	Access CIMC, and then access the VMware vSphere Hypervisor™ from CIMC.	See Accessing CIMC, on page 55.

Common Terms Used in This Guide

The following table provides the common terms used in this guide.

Table 3: Common Terms

Terms	Description
CIMC	Cisco Integrated Management Controller. CIMC is the management service for the E-Series Server. CIMC runs within the server. You can use CIMC to access, configure, administer, and monitor the server.
CLI	Command-Line Interface.
IMC	Integrated Management Controller. IMC is used in the Cisco IOS commands to configure CIMC.
BMC	Board Management Controller.
LOM	LAN on Motherboard. Shared LOM interfaces are used to configure CIMC access.
RAID	Redundant Array of Inexpensive Disks. RAID is used to store E-Series Server data files.



CHAPTER 3

Installing the E-Series Server into the Router

This chapter includes the following sections:

Basic Workflow for Installing the E-Series Server into the Router

1. Verify that the router, the E-Series Server, and the Cisco IOS software version that is installed on the router are compatible.
2. Install the E-Series Server into the router.

Important If you are migrating the E-Series Server from an ISR G2 into a Cisco ISR 4451-X, you must first update the CIMC firmware image to release 2.0(1.20130626092411) or the latest version and the BIOS firmware image to release 1.5.0.2 or the latest version—while the E-Series Server is still installed in the ISR G2—and then migrate it into the Cisco ISR 4451-X. For CIMC firmware installation instructions, see the "CIMC Firmware Management" chapter in the *GUI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller* on Cisco.com.

3. Verify that the E-Series Server is correctly detected by the router.

Verifying the Router, E-Series Server, and Cisco IOS Software Version Compatibility

The following table provides the router, the E-Series Server, and the Cisco IOS software version compatibility information.

Table 4: Router, E-Series Server, and Cisco IOS Version Compatibility

Router	Cisco IOS Software Version for Single-Wide E-Series Servers	Cisco IOS Software Version for Double-Wide E-Series Servers
2911	15.2(4)M and later versions	—
2921	15.2(4)M and later versions	15.2(4)M and later versions **Note** Supports 4-core only
2951	15.2(4)M and later versions	15.2(4)M and later versions **Note** Supports 4-core only
3925	15.2(4)M and later versions	15.2(4)M and later versions
3925e	15.2(4)M and later versions	15.2(4)M and later versions
3945	15.2(4)M and later versions	15.2(4)M and later versions
3945e	15.2(4)M and later versions	15.2(4)M and later versions
4451	XE 3.9S and later versions	XE 3.9S and later versions

Installing the E-Series Server into the Router

The following figure shows how to install the E-Series Server into a router. For detailed information, see the *Hardware Installation Guide for Cisco UCS E-Series Servers* on Cisco.com.

Installing the E-Series Server into the Router

Important If you are migrating the E-Series Server from an ISR G2 into a Cisco ISR 4451-X, you must first update the CIMC firmware image to release 2.0(1.20130626092411) or the latest version and the BIOS firmware image to release 1.5.0.2 or the latest version—while the E-Series Server is still installed in the ISR G2—and then migrate it into the Cisco ISR 4451-X. For CIMC firmware installation instructions, see the "CIMC Firmware Management" chapter in the *GUI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller* on Cisco.com.

We strongly recommend that you upgrade both the CIMC and the BIOS firmware images.

If you migrate the E-Series Server into the Cisco ISR 4451-X without first updating the CIMC firmware, the E-Series Server will continuously reset. To stop the reset and install the firmware, see Stopping the E-Series Server from Resetting and Updating the CIMC Firmware, on page 18.

Figure 6: Double-Wide E-Series Server in an ISR G2

Caution Before you install or remove the E-Series Server from a Cisco 2900 series ISR G2, make sure that you first power down the router, and then install or remove the E-Series Server.

Figure 7: Double-Wide E-Series Server in a Cisco ISR 4451-X

Stopping the E-Series Server from Resetting and Updating the CIMC Firmware

If you migrate the E-Series Server into the Cisco ISR 4451-X without first updating the CIMC firmware, the E-Series Server will continuously reset. Use this procedure to stop the reset and install the firmware.

Note Some of the steps in this procedure are performed from the router, and other steps are performed from the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router# **hw-module subslot** *slot/subslot* **maintenance enable**	Disables error recovery, which stops the E-Series Server from being reset. **Note** Enter the commands in Step 1 and Step 2 from the router.
Step 2	Router# **hw-module subslot** *slot/subslot* **session imc**	Starts a CIMC session.

	Command or Action	Purpose
Step 3	Server# **scope cimc**	Enters CIMC command mode. **Note** Enter the commands in Step 3 through Step 8 from the E-Series Server.
Step 4	Server/cimc # **scope firmware**	Enters CIMC firmware command mode.
Step 5	Server/cimc/firmware # **update** *tftp-ip-address path-and-filename*	Starts CIMC firmware update. The server will obtain the update firmware at the specified path and filename from the TFTP server at the specified IP address.
Step 6	Server/cimc/firmware # **show [detail]**	Displays the available firmware and status.
Step 7	Server/cimc/firmware # **activate** [**1** | **2**]	Activates the selected image. If no image number is specified, the server activates the currently inactive image.
Step 8	Click **Ctrl a Ctrl q**.	Exits the CIMC session.
Step 9	Router# **hw-module subslot** *slot/subslot* **maintenance disable**	Enables error recovery. **Note** Enter the commands in Step 9 and Step 10 from the router.
Step 10	Router# **hw-module subslot** *slot/subslot* **reload**	Reloads the E-Series Server. **Note** This reload power-cycles the E-Series Server.

Verifying E-Series Server Installation

Before You Begin

- Install the E-Series Server into the router.
- Load a compatible Cisco IOS image.
- Power on the server.

To verify the E-Series Server installation, use one of the following commands:

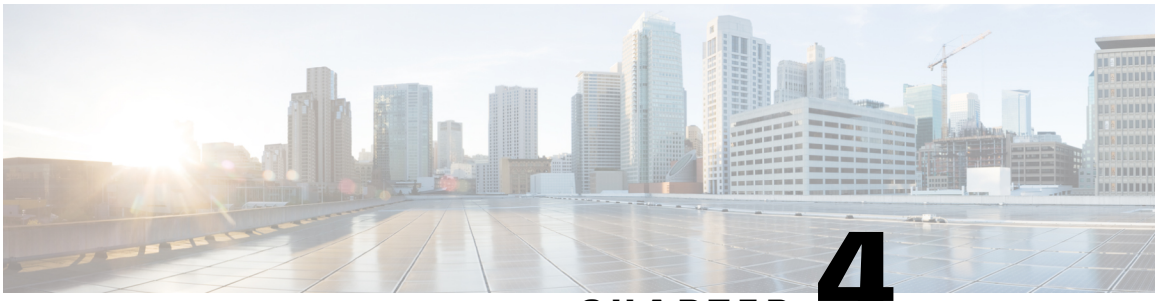
- To display a high-level overview of the entire physical system, use the **show platform** command:

```
Router# show platform
Chassis type: ISR4451/K9
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451/K9          ok                    1d01h
 0/0      ISR4400-4X1GE       ok                    1d01h
1         ISR4451/K9          ok                    1d01h
 1/0      UCS-E160DP-M1/K9    ok                    1d01h
2         ISR4451/K9          ok                    1d01h
R0        ISR4451/K9          ok, active            1d01h
```

```
F0        ISR4451/K9          ok, active            1d01h
P0        XXX-XXXX-XX         ok                    1d01h
P1        Unknown             ps,                   1d01h
P2        ACS-4450-FANASSY    ok                    1d01h

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------
0         12090323            12.2(20120829:165313)
1         12090323            12.2(20120829:165313)
2         12090323            12.2(20120829:165313)
R0        12090323            12.2(20120829:165313)
F0        12090323            12.2(20120829:165313)
```

- To verify that the router recognizes the E-Series Server, use the **show hw-module subslot all oir** command:

```
Router# show hw-module subslot all oir
Module        Model                Operational Status
------------- -------------------- ------------------------
subslot 0/0   ISR4451-X-4X1GE      ok
subslot 1/0   UCS-E140S-M1/K9      ok
subslot 2/0   UCS-E140S-M1/K9      ok
```



CHAPTER 4

Configuration Differences

This chapter includes the following sections:

Router Configuration Differences Between the Cisco SRE-V and the E-Series Server—ISR G2

The examples in the following table provide the key differences between the Cisco SRE-V and the E-Series Server configuration.

Table 5: Differences in Router Configuration Between the Cisco SRE-V and the E-Series Server—ISR G2

Cisco SRE-V Configuration	Cisco E-Series Server Configuration
interface GigabitEthernet0/0 ip address 10.0.0.1 255.0.0.0 interface sm 1/0 ip unnumbered GigabitEthernet0/0 service-module ip address 10.0.0.2 255.0.0.0 service-module ip default-gateway 10.0.0.1 interface SM1/1 switchport mode trunk ip route 10.0.0.2 255.255.255.255 sm1/0	interface GigabitEthernet0/0 ip address 10.0.0.1 255.0.0.0 interface ucse 1/0 ip unnumbered GigabitEthernet0/0 imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1 imc access-port shared-lom console interface ucse1/1 switchport mode trunk ip route 10.0.0.2 255.255.255.255 ucse1/0

Note the following differences:

- In the E-Series Server, the **sm** *slot/port* command is replaced by the **ucse** *slot/port* command.

- In the E-Series Server, the **service-module** keyword is replaced by the **imc** keyword.
- In the E-Series Server, the **default gateway** command resides in the same command line as the **imc ip address** command.
- Since the E-Series Server has different external interfaces, you must specify the access port using the **imc access-port** command.
- In the E-Series Server, you can either use the dedicated interface or one of the shared local area network on motherboard (shared LOM) interfaces to configure CIMC access. See Configuring CIMC Access, on page 25.

  In the above example, the **imc access-port shared-lom console** command uses the console interface for CIMC access, where:

  - **imc access-port—**is the physical Ethernet connection to the E-Series Server.
  - **shared-lom—**is shared LOM.
  - **console—**is the router interface.

The command to session into the server has also changed:

- Cisco SRE-V uses the **service-module sm** *slot*/**0 session** command to session into the server.
- E-Series Server uses the **ucse** *slot* **session {imc | host}** command to session into the server.

Router Configuration Differences Between the ISR G2 and the Cisco ISR 4451-X

The examples in the following table provide the key differences between the ISR G2 configuration and the Cisco ISR 4451-X configuration.

Table 6: Differences in Router Configuration Between the ISR G2 and the Cisco ISR 4451-X

Cisco ISR G2 Configuration	Cisco ISR 4451-X Configuration

`interface GigabitEthernet0/0`
` ip address 10.0.0.1 255.0.0.0`
 	
`interface ucse 1/0`
` ip unnumbered GigabitEthernet0/0`
` imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1`
` imc access-port shared-lom console`
 	
`interface ucse1/1`
` switchport mode trunk`
 	
`ip route 10.0.0.2 255.255.255.255 ucse1/0`
	`interface GigabitEthernet 0/0/0`
	` ip address 10.0.0.1 255.0.0.0`
	
	`ucse subslot 1/0`
	` imc access-port ge0`
	` imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1`
	
	`interface ucse1/0/0`
	` ip unnumbered GigabitEthernet0/0/0`
	` no negotiation auto`
	` switchport mode trunk`
	
	`ip route 10.0.0.2 255.255.255.255 ucse1/0/0`

Note the following differences:

- In the Cisco ISR 4451-X, the **interface ucse** *slot/port* command is replaced by the **ucse subslot** *slot/port* and the **interface ucse** *slot/port/subport* commands.
- In the Cisco ISR 4451-X (with Cisco IOS XE Release 3.9S), the **imc access-port shared-lom** command is replaced by the **imc access-port** command.
- In the ISR G2, you can use either the dedicated interface or one of the shared local area network on motherboard (shared LOM) interfaces to configure CIMC access.

  In the Cisco ISR 4451-X, you can use either the management interface or one of the NIC interfaces to configure CIMC access. See Configuring CIMC Access, on page 25.

  In the above example, the command configures CIMC access using the E-Series Server's internal GE0 NIC interface, where:

  - **imc access-port—**CIMC access port configuration.
  - **ge0—**E-Series Server's internal GE0 NIC interface.

The command to session into the server has also changed:

- In the ISR G2, you use the **ucse** *slot* **session {imc | host}** command to session into the server.
- In the Cisco ISR 4451-X, you use the **hw-module subslot** *slot*/**0 session {imc | server}** command to session into the server.

VMware vSphere Hypervisor Configuration Differences

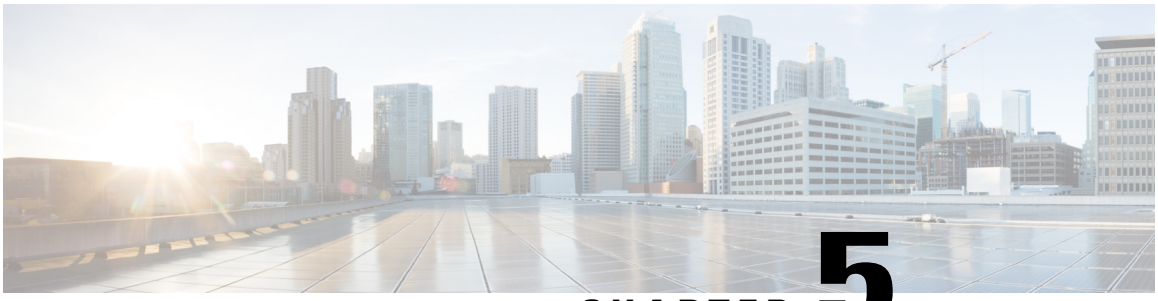
In the Cisco SRE-V, the IP address of the VMware vSphere Hypervisor™ host is the same as the IP address of the service module. For example, in the Cisco SRE-V, **service-module ip address 10.0.0.2** (see table) is also assigned to the VMware vSphere Hypervisor™ host.

Table 7: Differences in Router Configuration Between the Cisco SRE-V and the E-Series Server—ISR G2

Cisco SRE-V Configuration	Cisco E-Series Server Configuration
interface GigabitEthernet0/0 ip address 10.0.0.1 255.0.0.0 interface sm 1/0 ip unnumbered GigabitEthernet0/0 **service-module ip address 10.0.0.2** 255.0.0.0 service-module ip default-gateway 10.0.0.1 interface SM1/1 switchport mode trunk ip route 10.0.0.2 255.255.255.255 sm1/0	interface GigabitEthernet0/0 ip address 10.0.0.1 255.0.0.0 interface ucse 1/0 ip unnumbered GigabitEthernet0/0 **imc ip address 10.0.0.2** 255.0.0.0 default-gateway 10.0.0.1 imc access-port shared-lom console interface ucse1/1 switchport mode trunk ip route 10.0.0.2 255.255.255.255 ucse1/0

However, with the E-Series Server, the IMC IP address, which is also 10.0.0.2 (see the example above), is reserved for CIMC access. You enter this IP address (10.0.0.2) on your web browser to access the CIMC GUI.

In the E-Series Server, either the VMware vSphere Hypervisor™ assigns an IP address to the host using DHCP, or you can choose to assign a static IP address to the VMware vSphere Hypervisor™ host. See Assigning a Static IP Address to the VMware vSphere Hypervisor, on page 79.



CHAPTER 5

Configuring CIMC Access

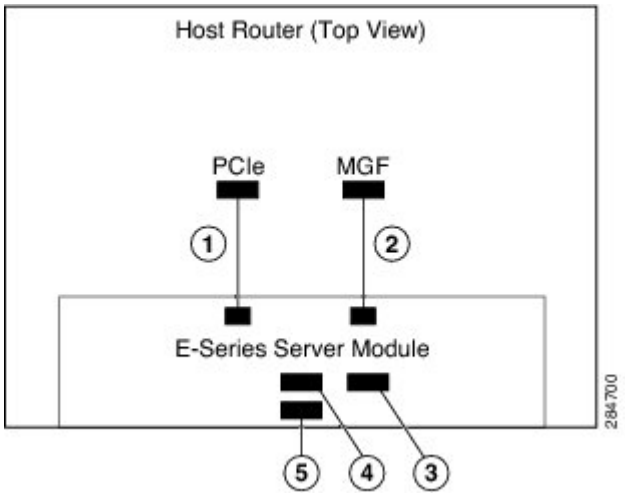
This chapter provides an overview of the E-Series Server interfaces and provides procedures to configure CIMC access when the E-Series Server is installed in ISR G2 and the Cisco ISR 4451-X. It contains the following sections:

Configuring CIMC Access - ISR G2

E-Series Server Interfaces Overview—ISR G2

The following figure shows the interfaces in a double-wide E-Series Server and the ISR G2 host router.

Figure 8: Interfaces in a Double-Wide E-Series Server



	Interface	Interface Location	Description
1	Router's PCIe *slot*/**0** Interface	Internal Interface	Also called Console interface. This interface connects the router's PCIe interface to the E-Series Server. The PCIe interface provides an internal Layer 3 GE link between the router and the E-Series Server. It can be used both for CIMC configuration and for host operating system configuration.
2	Router's MGF *slot*/**1** VLAN Interface	Internal Interface	Used to access CIMC over a high-speed backplane switch. The MGF VLAN interface provides an internal Layer 2 GE link between the router and the E-Series Server. This interface can be used both for CIMC configuration and for host operating system configuration.
3	Management (Dedicated) Interface	External Interface	Used for CIMC configuration and management.

4	GE3 Interface	External Interface	Used as a primary interface or as a backup interface. This interface can be used both for CIMC configuration and for host operating system configuration. **Note** The GE3 interface is only available on the double-wide E-Series Servers.
5	GE2 Interface	External Interface	Used as a primary interface or as a backup interface. This interface can be used both for CIMC configuration and for host operating system configuration.

CIMC Access Configuration Options—ISR G2

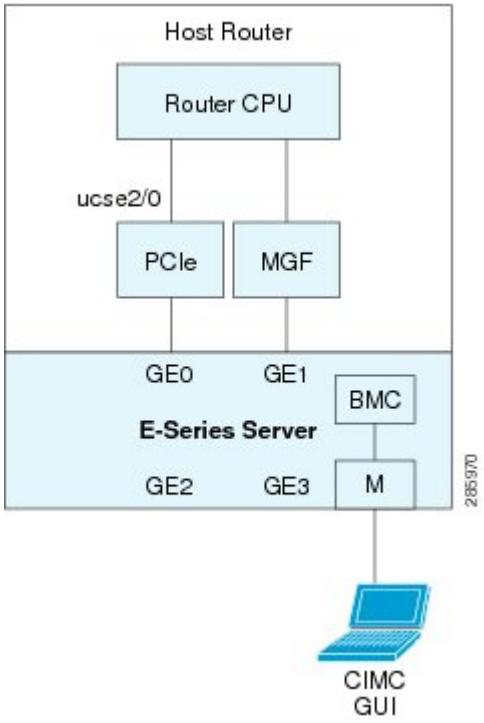
Depending on whether you are a remote user or a local user, do one of the following to configure CIMC access.

- If you are a remote user, use either the external Management (dedicated) interface or one of the following shared LOM interfaces to configure CIMC access:
  - Router's internal PCIe *slot*/**0** Console interface
  - Router's internal MGF *slot*/**1** VLAN interface
  - E-Series Server's external GE2 or GE3 interface
- If you are a local user, use the Cisco IOS CLI or the CIMC Configuration Utility to configure CIMC access.

Configuring CIMC Access Using the E-Series Server's External Management (Dedicated) Interface—ISR G2

See the following figure and the procedure that follows to configure CIMC access using the E-Series Server's external Management (dedicated) interface.

Figure 9: Configuring CIMC Access Using the E-Series Server's External Management (Dedicated) Interface



Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.
- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.

	Command or Action	Purpose
Step 3	Router (config)# **interface ucse** *slot/port*	Enters interface configuration mode for the slot and port where the E-Series Server is installed.
Step 4	Router (config-if)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router. • *cimc-gateway-ip-address*— IP address for the default gateway.
Step 5	Router (config-if)# **imc access-port dedicated**	Configures CIMC access through the server's external Management (dedicated) interface. See # 3 in E-Series Server Interfaces Overview—ISR G2.
Step 6	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 7	Router (config-if)# **end**	Exits configuration mode.
Step 8	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.
Step 9	Router# **copy running-config startup-config**	(Optional) Saves the new running configuration of the router as the startup configuration.

This example shows how to configure CIMC access using the server's external IMC dedicated interface:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# interface ucse 2/0
Router(config-if)# imc ip address 10.0.0.1 255.0.0.0 default-gateway 10.0.0.2
Router(config-if)# imc access-port dedicated
Router(config-if)# no shut
Router(config-if)# end

Router# show running-config
Router# copy running-config startup-config
```

Configuring CIMC Access Using Shared LOM—ISR G2

Use one of the following shared LOM interfaces to configure CIMC access:

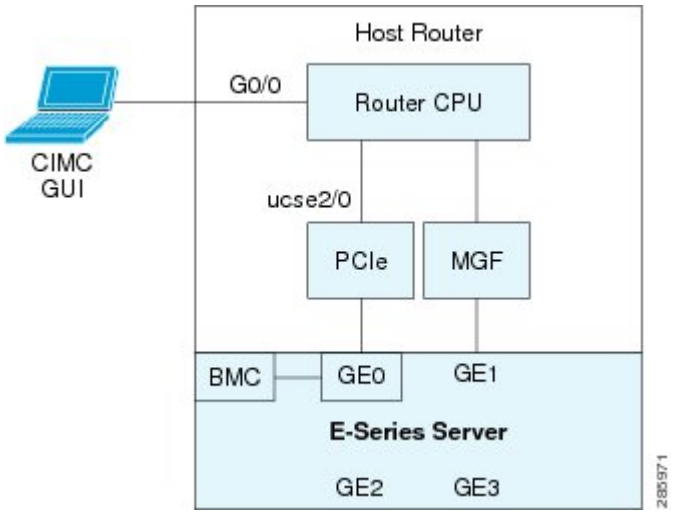
- Router's internal PCIe *slot*/**0** Console interface
- Router's internal MGF *slot*/**1** VLAN interface

- E-Series Server's external GE2 or GE3 interface

Configuring CIMC Access Using the Router's Internal PCIe Slot/0 Console Interface—ISR G2

See the following figure and the procedure that follows to configure CIMC access using the router's internal PCIe *slot*/**0** Console interface.

Figure 10: Configuring CIMC Access Using the Router's Internal PCIe Slot/0 Console Interface



Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.
- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface GigabitEthernet0/0**	Enters interface configuration mode for Gigabit Ethernet 0/0.
Step 4	Router (config-if)# **ip address** *ip-address subnet mask*	Specifies the IP address and subnet mask of the interface.

	Command or Action	Purpose
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **end**	Exits configuration mode.
Step 7	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 8	Router (config)# **interface ucse** *slot/port*	Enters interface configuration mode for the slot and port where the E-Series Server is installed.
Step 9	Router (config-if)# **ip unnumbered** *type number*	The **ip unnumbered** command enables IP processing on an interface without assigning an explicit IP address to that interface. • *type*—Type of interface on which the router has an assigned IP address. • *number*—Number of the interface and subinterface on which the router has an assigned IP address. **Note** The unnumbered interface must be unique. It cannot be another unnumbered interface. When you use the **ip unnumbered** command, you must use the **ip route** command to create a static route. **Caution** The **ip unnumbered** and **ipv6 unnumbered** commands create a point-to-point interface between devices. Broadcasting is not supported.
Step 10	Router (config-if)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router. • *cimc-gateway-ip-address*— IP address for the default gateway.
Step 11	Router (config-if)# **imc access-port shared-lom console**	Configures CIMC access using the router's PCIe slot/0 (console) interface. See # 1 in E-Series Server Interfaces Overview—ISR G2.
Step 12	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 13	Router (config-if)# **end**	Exits configuration mode.
Step 14	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 15	Router (config)# **ip route** *cimc-ip-address subnet-mask* **ucse** *slot/port*	Creates a static route. • *cimc-ip-address*—IP address of CIMC.

	Command or Action	Purpose
		• *slot/port*—Slot and port where the E-Series Server is installed.
Step 16	Router (config-if)# **end**	Exits configuration mode.
Step 17	Router# **ping** *cimc-ip-address*	Verifies connection from the router to CIMC through the router's internal PCIe *slot*/**0** console interface.
Step 18	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.
Step 19	Router# **copy running-config startup-config**	(Optional) Saves the new running configuration of the router as the startup configuration.

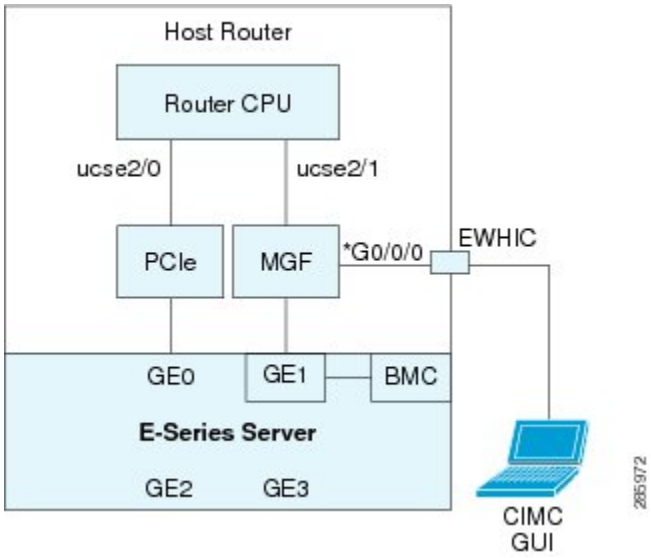
This example shows how to configure CIMC access using the server's internal PCIe *slot*/**0** console interface:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# end

Router# configure terminal
Router(config)# interface ucse 2/0
Router(config)# ip unnumbered GigabitEthernet0/0
Router(config-if)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-if)# imc access-port shared-lom console
Router(config-if)# no shut
Router(config)# end

Router# configure terminal
Router(config)# ip route 10.0.0.2 255.255.255.255 ucse 2/0
Router(config)# end

Router# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router# show running-config
Router# copy running-config startup-config
```

Configuring CIMC Access Using the Router's Internal MGF Slot/1 VLAN Interface—ISR G2

See the following figure and the procedure that follows to configure CIMC access using the router's internal MGF *slot*/**1** VLAN interface.

Figure 11: Configuring CIMC Access Using the Router's Internal MGF Slot/1 VLAN Interface



Note * For a list of supported Cisco EtherSwitch EHWICs, see Supported Cisco EtherSwitch EHWIC and Cisco EtherSwitch Service Modules.

Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.
- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **show vlan-switch**	Displays VLANs.
Step 3	Router# **configure terminal**	Enters global configuration mode on the host router.

	Command or Action	Purpose
Step 4	Router (config)# **interface vlan** *vlan-number*	Enters VLAN configuration mode for the specified VLAN number.
Step 5	Router (config-if)# **ip address** *vlan-ip-address subnet mask*	Specifies the IP address for the VLAN. • *vlan-ip-address*—IP address of the VLAN. • *subnet-mask*—Subnet mask to append to the IP address.
Step 6	Router (config-if)# **end**	Exits configuration mode.
Step 7	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 8	Router (config)# **interface ucse** *slot/port*	Enters interface configuration mode for the slot and port where the E-Series Server is installed.
Step 9	Router (config-if)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router. • *cimc-gateway-ip-address*— IP address for the default gateway.
Step 10	Router (config-if)# **imc access-port shared-lom GE1**	Configures CIMC access using the router's internal *slot*/**1** MGF VLAN interface. See # 2 in E-Series Server Interfaces Overview—ISR G2.
Step 11	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 12	Router (config-if)# **end**	Exits configuration mode.
Step 13	Router# **ping** *cimc-ip-address*	Verifies connection from the router to CIMC through the router's internal MGF*slot*/**1** VLAN interface.
Step 14	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.
Step 15	Router# **copy running-config startup-config**	(Optional) Saves the new running configuration of the router as the startup configuration.

This example shows how to configure CIMC access using the router's internal MGF *slot*/**1** VLAN interface:

```
Router> enable
Router> password
Router> show vlan-switch
VLAN Name                             Status    Ports
```

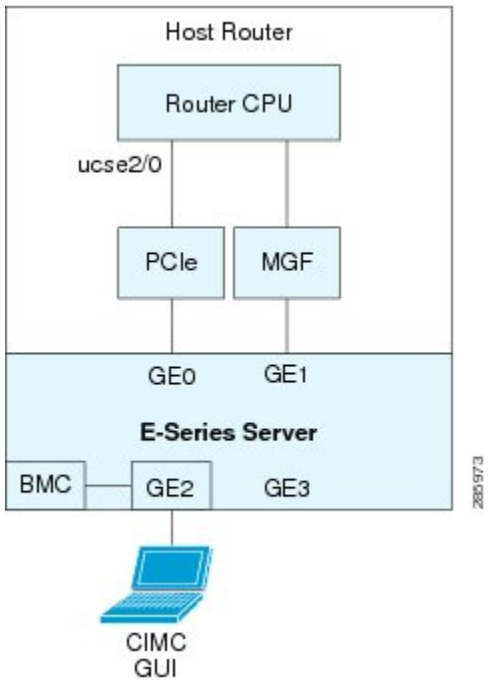
```
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0/0, Gi0/0/1, Gi0/0/2
                                                Gi0/0/3, uc2/1
Router# configure terminal
Router(config)# interface vlan 1
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# end

Router# configure terminal
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-if)# imc access-port shared-lom GE1
Router(config-if)# no shut
Router(config-if)# end

Router# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router# show running-config
Router# copy running-config startup-config
```

Configuring CIMC Access Using the E-Series Server's External GE2 or GE3 Interface—ISR G2

See the following figure and the procedure that follows to configure CIMC access using the E-Series Server's external GE2 or GE3 interface.

Note This figure shows how to configure CIMC access using the E-Series Server's external GE2 interface.

Figure 12: Configuring CIMC Access Using the E-Series Server's External GE2 Interface



Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.
- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface ucse** *slot/port*	Enters interface configuration mode for the slot and port where the E-Series Server is installed.
Step 4	Router (config-if)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router. • *cimc-gateway-ip-address*— IP address for the default gateway.
Step 5	Router (config-if)# **imc access-port shared-lom** {**GE2** | **GE3**}	Configures CIMC access through E-Series Server's external GE2 or GE3 interface. See # 4 and 5 in E-Series Server Interfaces Overview—ISR G2.
Step 6	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 7	Router (config-if)# **end**	Exits configuration mode.
Step 8	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.
Step 9	Router# **copy running-config startup-config**	(Optional) Saves the new running configuration of the router as the startup configuration.

This example shows how to configure CIMC access using the server's external GE2 interface:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# interface ucse 2/0
```

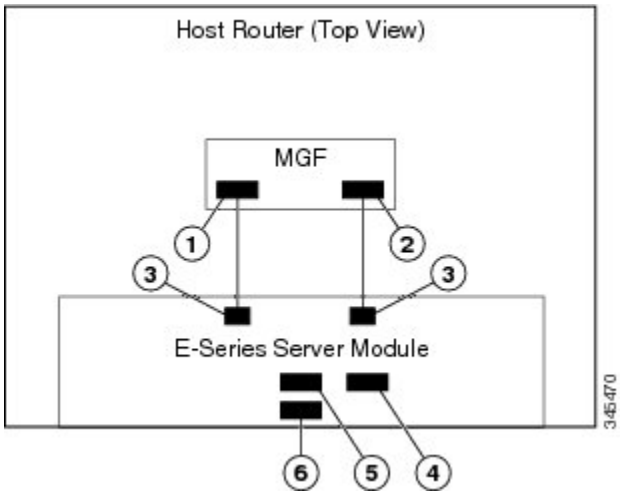
```
Router(config-if)# imc ip address 10.0.0.1 255.0.0.0 default-gateway 10.0.0.2
Router(config-if)# imc access-port shared-lom GE2
Router(config-if)# no shut
Router(config-if)# end

Router# show running-config
Router# copy running-config startup-config
```

Configuring CIMC Access - Cisco ISR 4451-X

E-Series Server Interfaces Overview—Cisco ISR 4451-X

The following figure shows the interfaces in a double-wide E-Series Server and the Cisco ISR 4451-X host router.

Figure 13: Interfaces in a Double-Wide E-Series Server



	Interface	Interface Location	Description
1	Router's **ucse** *slot*/**0/0** Interface	Internal Interface	Used to access CIMC over a high-speed backplane switch. The MGF interface provides an internal Layer 2 GE link between the router and the E-Series Server. This interface can be used both for CIMC configuration and for host operating system configuration. **Note** This interface is used to access the E-Series Server's internal GE0 interface.

2	Router's **ucse** *slot*/**0/1** Interface	Internal Interface	Used to access CIMC over a high-speed backplane switch. The MGF interface provides an internal Layer 2 GE link between the router and the E-Series Server. This interface can be used both for CIMC configuration and for host operating system configuration. **Note** This interface is used to access the E-Series Server's internal GE1 interface.
3	GE0 and GE1 Interfaces	Internal Interfaces	E-Series Server's internal NIC interfaces.
4	Management (Dedicated) Interface	External Interface	Used for CIMC configuration and management.
5	GE3 Interface	External Interface	Can be used both for CIMC configuration and for host operating system configuration. **Note** The GE3 interface is only available on the double-wide E-Series Servers.
6	GE2 Interface	External Interface	Can be used both for CIMC configuration and for host operating system configuration.

CIMC Access Configuration Options—Cisco ISR 4451-X

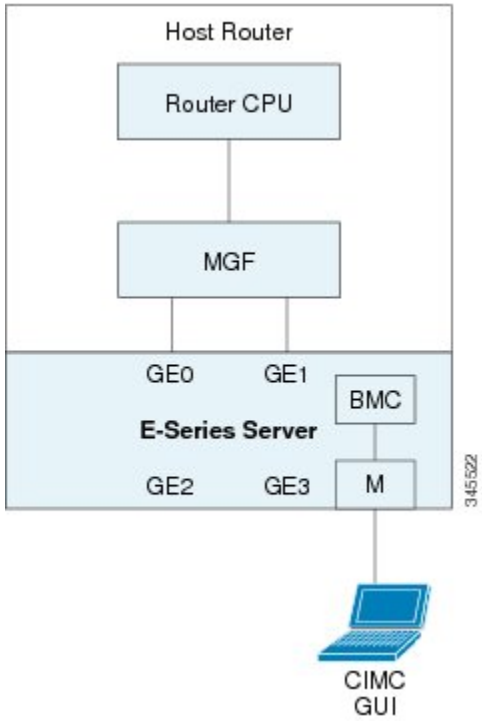
Depending on whether you are a remote user or a local user, do one of the following to configure CIMC access.

- If you are a remote user, use the Cisco IOS CLI to configure CIMC access by using one of the following interfaces:
  - CIMC Management (dedicated) interface
  - E-Series Server's internal GE0 and the router's **ucse** *slot*/**0/0** interface
  - E-Series Server's internal GE1 interface and the router's **ucse** *slot*/**0/1** interface
  - E-Series Server's external GE2 or GE3 interface
- If you are a local user, use the CIMC Configuration Utility or the Cisco IOS CLI (mentioned above) to configure CIMC access.

Configuring CIMC Access Using the E-Series Server's External Management (Dedicated) Interface—Cisco ISR 4451-X

See the following figure and the procedure that follows to configure CIMC access using the E-Series Server's external Management (dedicated) interface.

Figure 14: Configuring CIMC Access Using the E-Series Server's External Management (Dedicated) Interface



Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.
- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.

	Command or Action	Purpose
Step 3	Router (config)# **ucse subslot** *slot/port*	Enters ucse interface configuration mode for the slot and port where the E-Series Server is installed.
Step 4	Router (config-ucse)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router. • *cimc-gateway-ip-address*—IP address for the default gateway.
Step 5	Router (config-ucse)# **imc access-port mgmt** or Router (config-ucse)# **imc access-port dedicated**	Configures CIMC access through the server's external Management (dedicated) interface. See # 4 in E-Series Server Interfaces Overview—Cisco ISR 4451-X, on page 37. • Use the **imc access-port mgmt** command if you installed the Cisco IOS XE Release 3.9S. • Use the **imc access-port dedicated** command if you installed the Cisco IOS XE Release 3.10S and later versions.
Step 6	Router (config-ucse)# **end**	Returns to privileged EXEC mode on the host router.
Step 7	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.
Step 8	Router# **copy running-config startup-config**	(Optional) Saves the new running configuration of the router as the startup configuration.

This example shows how to configure CIMC access using the server's external management interface—Applicable only with Cisco IOS XE Release 3.9S:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.1 255.0.0.0 default-gateway 10.0.0.2
Router(config-ucse)# imc access-port mgmt
Router(config-ucse)# end

Router# show running-config
Router# copy running-config startup-config
```

This example shows how to configure CIMC access using the server's external dedicated interface—Applicable with Cisco IOS XE Release 3.10S and later versions:

```
Router> enable
```

```
Router> password
Router# configure terminal

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.1 255.0.0.0 default-gateway 10.0.0.2
Router(config-ucse)# imc access-port dedicated
Router(config-ucse)# end

Router# show running-config
Router# copy running-config startup-config
```

Configuring CIMC Access Using the E-Series Server's NIC Interfaces—Cisco ISR 4451-X

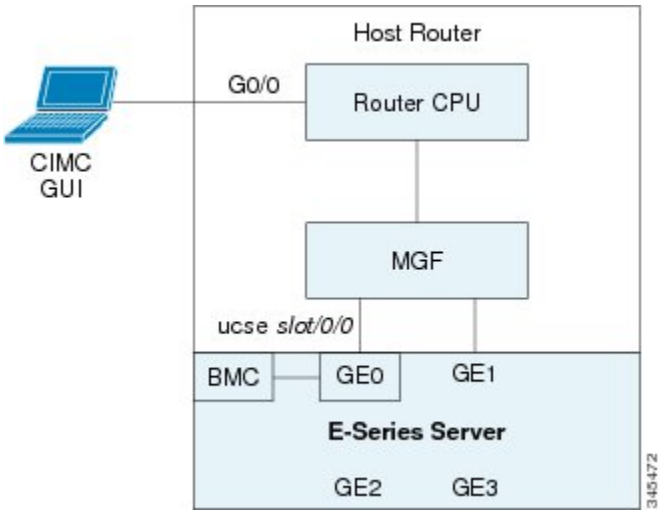
Use one of the following E-Series Server's NIC interfaces to access CIMC:

- E-Series Server's internal GE0 and the router's **ucse** *slot*/**0/0** interface
- E-Series Server's internal GE1 interface and the router's **ucse** *slot*/**0/1** interface
- E-Series Server's external GE2 or GE3 interface

Configuring CIMC Access Using the E-Series Server's Internal GE0 Interface and the Cisco ISR 4451-X ucse *slot*/0/0 Interface

See the following figure and the procedure that follows to configure CIMC access using the E-Series Server's internal GE0 interface and the router's ucse *slot*/**0/0** interface.

Figure 15: Configuring CIMC Access Using the E-Series Server's Internal GE0 Interface and the Router's ucse slot/0/0 Interface



Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.

- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface GigabitEthernet 0/0/0**	Enters interface configuration mode for Gigabit Ethernet interface 0/0/0.
Step 4	Router (config-if)# **ip address** *ip-address subnet-mask*	Specifies the IP address and subnet mask of the interface.
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **exit**	Exits interface configuration mode.
Step 7	Router (config)# **interface ucse** *slot*/**0/0**	Enters ucse interface configuration mode for the slot, port, and subport where the E-Series Server is installed.
Step 8	Router (config-if)# **ip unnumbered** *type number*	The **ip unnumbered** command enables IP processing on an interface without assigning an explicit IP address to that interface. • *type*—Type of interface on which the router has an assigned IP address. • *number*—Number of the interface and subinterface on which the router has an assigned IP address. **Note** The unnumbered interface must be unique. It cannot be another unnumbered interface. When you use the **ip unnumbered** command, you must use the **ip route** command to create a static route. **Caution** The **ip unnumbered** and **ipv6 unnumbered** commands create a point-to-point interface between devices. Broadcasting is not supported.
Step 9	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 10	Router (config-if)# **exit**	Exits interface configuration mode.
Step 11	Router (config)# **ucse subslot** *slot/port*	Enters ucse interface configuration mode for the slot and port where the E-Series Server is installed.
Step 12	Router (config-ucse)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router.

	Command or Action	Purpose
		• *cimc-gateway-ip-address*—IP address for the default gateway.
Step 13	Router (config-ucse)# **imc access-port ge0** or Router (config-ucse)# **imc access-port shared-lom console**	Configures CIMC access using the E-Series Server's internal GE0 or console interface. See # 3 in E-Series Server Interfaces Overview—Cisco ISR 4451-X, on page 37. • Use the **imc access-port ge0** command if you installed the Cisco IOS XE Release 3.9S. • Use the **imc access-port shared-lom console** command if you installed the Cisco IOS XE Release 3.10S and later versions.
Step 14	Router (config-ucse)# **exit**	Exits ucse interface configuration mode.
Step 15	Router (config)# **ip route** *cimc-ip-address subnet-mask* **ucse** *slot/port/subport*	Creates a static route. • *cimc-ip-address*—IP address of CIMC. • *slot/port/subport*—Slot, port, and subport where the E-Series Server is installed.
Step 16	Router (config)# **end**	Exits configuration mode.
Step 17	Router# **ping** *cimc-ip-address*	Verifies the connection from the router to CIMC through the **ucse** *slot*/**0/0** interface.
Step 18	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.
Step 19	Router# **copy running-config startup-config**	(Optional) Saves the new running configuration of the router as the startup configuration.

This example shows how to configure CIMC access using the E-Series Server's internal GE0 interface and the router's ucse *slot*/**0/0** interface—Applicable only with Cisco IOS XE Release 3.9S:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# interface ucse 1/0/0
Router(config-if)# ip unnumbered GigabitEthernet0/0/0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-ucse)# imc access-port ge0
```

```
Router(config-ucse)# exit

Router(config)# ip route 10.0.0.2 255.255.255.255 ucse 1/0/0
Router(config)# end

Router# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router# show running-config
Router# copy running-config startup-config
```

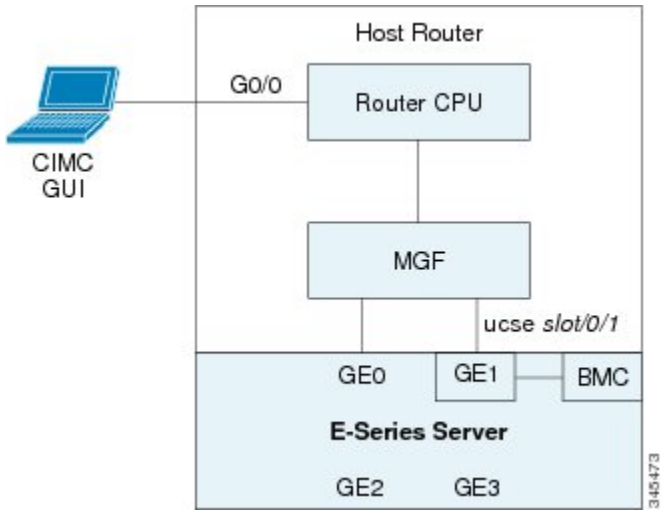
This example shows how to configure CIMC access using the E-Series Server's internal console interface and the router's ucse *slot*/**0/0** interface**—**Applicable with Cisco IOS XE Release 3.10S and later versions:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# interface ucse 1/0/0
Router(config-if)# ip unnumbered GigabitEthernet0/0/0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-ucse)# imc access-port shared-lom console
Router(config-ucse)# exit

Router(config)# ip route 10.0.0.2 255.255.255.255 ucse 1/0/0
Router(config)# end

Router# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router# show running-config
Router# copy running-config startup-config
```

Configuring CIMC Access Using the E-Series Server's Internal GE1 Interface and the Cisco ISR 4451-X ucse *slot*/0/1 Interface

See the following figure and the procedure that follows to configure CIMC access using the E-Series Server's internal GE1 interface and the router's ucse *slot*/**0/1** interface.

Figure 16: Configuring CIMC Access Using the E-Series Server's Internal GE1 Interface and the Router's ucse slot/0/1 Interface



Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.
- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface GigabitEthernet 0/0/0**	Enters interface configuration mode for Gigabit Ethernet interface 0/0/0.
Step 4	Router (config-if)# **ip address** *ip-address subnet-mask*	Specifies the IP address and subnet mask of the interface.
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.

	Command or Action	Purpose
Step 6	Router (config-if)# **exit**	Exits interface configuration mode.
Step 7	Router (config)# **interface ucse** *slot*/**0/1**	Enters ucse interface configuration mode for the slot, port, and subport where the E-Series Server is installed.
Step 8	Router (config-if)# **ip unnumbered** *type number*	The **ip unnumbered** command enables IP processing on an interface without assigning an explicit IP address to that interface. • *type*—Type of interface on which the router has an assigned IP address. • *number*—Number of the interface and subinterface on which the router has an assigned IP address. **Note** The unnumbered interface must be unique. It cannot be another unnumbered interface. When you use the **ip unnumbered** command, you must use the **ip route** command to create a static route. **Caution** The **ip unnumbered** and **ipv6 unnumbered** commands create a point-to-point interface between devices. Broadcasting is not supported.
Step 9	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 10	Router (config-if)# **exit**	Exits interface configuration mode.
Step 11	Router (config)# **ucse subslot** *slot/port*	Enters ucse interface configuration mode for the slot and port where the E-Series Server is installed.
Step 12	Router (config-ucse)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router. • *cimc-gateway-ip-address*—IP address for the default gateway.
Step 13	Router (config-ucse)# **imc access-port ge1** or Router (config-ucse)# **imc access-port shared-lom ge1**	Configures CIMC access using the E-Series Server's internal GE1 interface. See # 3 in E-Series Server Interfaces Overview—Cisco ISR 4451-X, on page 37. • Use the **imc access-port ge1** command if you installed the Cisco IOS XE Release 3.9S. • Use the **imc access-port shared-lom ge1** command if you installed the Cisco IOS XE Release 3.10S and later versions.

	Command or Action	Purpose
Step 14	Router (config-ucse)# **exit**	Exits ucse interface configuration mode.
Step 15	Router (config)# **ip route** *cimc-ip-address subnet-mask* **ucse** *slot/port/subport*	Creates a static route. • *cimc-ip-address*—IP address of CIMC. • *slot/port/subport*—Slot, port, and subport where the E-Series Server is installed.
Step 16	Router (config)# **end**	Exits configuration mode.
Step 17	Router# **ping** *cimc-ip-address*	Verifies the connection from the router to CIMC through the **ucse** *slot*/**0/1** interface.
Step 18	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.
Step 19	Router# **copy running-config startup-config**	(Optional) Saves the new running configuration of the router as the startup configuration.

This example shows how to configure CIMC access using the E-Series Server's internal GE1 interface and the router's ucse *slot*/**0/1** interface—Applicable only with Cisco IOS XE Release 3.9S:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# interface ucse 1/0/1
Router(config-if)# ip unnumbered GigabitEthernet0/0/0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-ucse)# imc access-port ge1
Router(config-ucse)# exit

Router(config)# ip route 10.0.0.2 255.255.255.255 ucse 1/0/1
Router(config)# end

Router# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router# show running-config
Router# copy running-config startup-config
```

This example shows how to configure CIMC access using the E-Series Server's internal GE1 interface and the router's ucse *slot*/**0/1** interface—Applicable with Cisco IOS XE Release 3.10S and later releases:

```
Router> enable
```

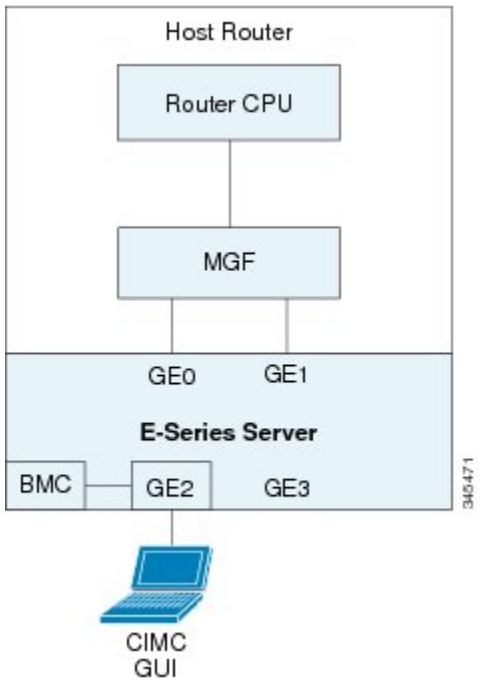
```
Router> password
Router# configure terminal

Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# interface ucse 1/0/1
Router(config-if)# ip unnumbered GigabitEthernet0/0/0
Router(config-if)# no shut
Router(config-if)# exit

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-ucse)# imc access-port shared-lom ge1
Router(config-ucse)# exit

Router(config)# ip route 10.0.0.2 255.255.255.255 ucse 1/0/1
Router(config)# end

Router# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router# show running-config
Router# copy running-config startup-config
```

Configuring CIMC Access Using the E-Series Server's External GE2 or GE3 Interface—Cisco ISR 4451-X

See the following figure and the procedure that follows to configure CIMC access using the E-Series Server's external GE2 or GE3 interface.

Note This figure shows how to configure CIMC access using the E-Series Server's external GE2 interface.

Figure 17: Configuring CIMC Access Using the E-Series Server's External GE2 Interface



Before You Begin

Make sure that you have the following information:

- IP address of CIMC.
- Username and password for logging in to the router.
- Slot and port number of the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **ucse subslot** *slot/port*	Enters ucse interface configuration mode for the slot and port where the E-Series Server is installed.

	Command or Action	Purpose
Step 4	Router (config-ucse)# **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*	Specifies the IP address of CIMC and the IP address of the default gateway that CIMC must use. • *cimc-ip-address*—IP address of CIMC. • *subnet-mask*—Subnet mask used to append to the IP address; must be in the same subnet as the host router. • *cimc-gateway-ip-address*—IP address for the default gateway.
Step 5	Router (config-ucse)# **imc access-port** {**GE2** | **GE3**} or Router (config-ucse)# **imc access-port shared-lom** {**GE2** | **GE3**}	Configures CIMC access through the E-Series Server's external GE2 or GE3 interface. See # 5 and 6 in E-Series Server Interfaces Overview—Cisco ISR 4451-X, on page 37. • Use the **imc access-port** {**GE2** | **GE3**} command if you installed the Cisco IOS XE Release 3.9S. • Use the **imc access-port shared-lom** {**GE2** | **GE3**} command if you installed the Cisco IOS XE Release 3.10S and later versions.
Step 6	Router (config-ucse)# **end**	Returns to privileged EXEC mode on the host router.
Step 7	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.

This example shows how to configure CIMC access using the server's external GE2 interface—Applicable only with Cisco IOS XE Release 3.9S:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.1 255.0.0.0 default-gateway 10.0.0.2
Router(config-ucse)# imc access-port GE2
Router(config-ucse)# no shut
Router(config-ucse)# end

Router# show running-config
```

This example shows how to configure CIMC access using the server's external GE2 interface—Applicable with Cisco IOS XE Release 3.10S and later releases:

```
Router> enable
Router> password
Router# configure terminal

Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip address 10.0.0.1 255.0.0.0 default-gateway 10.0.0.2
Router(config-ucse)# imc access-port shared-lom GE2
Router(config-ucse)# no shut
Router(config-ucse)# end
```

```
Router# show running-config
```

Configuring CIMC Access Using the CIMC Configuration Utility

If you are a local user, you can use either the Cisco IOS CLI or the CIMC Configuration Utility to configure CIMC access. To configure CIMC access using the Cisco IOS CLI, see Configuring CIMC Access Using the Cisco IOS CLI.

Note When you use the CIMC Configuration Utility to configure CIMC access, the configuration is not reflected as Cisco IOS configuration. In other words, if you execute the **show running-config** command from the Cisco IOS CLI, the changes that you made using the CIMC Configuration Utility are not reflected.

Procedure

Step 1 Power on the router.

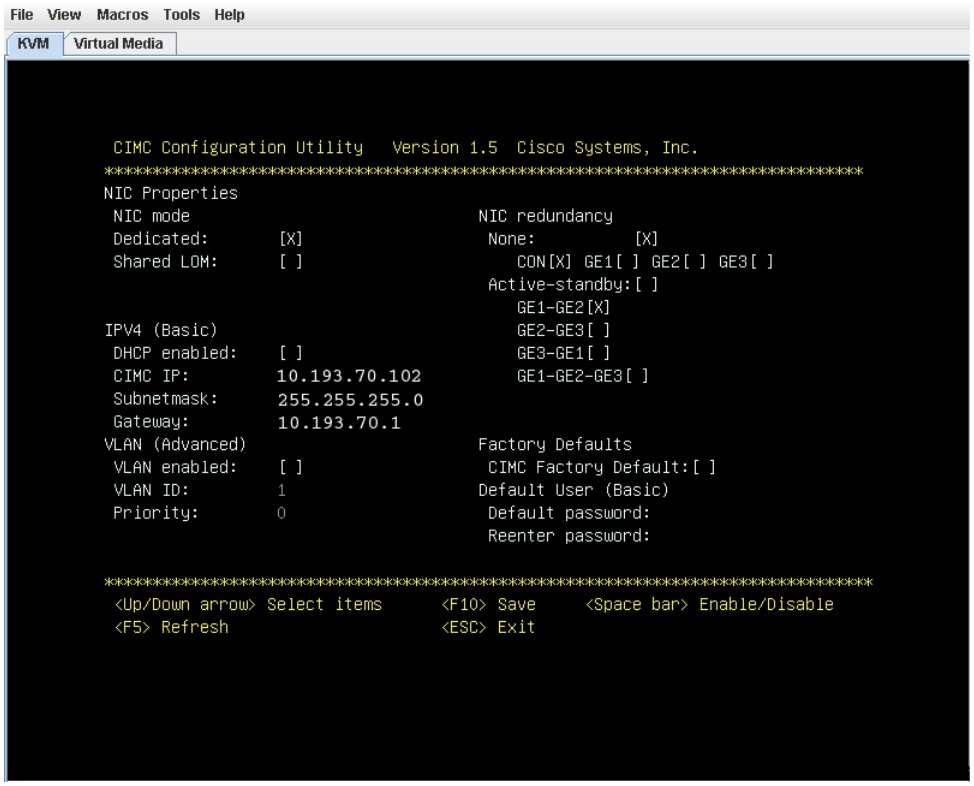
Step 2 Connect a keyboard and monitor to the front panel of the E-Series Server.

Step 3 Press the **Power** button to boot the E-Series Server. During bootup, watch for the prompt to press **F8**.

Step 4 When you see the prompt, press **F8**.

The **CIMC Configuration Utility** appears.

Figure 18: CIMC Configuration Utility



Step 5 Use the CIMC configuration Utility to set the NIC mode and NIC redundancy, and to choose whether to enable DHCP or set static network settings.

a) From the **NIC mode** area, choose a port to access CIMC. Options are:

- Dedicated—The 10/100 IMC port is used to access CIMC.
- Shared LOM (default)—The four 1Gb Ethernet ports are used to access the CIMC. This is the factory default setting.

b) From the **NIC redundancy** area, choose the NIC redundancy. Options are:

- None—The Ethernet ports operate independently and do not fail over if there is a problem.
- Active-standby—If an active Ethernet port fails, the traffic falls over to a standby port. This is the factory default setting.

c) From the **IPV4 (Basic)** area, do one of the following:

- DHCP Enabled—Select this option to enable DHCP for dynamic network settings. Before you enable DHCP, your DHCP server must be preconfigured with the range of MAC addresses for this server. The MAC address is printed on a label on the rear of the server. This server has a range of six MAC

addresses assigned to CIMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

- CIMC IP—IP address of CIMC.

  Subnet Mask—Enter the subnet mask to append to the CIMC IP address; must be in the same subnet as the host router.

  Gateway—IP address of the default gateway router.

d) (Optional) From the **VLAN (Advanced)** area, configure VLAN settings.
e) Press **F5** to refresh the page and have the new settings appear.
The page refresh takes approximately 45 seconds.
f) Press **F10** to save your settings and reboot the server.
If you chose to enable DHCP, the dynamically assigned IP and MAC addresses are displayed on the console screen during bootup.

Step 6 Using the ports that you selected for the NIC Mode settings in Step 5, substep a, connect Ethernet cables from your LAN to the E-Series Server.

Step 7 In your web browser, enter the IP address that you configured to access CIMC. The CIMC IP address is based upon the settings that you configured in Step 5, substep c (either a static IP address or the IP address assigned by your DHCP server).
The default user name to log into CIMC is **admin** and the default password is **password**.

Step 8 Use the CIMC GUI or CIMC CLI to manage and monitor the server.
See the *GUI Configuration Guide for Cisco UCS E-Series Servers* or the *CLI Configuration Guide for Cisco UCS E-Series Servers*.

Defining Network Static Settings Using a Script File

Use this procedure to define static network settings for multiple servers by automating the configuration process with a script file.

Procedure

Step 1 Use a text editor to create a file named **network.cfg**.

Step 2 Create the contents of **network.cfg** in the following format by using only the tags that you want to set:

```
dhcp-enabled:
v4-addr:
v4-netmask:
v4-gateway:
vlan-enabled:
vlan-id:
vlan-priority:
password:
mode:
redundancy:
```

For example, to disable DHCP, set the IP address, subnet mask, gateway, and user password, use the following sample values:

```
dhcp-enabled: 0
v4-addr: 10.193.70.102
v4-netmask: 255.255.255.0
v4-gateway: 10.193.70.1
password: nonpasswd
mode:
redundancy:
```

Step 3 Use a text editor to create a file named **startup.nsh** with the following contents:

```
fs0:
cimcconfig
```

Step 4 Copy your **network.cfg** file and your **startup.nsh** file to a USB thumb drive.

Step 5 Insert the USB thumb drive into a USB port on the server.

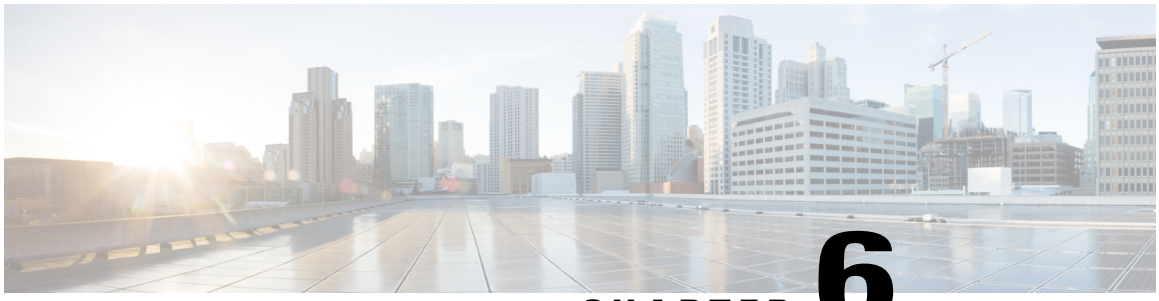
Step 6 Press and release the **Power** button to boot the server.

Step 7 Observe the booting process and press **F6** when prompted to enter the BIOS Boot Manager.

Step 8 Select EFI as the boot device and then press **Enter**.
The server power-cycles and launches the configuration utility, which runs the **startup.nsh** file. Any errors are displayed on the screen and on an **errors.txt** file.

Step 9 Remove the USB thumb drive, alter the **network.cfg** file with your next IP address, and then insert the USB thumb drive into the next server that you want to configure.

Step 10 After the server has been assigned an IP address, you can use that address to access the service processor's GUI or CLI management system.



CHAPTER 6

Accessing CIMC

This chapter includes the following sections:

CIMC Overview

The Cisco Integrated Management Controller (CIMC) is the management service for the E-Series Servers. CIMC runs within the server. You can use a web-based GUI or the SSH-based CLI to access, configure, administer, and monitor the server.

You can use CIMC to perform the following server management tasks:

- Power on, power off, power cycle, reset, and shut down the server
- Configure the server boot order
- Manage RAID levels
- View server properties and sensors
- Manage remote presence
- Create and manage local user accounts, and enable remote user authentication through the Active Directory
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security
- Configure communication services, including HTTP, SSH, IPMI over LAN, and SNMP
- Manage certificates
- Configure platform event filters

- Update CIMC firmware
- Update BIOS firmware
- Install the host image from an internal repository
- Monitor faults, alarms, and server status
- Collect technical support data in the event of server failure

Almost all tasks can be performed in either the GUI interface or CLI interface, and the results of tasks performed in one interface are displayed in another. However, you *cannot*:

- Use the CIMC GUI to invoke the CIMC CLI
- View a command that has been invoked through the CIMC CLI in the CIMC GUI
- Generate CIMC CLI output from the CIMC GUI

CIMC GUI

The CIMC GUI is a web-based management interface for E-Series Servers. You can launch the CIMC GUI and manage the server from any remote host that meets the following minimum requirements:

- Java 1.6 or later
- HTTP and HTTPS enabled
- Adobe Flash Player 10 or later

CIMC CLI

The CIMC CLI is a command-line management interface for E-Series Servers. You can launch the CIMC CLI in the following ways:

- By the serial port.
- Over the network by SSH.
- From the router by using the **hw-module subslot** *slot/port* **session imc** command.

A CLI user can have one of the three roles: admin, user (can control but cannot configure), and read-only.

Logging In to the CIMC GUI

Before You Begin

- Make sure that you have configured the IP address to access CIMC.
- If not installed, install Adobe Flash Player 10 or later on your local machine.

Procedure

Step 1 In your web browser, enter the IP address that you configured to access CIMC during initial setup.

Step 2 If a security dialog box displays, do the following:

a) (Optional) Check the check box to accept all content from Cisco.

b) Click **Yes** to accept the certificate and continue.

Step 3 In the log in window, enter your username and password.

Tip When logging in for the first time to an unconfigured system, use **admin** as the username and **password** as the password.

Step 4 Click **Log In**.

The **Change Password** dialog box appears.

Note The **Change Password** dialog box only appears the first time you log into CIMC. It does not appear for subsequent reboots.

Step 5 In the **New Password** field, enter your new password.

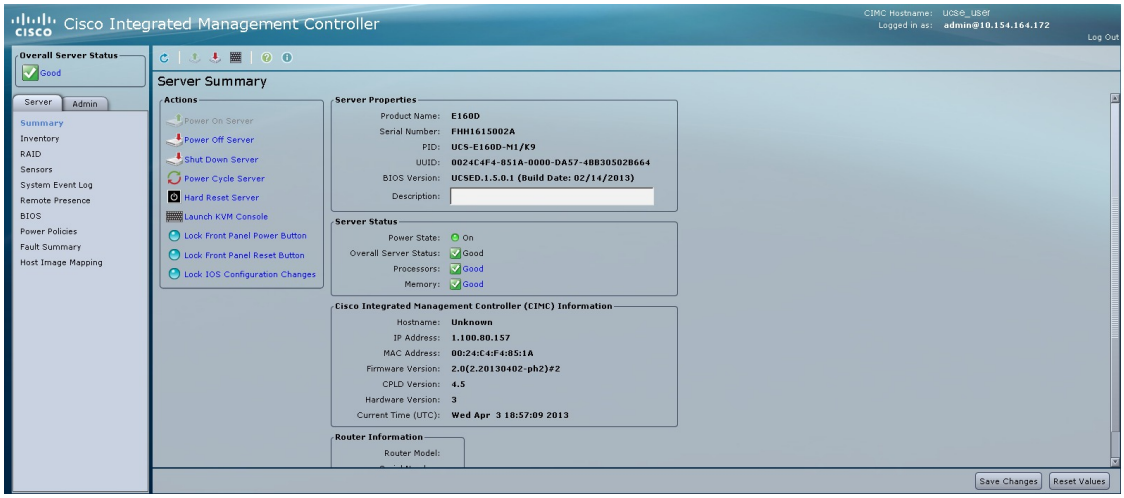
Step 6 In the **Confirm Password** field, enter the password again to confirm it.

Step 7 Click **Save Changes**.

The **Server Summary** page appears, which is the CIMC home page. See CIMC Home Page, on page 57.

CIMC Home Page

Figure 19: CIMC Home Page



Accessing the Microsoft Windows Server from CIMC

Before You Begin

- CIMC IP address is configured for CIMC access.
- Microsoft Windows Server is installed on the E-Series Server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 From the **Actions** area of the **Server Summary** page, click the **Launch KVM Console** icon.
The **KVM Console** opens in a separate window.

Step 4 From the KVM console, access the installed Microsoft Windows Server operating system.

Accessing the VMware vSphere Hypervisor from CIMC

Before You Begin

- CIMC IP address is configured for CIMC access.
- VMware vSphere Hypervisor is installed on the E-Series Server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 From the **Actions** area of the **Server Summary** page, click the **Launch KVM Console** icon.
The **KVM Console** opens in a separate window.

Step 4 From the KVM console, click the **KVM** tab.
The VMware vSphere Hypervisor™ Direct Console User Interface (DCUI) appears. If VMware vSphere Hypervisor™ has assigned an IP address to the host, then that IP address is displayed on the DCUI page, or you can specify a static IP address. See Assigning a Static IP Address to the VMware vSphere Hypervisor, on page 79.

Step 5 Make sure that you have installed vSphere Client. If not, install it. See Downloading and Installing the vSphere Client, on page 81.

Step 6 From the vSphere Client, log into the VMware vSphere Hypervisor™.
To log in, use either the IP address that is assigned by VMware vSphere Hypervisor™ or the static IP address that you specified in Step 4.

Note The default username for the preinstalled VMware vSphere Hypervisor™ is **root**, which cannot be changed and the default password is **password**. After you login, we recommend that you change the password.

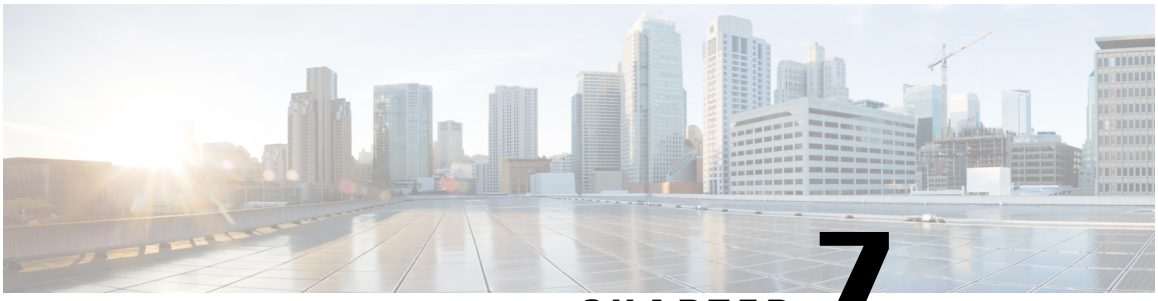
What to Do Next

Do one of the following as appropriate:

- If you purchased E-Series Server Option 2 (E-Series Server with preinstalled Microsoft Windows Server) or Option 3 (E-Series Server with preinstalled VMware vSphere Hypervisor™), use the CIMC GUI or CIMC CLI to manage and monitor the server.

  See the *GUI Configuration Guide for Cisco UCS E-Series Server Integrated Management Controller* or the *CLI Configuration Guide for Cisco UCS E-Series Server Integrated Management Controller*.

- If you purchased E-Series Server Option 1 (E-Series Server without preinstalled operating system or hypervisor), configure RAID. See Managing RAID, on page 61.



CHAPTER 7

Managing RAID

Note If you purchased E-Series Server Option 1 (E-Series Server without preinstalled operating system or hypervisor), and you want to store data files on local Redundant Array of Inexpensive Disks (RAID), you must configure RAID.

This chapter includes the following sections:

RAID Options

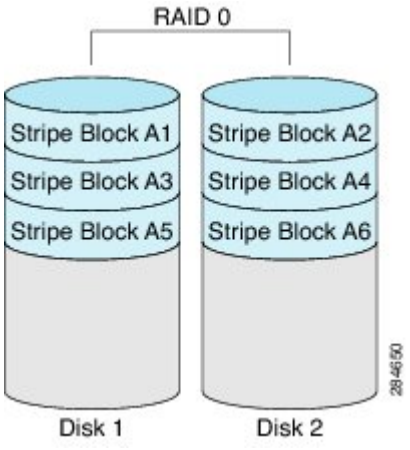
You can choose to store the E-Series Server data files on local Redundant Array of Inexpensive Disks (RAID). The following RAID levels are supported:

- The single-wide E-Series Server supports RAID 0 and RAID 1 levels.
- The double-wide E-Series Server supports RAID 0, RAID 1, and RAID 5 levels.
- The double-wide E-Series Server with the PCIe option supports RAID 0 and RAID 1 levels.

RAID 0

With RAID 0, the data is stored evenly in stripe blocks across one or more disk drives without redundancy (mirroring). The data in all of the disk drives is different.

Figure 20: RAID 0



Compared to RAID 1, RAID 0 provides additional storage because both disk drives are used to store data. The performance is improved because the read and write operation occurs in parallel within the two disk drives.

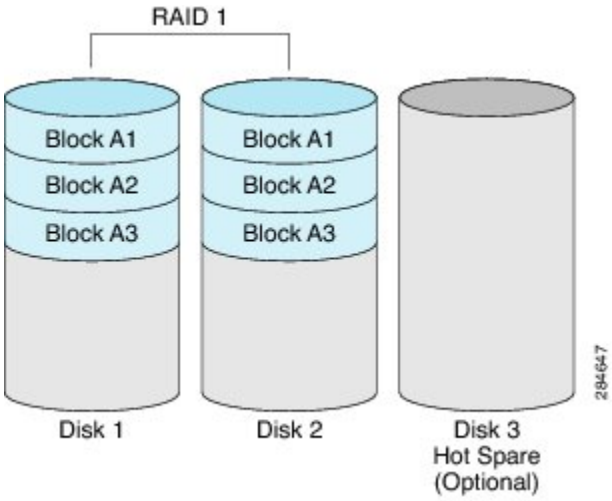
However, there is no fault tolerance, error checking, hot spare, or hot-swapping. If one disk drive fails, the data in the entire array is destroyed. Because there is no error checking or hot-swapping, the array is susceptible to unrecoverable errors.

RAID 1

RAID 1 creates a mirrored set of disk drives, where the data in both the disk drives is identical, providing redundancy and high availability. If one disk drive fails, the other disk drive takes over, preserving the data.

RAID 1 also allows you to use a hot spare disk drive. The hot spare drive is always active and is held in readiness as a hot standby drive during a failover.

Figure 21: RAID 1



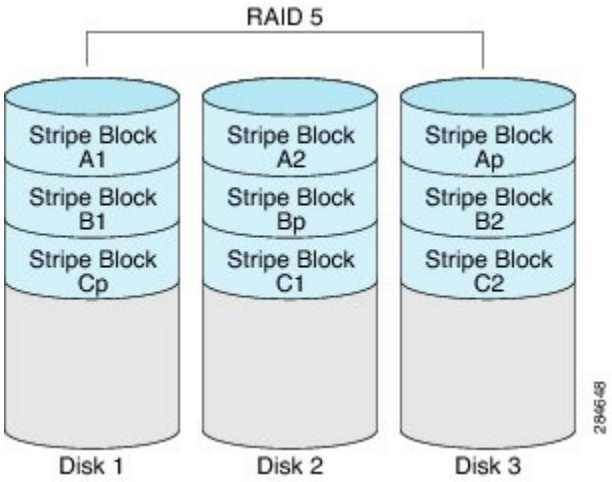
RAID 1 supports fault tolerance and hot-swapping. When one disk drive fails, you can remove the faulty disk drive and replace it with a new disk drive.

However, compared to RAID 0, there is less storage space because only half of the total potential disk space is available for storage and there is an impact on performance.

RAID 5

With RAID 5, the data is stored in stripe blocks with parity data staggered across all disk drives, providing redundancy at a low cost.

Figure 22: RAID 5



RAID 5 provides more data storage capacity than RAID 1 and better data protection than RAID 0. It also supports hot swapping; however, RAID 1 offers better performance.

Non-RAID

When the disk drives of a computer are not configured as RAID, the computer is in non-RAID mode. Non-RAID mode is also referred to as Just a Bunch of Disks or Just a Bunch of Drives (JBOD). Non-RAID mode does not support fault tolerance, error checking, hot-swapping, hot spare, or redundancy.

Summary of RAID Options

RAID Option	Description	Advantages	Disadvantages
RAID 0	Data stored evenly in stripe blocks without redundancy	• Better storage • Improved performance	• No error checking • No fault tolerance • No hot-swapping • No redundancy • No hot spare
RAID 1	Mirrored set of disk drives and an optional hot spare disk drive	• High availability • Fault tolerance • Hot spare • Hot-swapping	• Less storage • Performance impact
RAID 5	Data stored in stripe blocks with parity data staggered across all disk drives	• Better storage efficiency than RAID 1 • Better fault tolerance than RAID 0 • Low cost of redundancy • Hot-swapping	• Slow performance
Non-RAID	Disk drives not configured for RAID Also referred to as JBOD	• Portable	• No error checking • No fault tolerance • No hot-swapping • No redundancy • No hot spare

Configuring RAID

You can use the CIMC GUI or the WebBIOS, which is accessible from the KVM console, to configure RAID.

Configuring RAID Using the CIMC GUI

Use this procedure to configure the RAID level, strip size, host access privileges, drive caching, and initialization parameters on a virtual drive. You can also use this procedure to designate the drive as a hot spare drive and to make the drive bootable.

Procedure

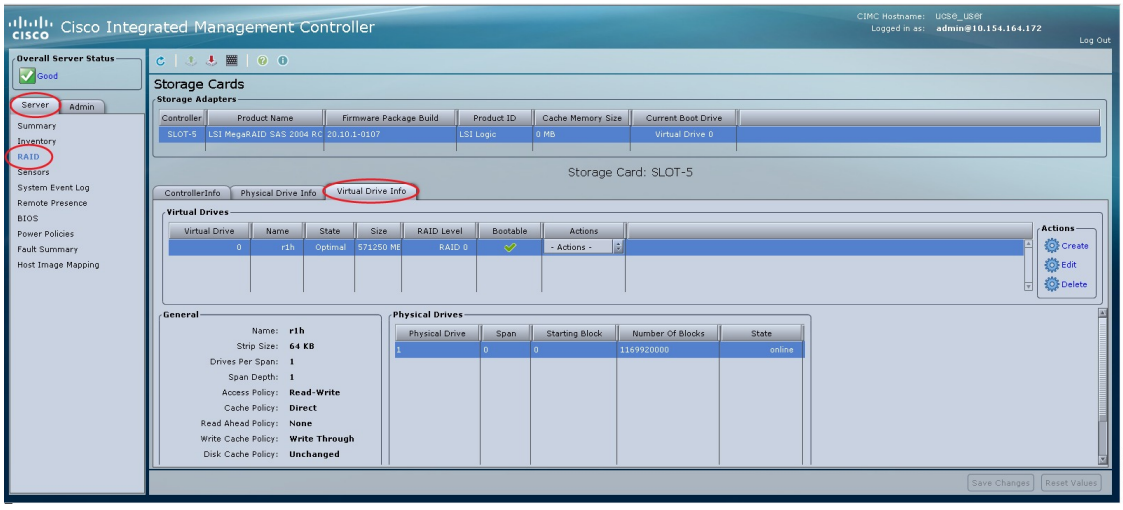
Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **RAID**. Do one of the following:

- If the **Configure Virtual Drive** dialog box does not appear, proceed to the next step.
- If the **Configure Virtual Drive** dialog box appears, and the virtual drives are not configured, complete the fields as shown in Step 5.

Step 3 In the tabbed menu of the **Storage Cards** area, click the **Virtual Drive Info** tab.

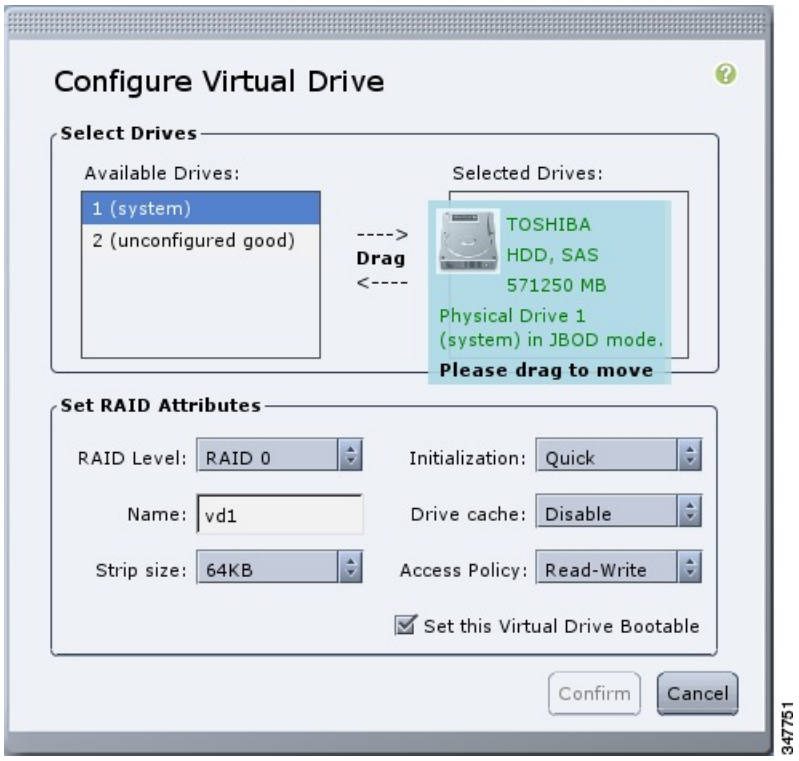
Figure 23: Virtual Drive Info Tab



Step 4 In the **Actions** area of the **Virtual Drive Info** tab, click **Create**.

The **Configure Virtual Drive** dialog box appears.

Figure 24: Configure Virtual Drive Dialog Box



Step 5 Complete the following fields as appropriate:

Name	Description
Available Drives table	Displays the drives that are available for RAID configuration. **Note** To move a drive, click and drag a drive to the appropriate table.
Selected Drives table	Displays the drives that are selected for RAID configuration. **Note** To move a drive, click and drag a drive to the appropriate table.
RAID Level drop-down list	The RAID level options. This can be one of the following: • **RAID 0—**Block striping. • **RAID 1—**Mirroring. • **RAID 5—**Block striping with parity. **Note** The single-wide E-Series Server supports RAID 0 and RAID 1 levels. The double-wide E-Series Server supports RAID 0, RAID 1, and RAID 5 levels. The double-wide E-Series Server with the PCIe option supports RAID 0 and RAID 1 levels.

Name	Description
Name field	The name of the virtual drive. Enter a maximum of 15 characters. The characters can have numbers and upper- or lower-case letters. Special characters are not supported.
Strip Size drop-down list	The strip size options. This can be one of the following: • **64 KB** • **32 KB** • **16 KB** • **8 KB**
Initialization drop-down list	How the controller initializes the drives. This can be one of the following: • **Quick—**The controller initializes the drive quickly. This is the default and recommended option. • **Full—**The controller does a complete initialization of the new configuration. **Note** Depending on the size of the drives, full initialization can take several hours to complete. To view the progress, see the **Initialize Progress** and **Initialize Time Elapsed** fields in the **General** area. • **None—**The controller does not initialize the drives.
Drive Cache drop-down list	How the controller handles drive caching. This can be one of the following: • **Disable—**Caching is disabled on the drives. **Note** This is the default and recommended option. • **Unchanged—**The controller uses the caching policy specified on the drive. This is the default and recommended option. • **Enable—**Caching is enabled on the drives. This option minimizes the delay in accessing data. **Caution** Enabling Drive Cache, voids all warranty on the hard disk drives. This configuration option is not supported. Use this option at your own risk.

Name	Description
Access Policy drop-down list	Configures host access privileges. This can be one of the following: • **Read-Write—**The host has full access to the drive. • **Read Only—**The host can read only data from the drive. • **Blocked—**The host cannot access the drive.
Set this Virtual Drive Bootable check box	How the controller boots the drive. This can be one of the following: • **Enable—**The controller makes this drive bootable. • **Disable—**This drive is not bootable. **Note** If you plan to install an operating system or Hypervisor into the RAID array, we recommend that you check this check box.
Use the Remaining Drive as Hot Spare check box	Designates the drive that is in the Available Drives table as a hot spare drive. **Note** Applicable for RAID 1 only. This check box is greyed out for other RAID levels. Applicable for double-wide E-Series Servers.

Step 6 Review the RAID configuration, and then click **Confirm** to accept the changes.

Configuring RAID Using the WebBIOS

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

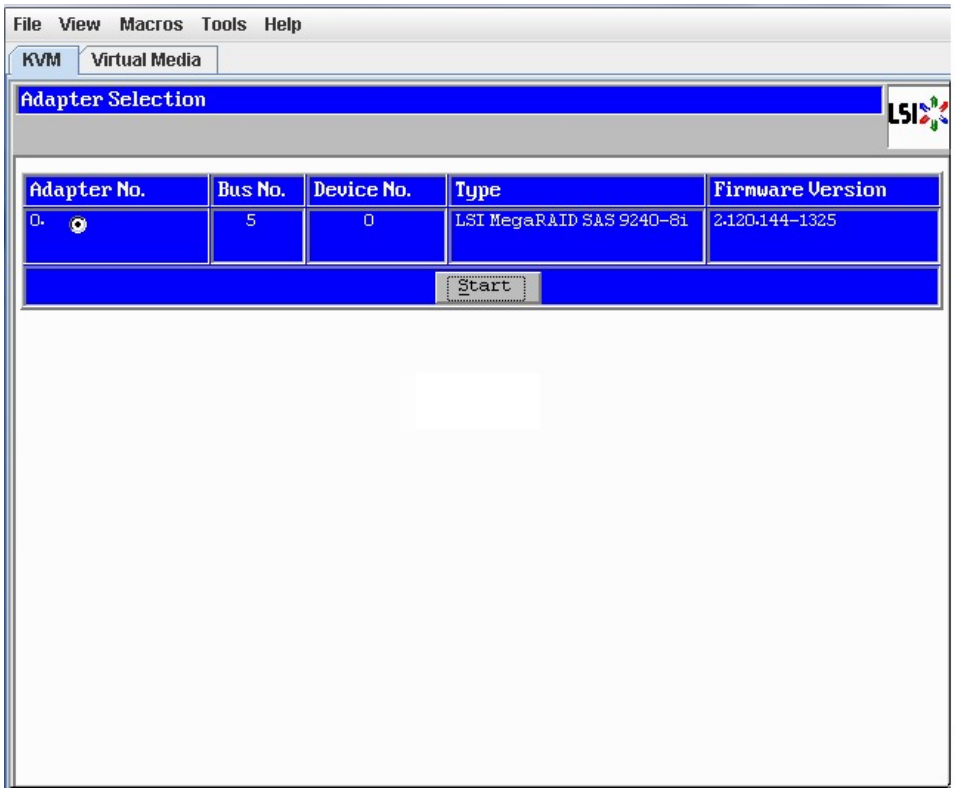
Step 3 From the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.

Step 4 From the **Server Summary** page, click **Power Cycle Server** to reboot the server.

Step 5 Press the **Ctrl** key, and then press **H** during bootup to access the WebBIOS.

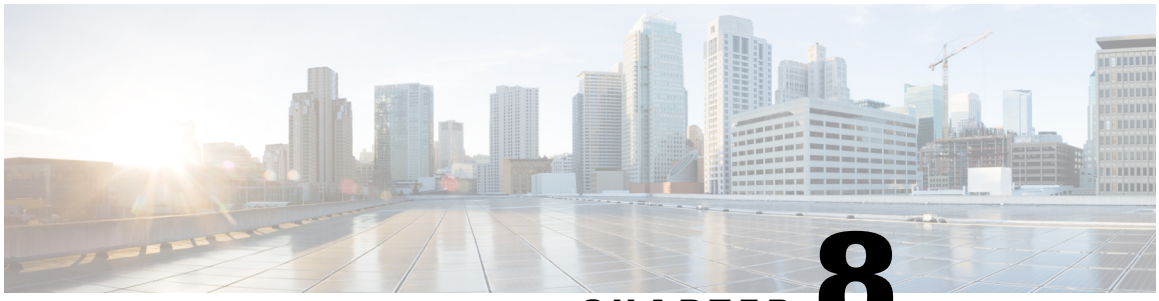
The **Adapter Selection** page from LSI Logic appears, which allows you to configure RAID. For information about this page, see the LSI Logic documentation.

Figure 25: WebBIOS



What to Do Next

If you purchased E-Series Server Option 1 (E-Series Server without preinstalled operating system or hypervisor), install the operating system. See Installing the Operating System or Hypervisor, on page 71.



CHAPTER 8

Installing the Operating System or Hypervisor

Note If you purchased E-Series Server Option 1 (E-Series Server without preinstalled operating system or hypervisor), you must install an operating system or hypervisor.

This chapter includes the following sections:

Operating System or Hypervisor Installation Methods

E-Series Servers support several operating systems and hypervisors. Regardless of the platform being installed, you can install it on your server using one of the following methods:

- KVM console
- PXE installation server
- Host image mapping

Caution You must use only one method to map virtual drives. For example, you must use either the KVM console or the Host Image Mapping method. Using a combination of methods will cause the server to be in an undefined state.

KVM Console

The KVM console is an interface accessible from the CIMC that emulates a direct keyboard, video, and mouse connection to the server. The KVM console allows you to connect to the server from a remote location. Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer

You can use the KVM console to install an operating system or hypervisor on the server and to do the following:

- Access the BIOS setup menu by pressing **F2** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.
- Access the WebBIOS to configure RAID, by pressing the **Ctrl** and **H** keys during bootup.

Installing an Operating System or Hypervisor Using the KVM Console

Before You Begin

Locate the operating system or hypervisor installation disk or disk image file.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 79.

Procedure

Step 1 Load the operating system or hypervisor installation disk into your CD/DVD drive, or copy the disk image files to your computer.

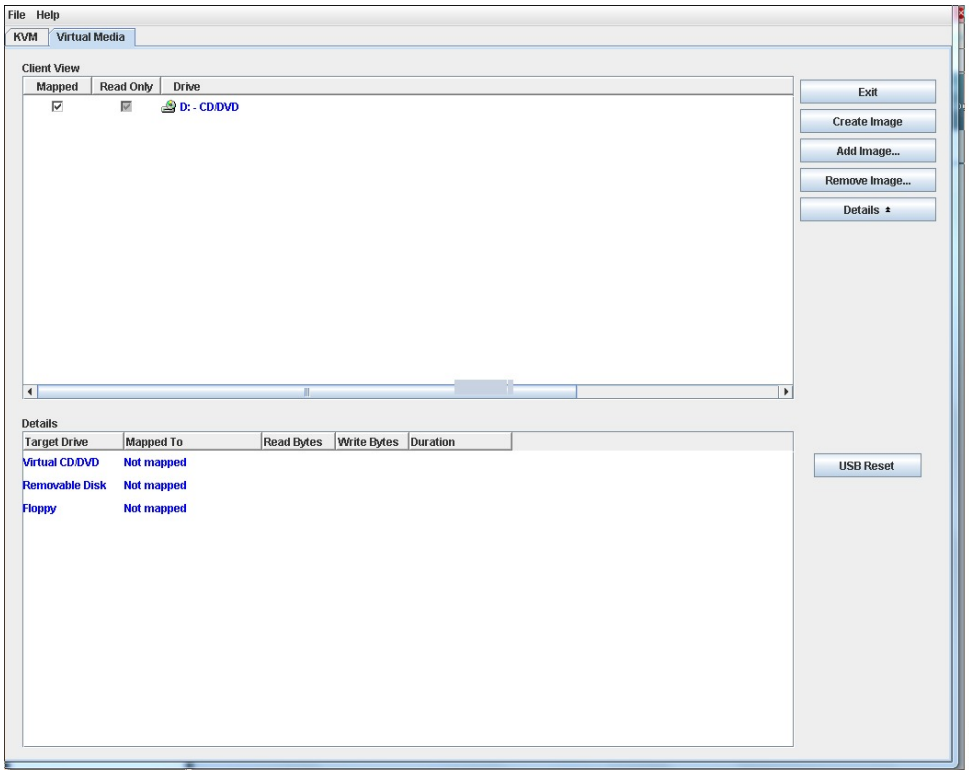
Step 2 If CIMC is not open, log into the CIMC GUI.

Step 3 In the **Navigation** pane, click the **Server** tab.

Step 4 On the **Server** tab, click **Summary**.

Step 5 From the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.

Step 6 From the KVM console, click the **Virtual Media** tab.



Step 7 In the **Virtual Media** tab, map the virtual media using either of the following methods:

- Check the **Mapped** check box for the CD/DVD drive containing the operating system or hypervisor installation disk.
- Click **Add Image**, navigate to and select the operating system or hypervisor installation disk image, click **Open** to mount the disk image, and then check the **Mapped** check box for the mounted disk image.

Note You must keep the **Virtual Media** tab open during the installation process. Closing the tab unmaps all virtual media.

Step 8 Set the boot order to make the virtual CD/DVD drive as the boot device.
To set the boot order, see Configuring the Server Boot Order, on page 81.

Step 9 Reboot the server.
When the server reboots, it begins the installation process from the virtual CD/DVD drive. Refer to the installation guide for the platform being installed to guide you through the rest of the installation process.

Step 10 If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. See the appropriate operating system or hypervisor documentation for instructions on how to install drivers. For instructions on how to install drivers on a Microsoft Windows operating system, see Installing Drivers for the Microsoft Windows Server, on page 77.

What to Do Next

After the installation is complete, reset the virtual media boot order to its original setting.

PXE Installation Servers

A Preboot Execution Environment (PXE) installation server allows a client to boot and install an operating system or hypervisor from a remote location. To use this method, a PXE environment must be configured and available on your VLAN, typically a dedicated provisioning VLAN. In addition, the server must be set to boot from the network. When the server boots, it sends a PXE request across the network. The PXE installation server acknowledges the request, and starts a sequence of events that installs the operating system or hypervisor on the server.

PXE servers can use installation disks, disk images, or scripts to install the operating system or hypervisor. Proprietary disk images can also be used to install the platform, additional components, or applications.

Note PXE installation is an efficient method for installing a platform on a large number of servers. However, considering that this method requires setting up a PXE environment, it might be easier to use another installation method.

Installing an Operating System or Hypervisor Using a PXE Installation Server

Before You Begin

Verify that the server can be reached over a VLAN.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 79.

Procedure

Step 1 Set the boot order to **PXE**.

Step 2 Reboot the server.
If a PXE install server is available on the VLAN, the installation process begins when the server reboots. PXE installations are typically automated and require no additional user input. Refer to the installation guide for the operating system or hypervisor being installed to guide you through the rest of the installation process.

What to Do Next

After the installation is complete, reset the LAN boot order to its original setting.

Host Image Mapping

The Host Image Mapping feature allows you to download, map, unmap, or delete a host image. Download a host image, such as Microsoft Windows, Linux, or VMware from a remote FTP or HTTP server onto the

CIMC internal repository, and then map the image onto the virtual drive of a USB controller in the E-Series Server. After you map the image, set the boot order to make the virtual drive, in which the image is mounted, as the first boot device, and then reboot the server. The host image must have .iso or .img as the file extension.

The Host Image Mapping feature also allows you to download and mount a diagnostics image. The diagnostics image must have .diag as the file extension.

Mapping the Host Image

Before You Begin

- Log into CIMC as a user with admin privileges.
- Obtain the host image file from the appropriate third-party.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 79.

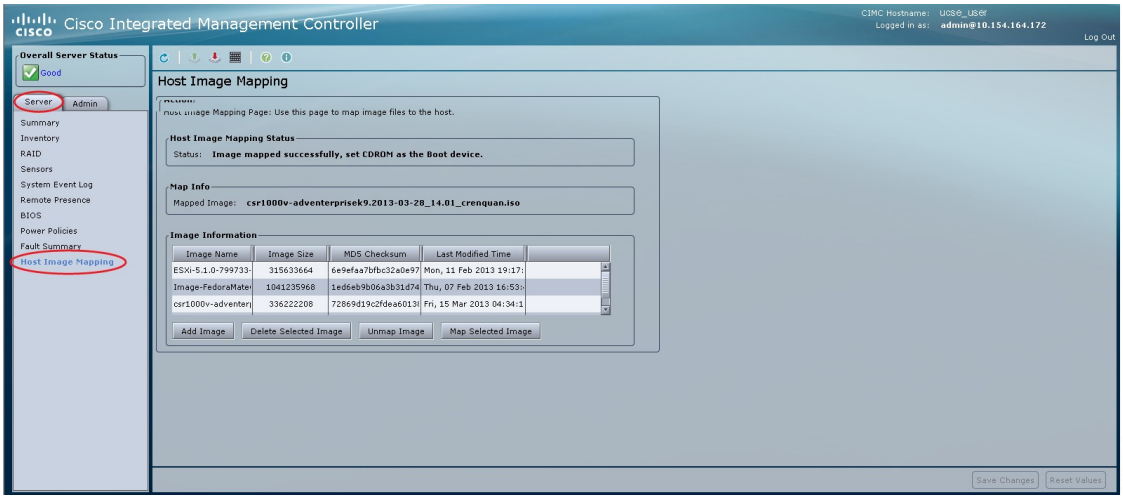
Note If you start an image update while an update is already in process, both updates will fail.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Host Image Mapping**.

Figure 26: Host Image Mapping



Step 3 From the **Host Image Mapping** page, click **Add Image**.

The **Download Image** dialog box opens. Complete the following fields:

Name	Description
Download Image From drop-down list	The type of remote server on which the image is located. This can be one of the following: • **FTP** • **HTTP** **Note** Depending on the remote server that you select, the fields that display change.
FTP or **HTTP Server IP Address** field	The IP address of the remote FTP or HTTP server.
FTP or **HTTP File Path** field	The path and filename of the remote FTP or HTTP server. The path and filename can contain up to 80 characters. • If you are installing a host image, that image must have .iso or .img as the file extension. • If you are installing a diagnostics image, that image must have .diag as the file extension.
Username field	The username of the remote server. The username can contain 1 to 20 characters. **Note** If the username is not configured, enter **anonymous** for the username and any character(s) for the password.
Password field	The password for the username. The password can contain 1 to 20 characters. **Note** If the username is not configured, enter **anonymous** for the username and any character(s) for the password.

Step 4 Click **Download**.
The **Host Image Mapping** page opens. You can view the status of the image download in the **Host Image Mapping Status** area. After the image is downloaded and processed successfully, refresh the page. After the page refreshes, the new image displays in the **Image Information** area.

Step 5 From the **Image Information** area, select the image to map, and then click **Map Selected Image**.
The image is mapped and mounted on the virtual drive of a USB controller. The virtual drive can be one of the following:

- HDD—Hard disk drive
- FDD—Floppy disk drive
- CD/DVD—Bootable CD-ROM or DVD drive

Step 6 Set the boot order to make the virtual drive in which the image is mounted as the first boot device.

To set the boot order, see Configuring the Server Boot Order, on page 81.

Tip To determine in which virtual drive the image is mounted, see the **Host Image Update Status** area in the **Host Image Mapping** page.

Step 7 Reboot the server.

Step 8 If the image contains an answer file, the operating system or hypervisor installation is automated and the image is installed. Otherwise, the installation wizard is displayed. Follow the wizard steps to install the image.

Step 9 If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. See the appropriate operating system or hypervisor documentation for instructions on how to install drivers. For instructions on how to install drivers on a Microsoft Windows operating system, see Installing Drivers for the Microsoft Windows Server, on page 77.

What to Do Next

- After the installation is complete, reset the virtual media boot order to its original setting.
- Unmap the host image. See Unmapping the Host Image, on page 78.

Installing Drivers for the Microsoft Windows Server

Note If you purchased E-Series Server Option 1 (E-Series Server without a preinstalled operating system or hypervisor), and you installed your own version of the Microsoft Windows Server, you must install drivers.

The Microsoft Windows operating system requires that you install three drivers:

- On-Board Network Drivers for Windows 2008 R2
- LSI Drivers (On-Board Hardware RAID Controller) for Windows 2008 R2
- Intel Drivers for Windows 2008 R2

Note Additional drivers are not needed for Windows 2012.

If you have purchased a 10-Gigabit add-on card, you must also install the 10G PCIe Network Drivers for Windows 2008 R2.

Procedure

Step 1 Download the drivers from Cisco.com. See Obtaining Software from Cisco Systems, on page 102.

Step 2 Copy the driver files into a USB flash drive.

Step 3 Install your own version of Microsoft Windows Server.
During the installation process, you will be prompted for the LSI Drivers.

Step 4 Plug the USB flash drive into the USB slot in the E-Series Server, and then install the LSI Drivers.

Step 5 After the Microsoft Windows Server installation is complete, install the On-Board Network Drivers (Broadcom) and the Intel Drivers.

Unmapping the Host Image

Before You Begin

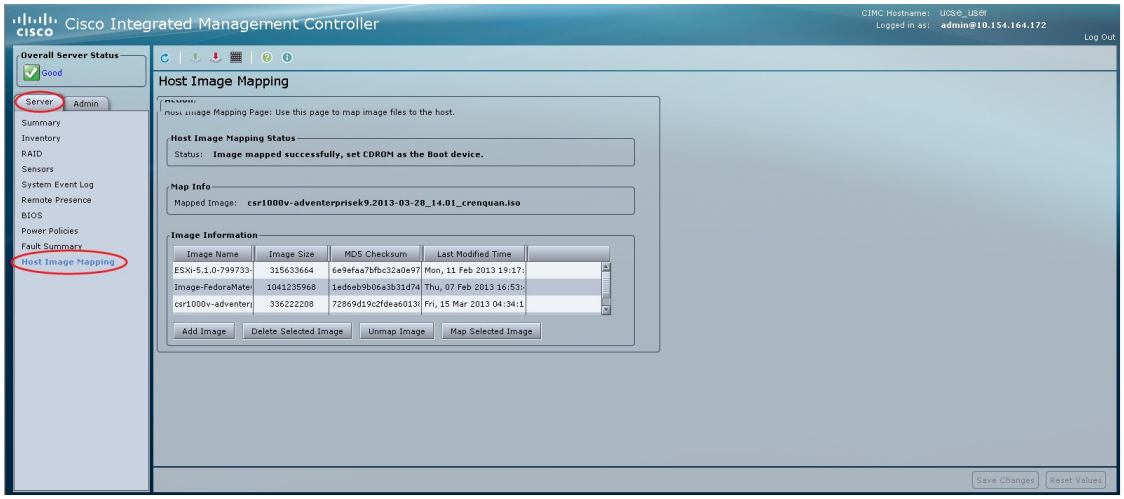
Log in to CIMC as a user with admin privileges.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Host Image Mapping**.

Figure 27: Host Image Mapping



Step 3 Click **Unmap Image**.
The mapped image is unmounted from the virtual drive of the USB controller.

Basic Workflow for Downloading and Installing the VMware vSphere Hypervisor

Caution If you are using VMware FL-SRE-V-HOST license (equivalent to VMware vSphere Hypervisor™ 5.X), make sure that the RAM that you are using is 32GB or less. If the RAM is more than 32GB, you will get an error message, and you will not be able to apply the license. If you want to use 48GB RAM, upgrade your license to FL-SRE-V-HOSTVC.

- Download the customized VMware vSphere Hypervisor™ image.
- Install the VMware vSphere Hypervisor image.
- Assign a static IP address to the VMware vSphere Hypervisor™.
- Download and install the vSphere Client.

Downloading the Customized VMware vSphere Hypervisor Image

Procedure

Step 1 Navigate to https://my.vmware.com/web/vmware/login.
The VMware login page appears.

Step 2 Enter your VMware credentials, and then click **Log In**.
If you do not have an account with VMware, click **Register** to create a free account.

Step 3 Under the **Support Requests** pane, click **Knowledge Base**.

Step 4 In the **Search** field located on the top right corner, enter **ESXi-5.0.0-623860-custom-Cisco-2.0.1.6.iso**, and then click **Search**.

Step 5 From the **Search Results**, click **Download VMware View 5.1** to download the customized VMware vSpere Hypervisor™ image.

What to Do Next

Install the VMware vSpere Hypervisor™ image. For installation instructions, see Mapping the Host Image.

Assigning a Static IP Address to the VMware vSphere Hypervisor

Use this procedure to assign a static IP address to the VMware vSphere Hypervisor™.

Before You Begin

- Download the customized VMware vSphere Hypervisor™ image. See Downloading the Customized VMware vSphere Hypervisor Image, on page 79.

Note You must have an account with VMware to download the customized image.

- Install the image onto the E-Series Server. For installation instructions, see Mapping the Host Image.

Procedure

Step 1 In your web browser, enter the IP address that you configured to access CIMC during initial setup and then log into CIMC.
The CIMC Home page, which is the **Server Summary** page, appears.

Step 2 From the **Actions** area of the **Server Summary** page, click the **Launch KVM Console** icon.
The **KVM Console** opens in a separate window.

Step 3 From the KVM console, click the **KVM** tab, and then do the following to configure the IP address:

a) Press **F2** to access the VMware vSphere Hypervisor™ DCUI customization menu.
The **DCUI** login page appears.

b) Log into the **DCUI**.
The **System Customization** page appears.

c) From the **System Customization** page, click **Configure Management Network**.
The **Configure Management Network** page appears, which has several menu options, including **Network Adapter**. The **Network Adapter** menu option allows you to view the existing network adapters and activate them.

Note By default, the network adapter, **vmnic0**, is activated. Make sure that it stays activated.

d) From the **Configure Management Network** page, click the **IP Configuration** menu option.
To assign a static IP address, do the following:

- In the **IP Configuration** dialog box, click the radio box to specify that a static IP address will be used.
- In the appropriate fields, enter the IP address, network mask, and the gateway IP address, and then press **Enter**. The **Configure Management Network** page appears.
- In the **Configure Management Network** page, click the **ESC** key. The **Configure Management Network Confirm** dialog box appears.
- Enter **y** to accept the changes and restart the management network.

e) In the router configuration, add a route to the VMware vSphere Hypervisor™ host IP address.
For example, if the host IP address is 192.168.1.25 and the ucse interface is ucse 2/0, add the following route:

```
ip route 192.168.1.25 255.255.255.255 ucse2/0
```

f) Install the vSphere Client. See Downloading and Installing the vSphere Client, on page 81. From the vSphere Client, use the host IP address to log into the VMware vSphere Hypervisor™.

Downloading and Installing the vSphere Client

Use this procedure to download and install the vSphere Client.

Before You Begin

- Make sure that you have assigned a static IP address to VMware vSphere Hypervisor™. See Assigning a Static IP Address to the VMware vSphere Hypervisor, on page 79.
- Verify that you have network connectivity. To download the vSphere Client, connection to the Internet is required.

Note The vSphere Client contains an online tutorial for first time users. It also contains embedded in-line getting started assistance, which allows you to set up your virtual infrastructure through an easy to use, step-by-step process. If you are an experienced user, you can choose to turn-off the getting started in-line assistance.

Procedure

Step 1 Go to https://*hypervisor-ip-address*. You are directed to the VMware website and the Welcome page opens.

Step 2 Click **Download vSphere Client**, and then click **Run** to download the vSphere Client. The VMware vSphere Client is installed and a shortcut icon to the client appears on your desktop.

Step 3 Click the **VMware vSphere Client** icon to open the login window.

Step 4 To manage the VMware vSphere Hypervisor™, enter the IP address or hostname of the VMware vSphere Hypervisor ™ and the username and password, and then click **Login**. The vSphere Client GUI opens.

Note The default username for the preinstalled VMware vSphere Hypervisor™ is **root**, which cannot be changed; and the default password is **password**. After you login, we recommend that you change the password.

Configuring the Server Boot Order

You can use the CIMC GUI or the BIOS setup menu to configure the server boot order.

Configuring the Server Boot Order Using the CIMC GUI

Before You Begin

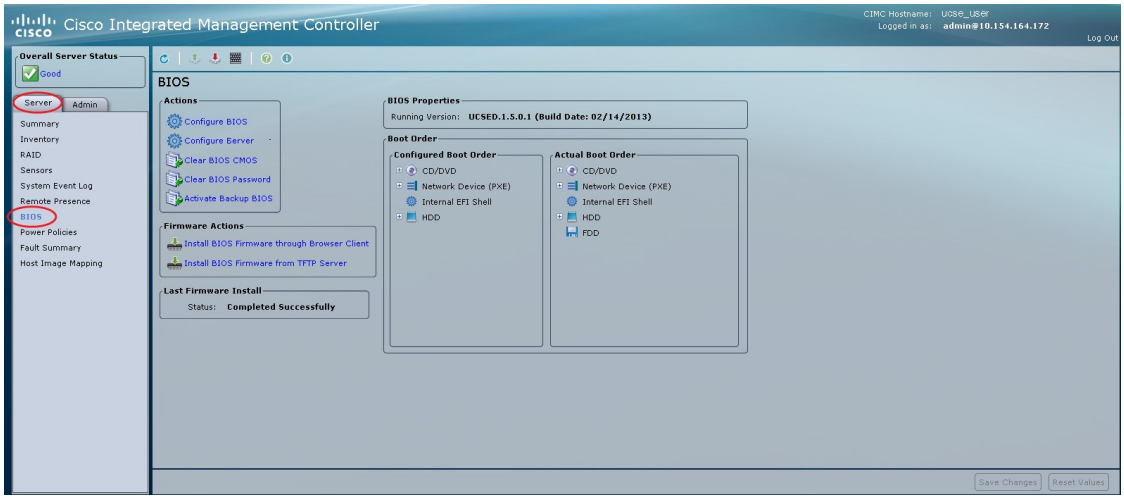
Log into CIMC as a user with admin privileges.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Figure 28: BIOS



Step 3 In the **Actions** area, click **Configure Boot Order**.

The **Configure Boot Order** dialog box appears.

Figure 29: Configure Boot Order Dialog Box

Step 4 In the **Configure Boot Order** dialog box, complete the following fields as appropriate:

Name	Description
Device Types table	The server boot options. This can be the following: • **HDD—**Hard disk drive. Contains the following options: ◦ **Cypress** ◦ **PCI RAID Adapter** ◦ **Linux Virtual FDD/HDD** • **FDD—**Floppy disk drive. Contains the following option: ◦ **Linux Virtual Floppy** • **CD/DVD—**Bootable CD-ROM. Contains the following option: ◦ **Linux Virtual CD/DVD** • **Network Devices (PXE)—**PXE boot. Contains the following options: ◦ **Console** or **GE0** • **Console—**Applicable for the Cisco 2900 and Cisco 3900 series ISR G2. • **GE0—**Applicable for the Cisco 4400 series ISR. ◦ **GE1** ◦ **GE2** ◦ **GE3—**Applicable for double-wide E-Series Servers. • **Internal EFI Shell—**Internal Extensible Firmware Interface.
Add >	Moves the selected device type to the **Boot Order** table.
< Remove	Removes the selected device type from the **Boot Order** table.
Boot Order table	Displays the device types from which this server can boot, in the order in which the boot will be attempted.
Up	Moves the selected device type to a higher priority in the **Boot Order** table.
Down	Moves the selected device type to a lower priority in the **Boot Order** table.

Step 5 Click **Apply**.

Additional device types may be appended to the actual boot order, depending on what devices you have connected to your server.

What to Do Next

- Reboot the server to boot with your new boot order.

Configuring the Boot Order Using the BIOS Setup Menu

Use this procedure if you want the server to boot from an external bootable device, such as an USB or an external CD ROM drive that is directly connected to the E-Series Server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

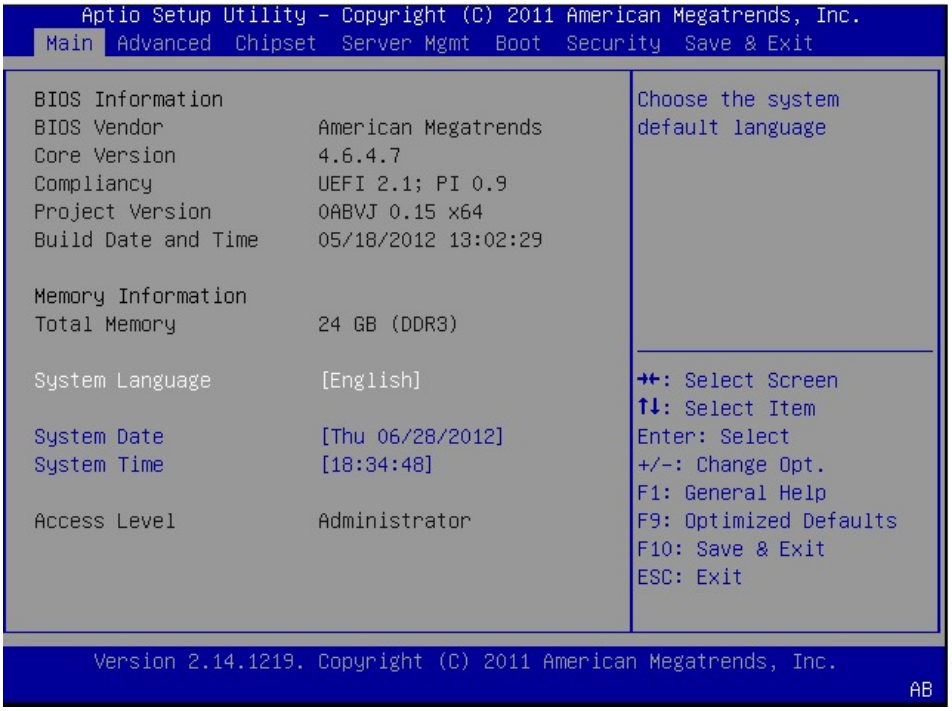
Step 3 From the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.

Step 4 From the **Server Summary** page, click **Power Cycle Server** to reboot the server.

Step 5 When prompted, press **F2** during bootup to access the BIOS setup menu.

The **Aptio Setup Utility** appears, which provides the BIOS setup menu options.

Figure 30: BIOS Setup Menu



Step 6 Click the **Boot** tab.

Step 7 Scroll down to the bottom of the page below the **Boot Options Priority** area. The following boot option priorities are listed:

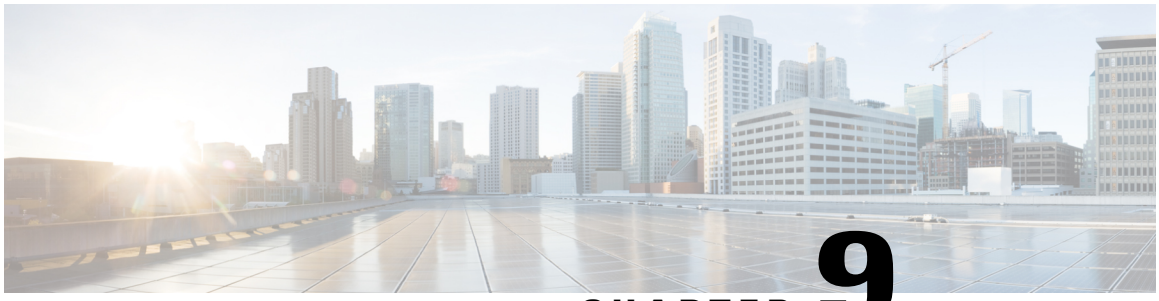
- Floppy Drive BBS Priorities
- Network Device BBS Priorities
- Hard Drive BBS Priorities
- CD/DVD ROM Drive BBS Priorities

Step 8 Use the **Up** or **Down arrow keys** on your keyboard to highlight the appropriate option.

Step 9 Press **Enter** to select the highlighted field.

Step 10 Choose the appropriate device as Boot Option 1.

Step 11 Press **F4** to save changes and exit.
The **Main** tab of the BIOS setup displays the device that you configured as Boot Option 1.



CHAPTER 9

Configuring a Connection Between the Router and the E-Series Server

This chapter provides procedures to configure an internal connection between the ISR G2 and the E-Series Server and between the Cisco ISR 4451-X and the E-Series Server. It contains the following sections:

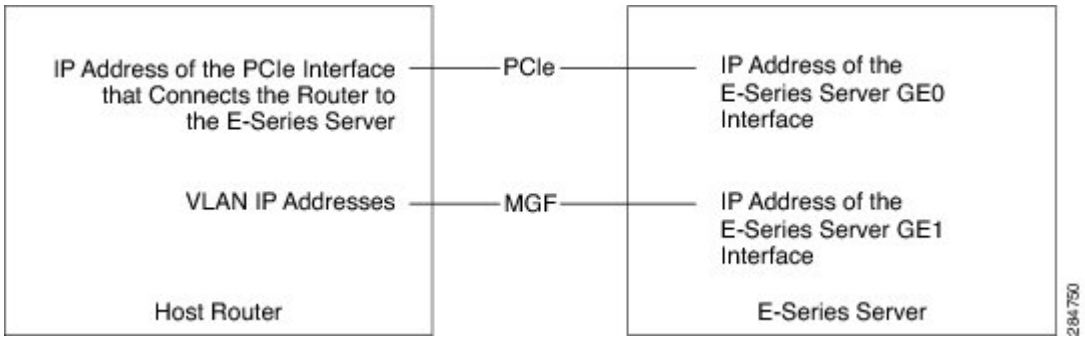
Configuring an Internal Connection Between the ISR G2 and the E-Series Server

Use this configuration if you want the traffic to your application or operating system to flow through the ISR G2. To configure an internal connection between the ISR G2 and the E-Series Server, you must configure these IP addresses:

- For traffic to flow through the PCIe connection (see next figure), configure the following:
  - IP address of the router's internal PCIe interface that connects the router to the E-Series Server's GE0 interface.
  - IP address of the E-Series Server's GE0 interface.
- For traffic to flow through the MGF connection (see next figure), configure the following:
  - IP address of the router's internal MGF VLAN interface.
  - IP address of the E-Series Server's GE1 interface.

The following figure shows the internal connection between the router and the E-Series Server.

Figure 31: Internal Connection Between the ISR G2 and the E-Series Server



Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface ucse** *slot*/**0**	Enters the ucse interface configuration mode for the router's PCIe *slot*/**0** interface.
Step 4	Enter one of the following commands: • Router (config-if)# **ip address** *router-to-e-series-server-interface-ip-address subnet mask* • Router (config-if)# **ip unnumbered** *type number*	The **ip address** command specifies the IP address of the router's internal PCIe interface that connects the router to the E-Series Server's GE0 interface. See figure above. or The **ip unnumbered** command enables IP processing on an interface without assigning an explicit IP address to that interface. • *type*—Type of interface on which the router has an assigned IP address. • *number*—Number of the interface on which the router has an assigned IP address. **Note** The unnumbered interface must be unique. It cannot be another unnumbered interface. **Caution** The **ip unnumbered** command creates a point-to-point interface between devices. Broadcasting is not supported.

	Command or Action	Purpose
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **end**	Exits configuration mode.
Step 7	Use the server's operating system to configure the E-Series Server's **GE0** interface. See figure above.	—
Step 8	Router (config)# **interface ucse** *slot*/**1**	Enters ucse interface configuration mode for the router's MGF *slot*/**1** VLAN interface. See figure above.
Step 9	Router (config-if)# **switchport mode trunk**	Puts the port into permanent trunking mode. The default configuration is access mode.
Step 10	Router (config-if)# **[switchport trunk allowed vlan** *vlan-numbers***]**	(Optional) Allows trunking on the specified VLANs. • *vlan-numbers*—VLAN numbers on which to allow trunking.
Step 11	Router (config-if)# **exit**	Exits interface configuration mode.
Step 12	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 13	Router (config)# **interface vlan** *vlan-number*	Enters VLAN configuration mode for the specified VLAN number.
Step 14	Router (config-if)# **ip address** *vlan-ip-address subnet-mask*	Specifies the IP address for the VLAN. See figure above. • *vlan-ip-address*—IP address of the VLAN. • *subnet-mask*—Subnet mask to append to the IP address.
Step 15	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 16	Router (config-if)# **end**	Exits configuration mode.
Step 17	Use the server's operating system to configure the E-Series Server's **GE1** interface. See figure above.	—
Step 18	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.

This example shows how to configure an internal connection between the router and the E-Series Server.

Note The IP addresses in this configuration example are for reference only and might not be valid.

```
Router> enable
Router# configure terminal

Router(config)# interface ucse 1/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# end

Use the server's operating system to configure the E-Series Server's GE0 interface

Router(config)# interface ucse 1/1
Router(config-if)# switchport mode trunk
Router(config-if)# exit

Router# configure terminal
Router(config)# interface vlan 1
Router(config-if)# ip address 20.0.0.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end

Use the server's operating system to configure the E-Series Server's GE1 interface.

Router# show running-config
```

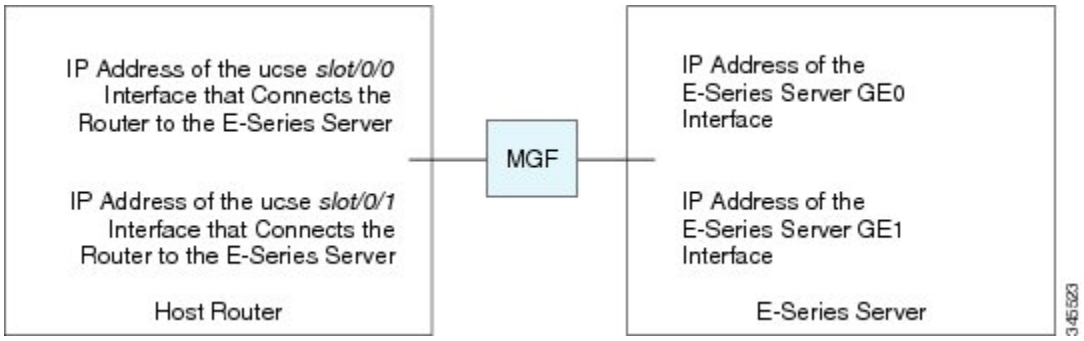
Configuring an Internal Connection Between the Cisco ISR 4451-X and the E-Series Server

Use this configuration if you want the traffic to your application or operating system to flow through the Cisco ISR 4451-X. To configure an internal connection between the Cisco ISR 4451-X and the E-Series Server, you must configure these IP addresses:

- For traffic to flow through the router's **ucse** *slot*/**0/0** and the E-Series Server's internal GE0 interface (see next figure), configure the following:
  - IP address of the router's **ucse** *slot*/**0/0** interface that connects the router to the E-Series Server's GE0 interface.
  - IP address of the E-Series Server's GE0 interface.
- For traffic to flow through the router's **ucse** *slot*/**0/1** and the E-Series Server's internal GE1 interface (see next figure), configure the following:
  - IP address of the router's **ucse** *slot*/**0/1** interface.
  - IP address of the E-Series Server's GE1 interface.

The following figure shows the internal connection between the router and the E-Series Server.

Figure 32: Internal Connection Between the Cisco ISR 4451-X and the E-Series Server



Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface ucse** *slot*/**0/0**	Enters interface configuration mode for the router's ucse *slot*/**0/0** interface.
Step 4	Enter one of the following commands: • Router (config-if)# **ip address** *router-to-e-series-server-interface-ip-address subnet-mask* • Router (config-if)# **ip unnumbered** *type number*	Specify the IP address of the router's **ucse** *slot* **0/0** interface that connects the router to the E-Series Server's GE0 interface. See figure above. or The **ip unnumbered** command enables IP processing on an interface without assigning an explicit IP address to that interface. • *type*—Type of interface on which the router has an assigned IP address. • *number*—Number of the interface on which the router has an assigned IP address. **Note** The unnumbered interface must be unique. It cannot be another unnumbered interface. **Caution** The **ip unnumbered** command creates a point-to-point interface between devices. Broadcasting is not supported.

	Command or Action	Purpose
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **end**	Exits configuration mode.
Step 7	Use the server's operating system to configure the E-Series Server's **GE0** interface. See figure above.	—
Step 8	Router (config)# **interface ucse** *slot*/**0/1**	Enters ucse interface configuration mode for the router's ucse *slot*/**0/1** interface. See figure above.
Step 9	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 10	Router (config-if)# **end**	Exits configuration mode.
Step 11	Use the server's operating system to configure the E-Series Server's **GE1** interface. See figure above.	—
Step 12	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.

This example shows how to configure an internal connection between the router and the E-Series Server.

Note The IP addresses in this configuration example are for reference only and might not be valid.

```
Router> enable
Router# configure terminal

Router(config)# interface ucse 1/0/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# end

Use the server's operating system to configure the E-Series Server's GE0 interface.

Router(config)# interface ucse 1/0/1
Router(config-if)# ip address 11.0.0.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end

Use the server's operating system to configure the E-Series Server's GE1 interface.

Router# show running-config
```

Creating an Ethernet Virtual Circuit Using the Native VLAN Between the E-Series Server and the Cisco ISR 4451-X

Use this procedure if you have added the native VLAN to encapsulate and transport selected data either to the operating system installed on the E-Series Server, or to the virtual machines created on the installed hypervisor.

Before You Begin

Configure an internal connection between the Cisco ISR 4451-X and the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface ucse** *slot*/**0/0**	Enters ucse interface configuration mode for the router's ucse *slot*/**0/0** interface.
Step 4	Router (config-if)# **service instance** *id* **ethernet**	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 5	Router (config-if-srv)# **encapsulation** *encapsulation-type vlan-id*	Defines the encapsulation type.
Step 6	Router (config-if-srv)# **bridge-domain** *bridge-id*	Configures the bridge domain.
Step 7	Router (config-if-srv)# **exit**	Exits Ethernet service configuration mode.
Step 8	Router (config-if)# **interface BDI** *bridge-id*	Enters the bridge domain interface.
Step 9	Router (config-if)# **ip address** *bdi-interface-ip-address*	Specifies the IP address of the BDI interface.
Step 10	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 11	Router (config-if)# **end**	Returns to global configuration mode on the host router.
Step 12	Use the server's operating system to configure the E-Series Server's **GE0** interface. See figure above.	—
Step 13	Router# **show running-config**	Displays the running configuration of the router so that you can verify the address configurations.

This example shows how to create an Ethernet Virtual Circuit using the native VLAN between the E-Series Server and the Cisco ISR 4451-X.

Note The IP addresses in this configuration example are for reference only.

```
Router> enable
Router# configure terminal

Router(config)# interface ucse 1/0/0
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation untagged
Router(config-if-srv)# bridge-domain 1
Router(config-if-srv)# exit

Router(config-if)# interface BDI 1
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shut
Router(config-if)# end

Use the server's operating system to configure the E-Series Server's GE0 interface.

Router# show running-config
```

Creating an Ethernet Virtual Circuit Using a Non-Native VLAN Between the E-Series Server and the Cisco ISR 4451-X

Use this procedure if you have added a non-native VLAN to encapsulate and transport selected data either to the operating system installed on the E-Series Server, or to the virtual machines created on the installed hypervisor.

Before You Begin

Configure an internal connection between the Cisco ISR 4451-X and the E-Series Server.

Procedure

	Command or Action	Purpose
Step 1	Router> **enable**	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 3	Router (config)# **interface ucse** *slot*/**0/0**	Enters ucse interface configuration mode for the router's ucse *slot*/**0/0** interface.
Step 4	Router (config-if)# **no ip address**	Removes an IP address or disables IP processing.
Step 5	Router (config-if)# **no negotiation auto**	Disables automatic negotiation on the interface.

	Command or Action	Purpose
Step 6	Router (config-if)# **switchport mode trunk**	Puts the port into permanent trunking mode.
Step 7	Router (config-if)# **service instance** *id* **ethernet**	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 8	Router (config-if-srv)# **encapsulation dot1q** *encapsulation-type vlan-id*	Defines the encapsulation type.
Step 9	Enter one of the following commands: • Router (config-if-srv)# **rewrite egress tag push dot1q** *encapsulation-type vlan-id* • Router (config-if-srv)# **rewrite ingress tag pop 1 symmetric** *encapsulation-type vlan-id*	• The **rewrite egress tag push dot1q** command specifies the encapsulation adjustment to be performed on a frame that is egressing a service instance. • The **rewrite ingress tag pop 1 symmetric** command specifies the encapsulation adjustment to be performed on a frame that is ingressing a service instance.
Step 10	Router (config-if-srv)# **bridge-domain** *bridge-id*	Configures the bridge domain.
Step 11	Router (config-if-srv)# **exit**	Exits Ethernet service configuration mode.
Step 12	Router (config-if)# **interface BDI** *bridge-id*	Enters the bridge domain interface.
Step 13	Router (config-if)# **ip address** *bdi-interface-ip-address*	Specifies the IP address of the BDI interface.
Step 14	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 15	Router (config-if)# **end**	Returns to global configuration mode on the host router.
Step 16	Use the server's operating system to configure the E-Series Server's **NIC** interface.	—
Step 17	Router# **ping** *server's-NIC-interface*	Shows if connection is established with the E-Series Server's **NIC** interface.
Step 18	Router# **show arp**	Displays the Access Resolution Protocol (ARP).
Step 19	Router# **show bridge-domain** *bridge-id*	Displays bridge domain information.

This example shows how to create an Ethernet Virtual Circuit using a non-native VLAN between the E-Series Server and the Cisco ISR 4451-X.

Note The IP addresses in this configuration example are for reference only.

```
Router> enable
Router# configure terminal
Router(config)# interface ucse 2/0/0
Router(config-if)# no ip address
Router(config-if)# no negotiation auto
Router(config-if)# switchport mode trunk
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite egress tag push dot1q 10
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# exit

Router(config-if)# interface BDI10
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end

Use the server's operating system to configure the E-Series Server's NIC interface.

Router#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              -   0022.bdfb.2783  ARPA   BDI10
Internet  192.168.1.2              1   0022.bde6.07b4  ARPA   BDI10

Router#show bridge-domain 10
Bridge-domain 10 (2 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 300 second(s)
    BDI10  (up)
    ucse2/0/0 service instance 10
   MAC address    Policy  Tag       Age  Pseudoport
   0022.BDE6.07B4 forward dynamic   246  ucse2/0/0.EFP10
   0022.BDFB.2783 to_bdi  static    0    BDI10
```

Note For additional details about the **rewrite** commands, see http://www.cisco.com/en/US/docs/ios-xml/ios/cether/command/ce-cr-book.html.

Understanding Network Interface Mapping

This section shows you how to determine the network interface mapping for the following devices:

- E-Series Server's Console, GE1, GE2, and GE3 interfaces—ISR G2
- E-Series Server's GE0, GE1, GE2, and GE3 interfaces—Cisco ISR 4451-X
- NetXtreme II 1 Gigabit Server (PCIe Card)
- NetXtreme II 10 Gigabit Server (PCIe Card)

Determining Network Interface Mapping for the E-Series Server's Console, GE1, GE2, and GE3 Interfaces—ISR G2

You can determine the port numbering of the E-Series Server by looking at the MAC addresses of the network interfaces. Note the following:

- Lowest numbered MAC address corresponds to the router's Console interface.
- Second lowest MAC address corresponds to the E-Series Server's GE1 interface.
- Third lowest MAC address corresponds to the E-Series Server's GE2 interface.
- Fourth lowest MAC address corresponds to the E-Series Server's GE3 interface.

Note To determine the MAC address of an interface, see the Determining the MAC Address in Microsoft Windows, Linux, and VMware vSphere Hypervisor , on page 98 section, or the appropriate platform documentation.

Determining Network Interface Mapping for the E-Series Server's GE0, GE1, GE2, and GE3 Interfaces—Cisco ISR 4451-X

You can determine the port numbering of the E-Series Server by looking at the MAC addresses of the network interfaces. Note the following:

- Lowest numbered MAC address corresponds to the E-Series Server's GE0 interface.
- Second lowest MAC address corresponds to the E-Series Server's GE1 interface.
- Third lowest MAC address corresponds to the E-Series Server's GE2 interface.
- Fourth lowest MAC address corresponds to the E-Series Server's GE3 interface.

Note To determine the MAC address of an interface, see the Determining the MAC Address in Microsoft Windows, Linux, and VMware vSphere Hypervisor , on page 98 section, or the appropriate platform documentation.

Determining the Interface Name and Port Mapping for the NetXtreme II 1 Gigabit Server

To determine which interface name maps to which port number in the NetXtreme II 1 Gigabit Server (PCIe card), do the following:

1. Connect the PCIe card's port 0 to an external network device using a network cable.
2. From the host operating system, check the status of the interface to determine which interface is connected.
3. Repeat Step 2 for ports 1, 2, and 3.

Note For information about how to determine the status of the interface, see the appropriate operating system documentation.

Determining the Interface Name and Port Mapping for the NetXtreme II 10 Gigabit Server

Note Only one port is enabled in the NetXtreme II 10 Gigabit Server (PCIe card).

To determine which interface name maps to which port number in the NetXtreme II 10 Gigabit Server (PCIe card), do the following:

1. Connect the PCIe card's port 0 to an external network device using a network cable.
2. From the host operating system, check the status of the interface to determine which interface is connected.

Note For information about how to determine the status of the interface, see the appropriate operating system documentation.

Determining the MAC Address in Microsoft Windows, Linux, and VMware vSphere Hypervisor

This section shows you how to determine the MAC addresses in Microsoft Windows, Linux, and VMware vSphere Hypervisor™.

Determining the MAC Address in the Microsoft Windows Operating System

To determine the MAC address of an interface in the Microsoft Windows operating systems, open a command window, and then enter the **ipconfig /all** command.

Determining the MAC Address in the Linux Operating System

To determine the MAC address of an interface in the Linux operating systems, open a terminal window, and then enter the **ifconfig -a** command to display the MAC address of all interfaces or **ifconfig** *interface-name* to display the MAC address of a particular interface.

Determining the MAC Address in the VMware vSphere Hypervisor

To determine the MAC address of an interface in the VMware vSphere Hypervisor™, do the following:

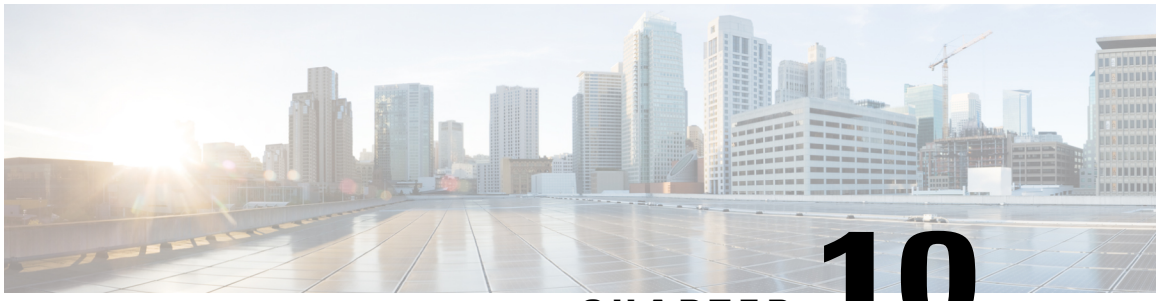
1. In your web browser, enter the IP address that you configured to access CIMC during initial setup and then log into CIMC.

   The CIMC Home page, which is the **Server Summary** page, appears.
2. From the **Actions** area of the **Server Summary** page, click the **Launch KVM Console** icon.

   The **KVM Console** opens in a separate window.
3. From the KVM Console, click the **KVM** tab, and then do the following:
   - Press **F2** to access the VMware vSphere Hypervisor™ DCUI customization menu. The **DCUI** login page appears.
   - Log into the **DCUI**. The **System Customization** page appears.

- From the **System Customization** page, click **Configure Management Network**.

  The **Configure Management Network** page appears, which has several menu options, including **Network Adapter**. The **Network Adapter** menu option allows you to view the MAC address of the interfaces.



CHAPTER 10

BIOS

This chapter includes the following sections:

BIOS Overview

BIOS initializes the hardware in the system. After it initializes the CPU, other chips on the motherboard get initialized. BIOS discovers bootable devices in the system and boots them in the provided sequence. It boots the operating system and configures the hardware for the operating system to use. BIOS manageability features allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, manage firmware, and create BIOS error reports.

BIOS provides the following features:

- Option ROM to provide PCI connected device boot
- Manage virtual and physical boot devices: SCSI, FC, network, and USB
- Processor Settings
- Memory Settings
- Power Management (C-states)

BIOS supports the following standard PC compatible functionality:

- ACPI 3.0, SMBIOS 2.5, WHEA, and USB 2.0
- EFI Shell boot

- EFI native operating system boot

Determining the Current BIOS Version

To view the current version and build number of the BIOS, press **F2** during server bootup. The **BIOS setup utility** appears. The listing on the **Main** page displays the current version and build number of the BIOS.

Options for Obtaining Firmware from Cisco Systems

- We recommend that you use the HUU ISO file to upgrade all firmware components, which includes the BIOS and CIMC firmware. For detailed instructions for upgrading the firmware using the HUU, see the "Upgrading the Firmware Using the HUU" section in the *Host Upgrade Utility User Guide for Cisco UCS E-Series Servers* at http://www.cisco.com/en/US/products/ps12629/prod_installation_guides_list.html.

Note The HUU is supported on CIMC, release 2.1.0 and later releases.

- If you choose to upgrade the CIMC and BIOS firmware manually, see Obtaining Software from Cisco Systems, on page 102.

Obtaining Software from Cisco Systems

Use this procedure to download drivers, BIOS and CIMC firmware, and the diagnostics image.

Procedure

Step 1 Navigate to http://www.cisco.com/.

Step 2 If you are not already logged in, click **Log In** at the top right-hand edge of the page and log in using your Cisco.com credentials.

Step 3 In the menu bar at the top, click **Support**.
A roll-down menu appears.

Step 4 From the Downloads (center) pane, click **All Downloads** (located at the bottom right corner).
The **Download Software** page appears.

Step 5 From the left pane, click **Products**.

Step 6 From the center pane, click **Unified Computing and Servers**.

Step 7 From the right pane, click **Cisco UCS E-Series Software**.

Step 8 From the right pane, click the name of the server model for which you want to download the software.
The **Download Software** page appears with the following categories.

- **Unified Computing System (UCSE) Server Drivers—**Contains drivers.

- **Unified Computing System (UCSE) Server Firmware—**Contains the Host Upgrade Utility and the BIOS and CIMC firmware images.
- **Unified Computing System (UCSE) Utilites—**Contains the diagnostics image.

Step 9 Click the appropriate software category link.

Step 10 Click the **Download** button associated with software image that you want to download.
The **End User License Agreement** dialog box appears.

Step 11 (Optional) To download multiple software images, do the following:

a) Click the **Add to cart** button associated with the software images that you want to download.

b) Click the **Download Cart** button located on the top right .
All the images that you added to the cart display.

c) Click the **Download All** button located at the bottom right corner to download all the images.
The **End User License Agreement** dialog box appears.

Step 12 Click **Accept License Agreement**.

Step 13 Do one of the following as appropriate:

- Save the software image file to a local drive.
- If you plan to install the software image from a TFTP server, copy the file to the TFTP server that you want to use.

  The server must have read permission for the destination folder on the TFTP server.

What to Do Next

Install the software image.

Installing the BIOS Firmware

You can install the BIOS firmware through the browser or from a TFTP server.

Installing the BIOS Firmware Through the Browser

Note To avoid potential problems, we strongly recommend that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels. For detailed information about this utility, see the *Host Upgrade Utility User Guide for Cisco UCS E-Series Servers* at http://www.cisco.com/en/US/products/ps12629/prod_installation_guides_list.html. This guide also provides information about the compatible HUU, CIMC, and BIOS software releases.

If you choose to upgrade the CIMC and BIOS firmware manually—instead of using the HUU—you must update the CIMC firmware first, and then the BIOS firmware. Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

Before You Begin

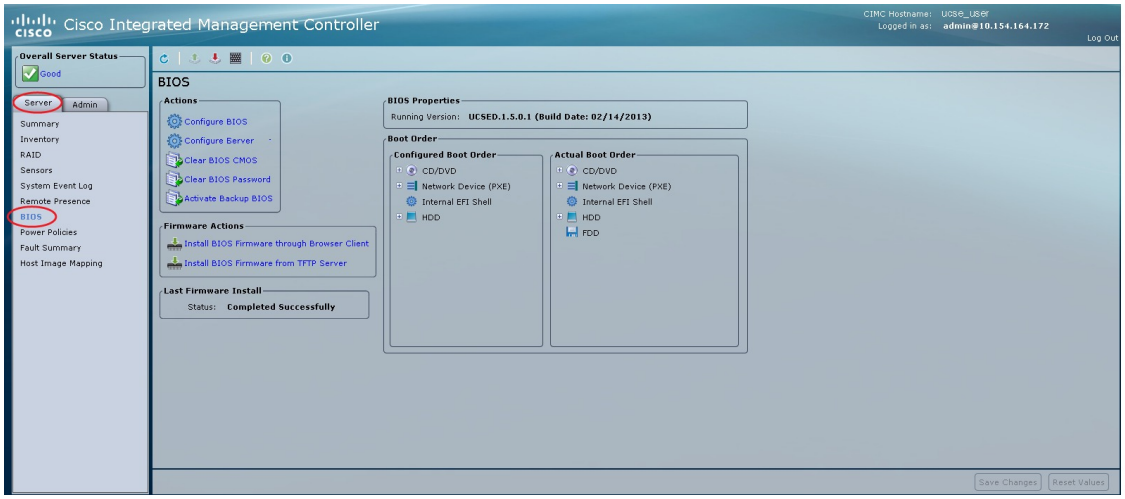
- Log in to CIMC as a user with admin privileges.
- Obtain the CIMC firmware file from Cisco Systems. See Obtaining Software from Cisco Systems, on page 102.
- Unzip the proper upgrade file to your local machine.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Figure 33: BIOS



Step 3 In the **Firmware Actions** area, click **Install BIOS Firmware through Browser Client**.

Step 4 In the **Install BIOS Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the file to install.

Step 5 Click **Install Firmware**.
The BIOS is downloaded, the host is powered off, the BIOS is upgraded, and then the host is powered on.

Installing the BIOS Firmware from a TFTP Server

Note To avoid potential problems, we strongly recommend that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels. For detailed information about this utility, see the *Host Upgrade Utility User Guide for Cisco UCS E-Series Servers* at http://www.cisco.com/en/US/products/ps12629/prod_installation_guides_list.html. This guide also provides information about the compatible HUU, CIMC, and BIOS software releases.

If you choose to upgrade the CIMC and BIOS firmware manually—instead of using the HUU—you must update the CIMC firmware first, and then the BIOS firmware. Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

Before You Begin

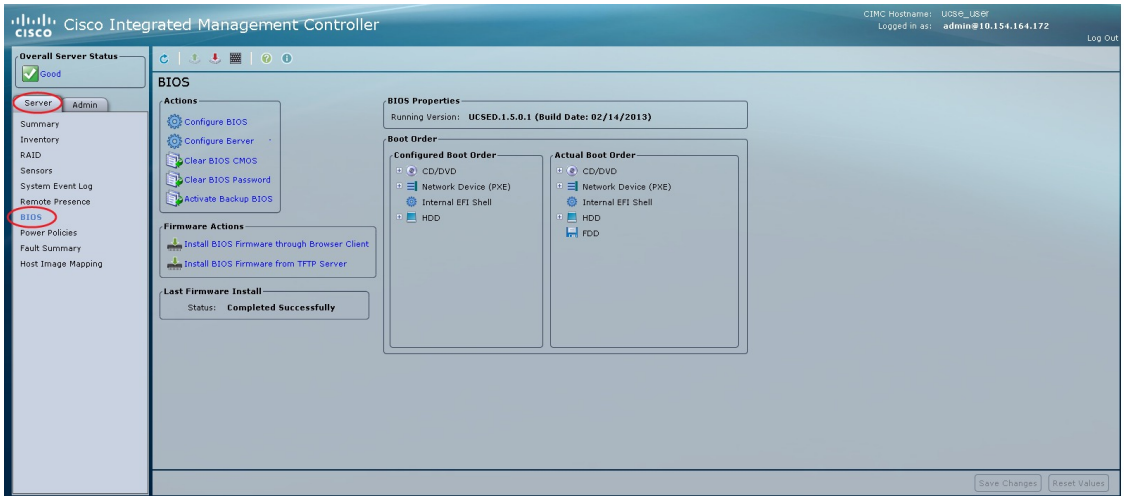
- Log in to CIMC as a user with admin privileges.
- Obtain the CIMC firmware file from Cisco Systems. See Obtaining Software from Cisco Systems, on page 102.
- Unzip the proper upgrade file on your TFTP server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Figure 34: BIOS



Step 3 In the **Firmware Actions** area, click **Install BIOS Firmware from TFTP Server**.

Step 4 In the **Install BIOS Firmware** dialog box, complete the following fields:

Name	Description
TFTP Server IP Address field	The IP address of the TFTP server on which the BIOS firmware image resides.
Image Path and Filename field	The BIOS firmware image filename on the server. When you enter this name, include the relative path for the image file from the top of the TFTP tree to the file location.

Step 5 Click **Install Firmware**.
The BIOS is downloaded, the host is powered off, the BIOS is upgraded, and then the host is powered on.

Accessing the BIOS Setup Menu

You can access the BIOS Setup menu in two ways:

- Through CIMC from the KVM console.
- Through a console that is physically attached to the E-Series Server.

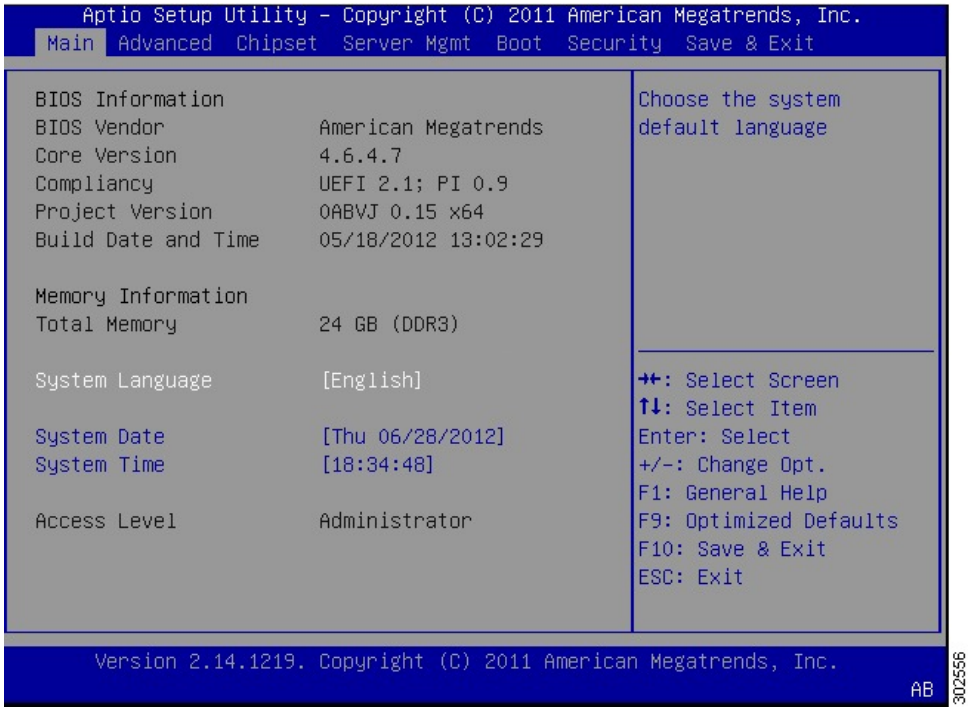
Accessing the BIOS Setup Menu from the KVM Console

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Summary**.
Step 3 From the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.
Step 4 From the **Server Summary** page, click **Power Cycle Server** to reboot the server.
Step 5 To access the BIOS setup menu, press **F2** during bootup.

The **Aptio Setup Utility** appears, which provides the BIOS setup menu options.

Figure 35: BIOS Setup Menu



The following table provides information about the BIOS setup menu tabs.

Tabs	Description
Main tab	Provides the following: • General information about the BIOS version, system memory, and access level • Settings to define the system date, time, and language
Advanced tab	Allows you to do the following: • Enable or disable boot option for legacy network devices and legacy mass storage devices with option ROM • Configure PCI, PCI-X, and PCI express, trusted computing settings, and WHEA configuration settings • Configure CPU, thermal, USB, and system IO chip parameters • Configure runtime error logging support setup options • Configure console redirection to the serial port

Chipset tab	Allows you to do the following: • Define North Bridge, South Bridge, and ME subsystem parameters
Server Mgmt tab	Provides the self test status of CIMC and allows you to do the following: • Enable or disable interfaces to communicate with CIMC • Enable or disable FRB-2 timer • Configure the FRB-2 timer expiration value and configure how the system responds when the FRB-2 timer expires • Enable or disable the OS watchdog timer • Log the report returned by the CIMC self test command • Change the system event log configuration
Boot tab	Allows you to do the following: • Configure the time in seconds the system should wait for the setup activation key • Enable or disable the keyboard NumLock keys • Define boot order rules • Configure Gate A20 parameters • Enable or disable CSM support • Define boot order for devices in the following groups: hard disk drives, network devices, CDROM, DVD, and floppy drives
Security tab	Allows you to do the following: • Define or change the BIOS administrator and user passwords
Save & Exit tab	Provides options to do the following: • Save changes, discard changes, or restore the configuration to its default settings

Changing Configuration Using the BIOS Setup Menu

Use this procedure to change the BIOS settings for your server. Detailed instructions are also printed on the BIOS pages.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

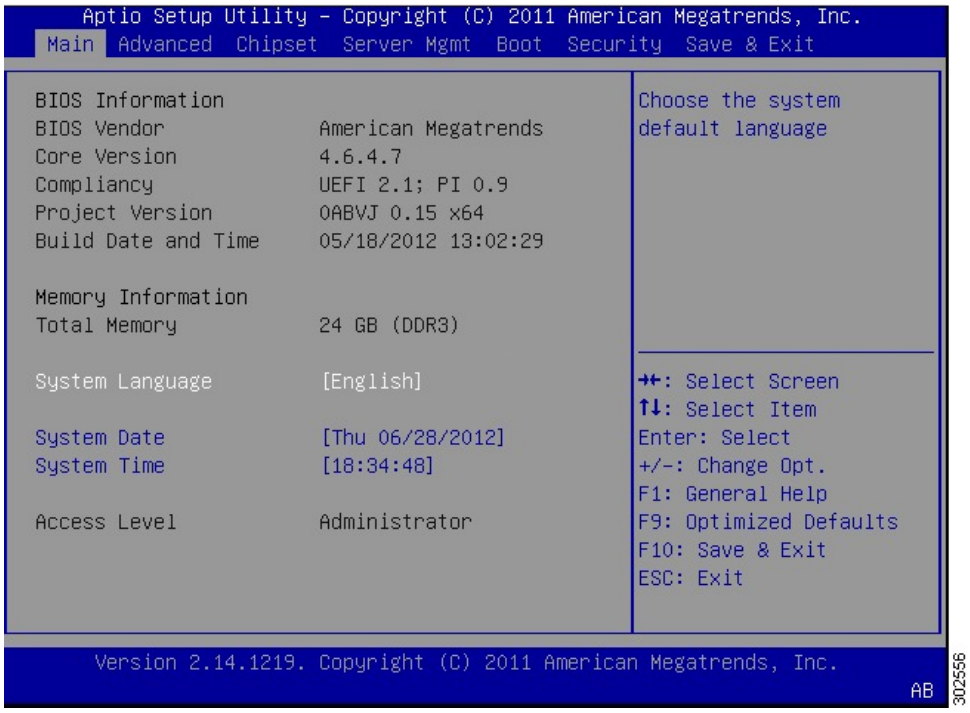
Step 2 On the **Server** tab, click **Summary**.

Step 3 From the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.

Step 4 From the **Server Summary** page, click **Power Cycle Server** to reboot the server.

Step 5 To access the BIOS setup menu, press **F2** during bootup.
The **Aptio Setup Utility** appears, which provides the BIOS setup menu options.

Figure 36: BIOS Setup Menu



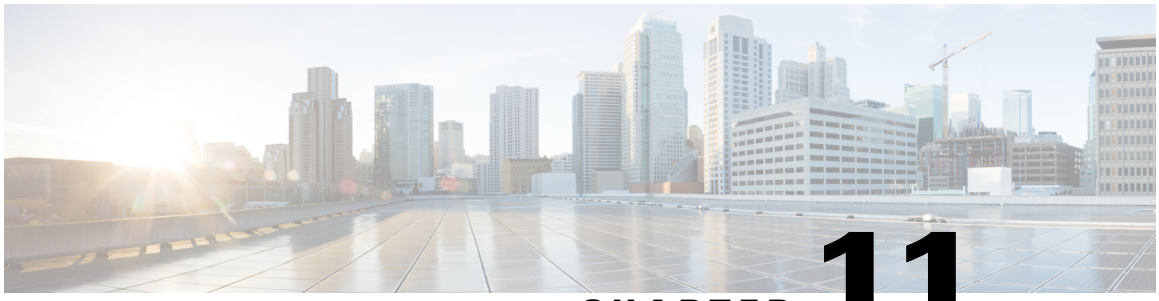
Step 6 To navigate between menu items, use the **right** or **left arrow keys** on your keyboard.

Step 7 To modify a field, do the following:

a) Use the **Up** or **Down arrow keys** on your keyboard to highlight the field to be modified.
b) Press **Enter** to select the highlighted field, and then change the value in the field.
c) Do one of the following:

- To save changes and exit the BIOS setup, press **F4**.
- To exit without saving changes, press **Esc**.

Step 8 To enable or disable a field, press the **space bar** on your keyboard.



CHAPTER 11

Recovering from Corrupt CIMC Firmware

This chapter includes the following sections:

CIMC Firmware Image Overview

If you have problems booting the E-Series Server, it could be that the CIMC firmware image is corrupted, or the SD card is faulty, or the file system is corrupted, or the CIMC firmware installation did not complete successfully. To recover from a corrupt CIMC firmware image, do one of the following as appropriate:

Important Due to security considerations, the **boot backup** command is disabled.

- If the CIMC firmware image is corrupted, see Recovering from a Corrupted CIMC Firmware Image, on page 111.
- If the SD card is faulty, see Recovering from a Faulty SD Card.
- If the file system is corrupted, see Recovering from a Corrupted File System, on page 115.
- If the CIMC firmware installation did not complete successfully, reinstall the CIMC firmware.

Recovering from a Corrupted CIMC Firmware Image

Before You Begin

- Connect the E-Series Server to your PC. Depending on the type of E-Series Server, do one of the following as appropriate:

- Double-wide—Connect one end of the serial cable to the E-Series Server's serial port and the other end to your PC.
- Single-wide—First, connect a KVM connector to the E-Series Server's KVM port; and then connect one end of a serial cable to the DB9 port of the KVM connector and the other end to your PC.

- Attach an Ethernet cable into the Management (dedicated) port of the E-Series Server.
- To view the serial output, start the Hyper Terminal or Minicom as appropriate. Do one of the following:
  - Microsoft Windows—Start Hyper Terminal.
  - Linux—Start Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router# **hw-module sm** *slot* **oir-stop**	Shuts down the power to the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2.
Step 2	Router# **hw-module sm** *slot* **oir-start**	Restarts the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2.
Step 3	***	From the Hyper Terminal or Minicom, enter the *** command to enter the bootloader prompt.
Step 4	ucse-cimc > **boot current recovery**	Boots the E-Series Server from the current image.
Step 5	Recovery-shell # **dedicated-interface** *management-interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the E-Series Server's Management (dedicated) interface.
Step 6	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 7	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote tftp server.

	Command or Action	Purpose
Step 8	Recovery-shell # **reboot**	Reboots CIMC.

This example recovers the CIMC firmware image:

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# dedicated-interface 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
        IP config: addr: 192.168.0.138 Mask: 255.255.255.0
        Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ...
activating installed image
done
Stage: NONE
Status: SUCCESS
Error: Success
recovery-shell# reboot
```

Recovering from a Faulty SD Card

If you have problems booting the E-Series Server, it could be because the SD card is faulty. Use this procedure to recover the CIMC firmware image on a new SD card.

Before You Begin

- Connect the E-Series Server to your PC. Depending on the type of E-Series Server, do one of the following as appropriate:
  - Double-wide—Connect one end of the serial cable to the E-Series Server's serial port and the other end to your PC.
  - Single-wide—First, connect a KVM connector to the E-Series Server's KVM port; and then connect one end of a serial cable to the DB9 port of the KVM connector and the other end to your PC.
- Attach an Ethernet cable into the Management (dedicated) port of the E-Series Server.
- To view the serial output, start the Hyper Terminal or Minicom as appropriate. Do one of the following:
  - Microsoft Windows—Start Hyper Terminal.
  - Linux—Start Minicom.

- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router# **hw-module sm** *slot* **oir-stop**	Shuts down the power to the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2.
Step 2	Remove the faulty SD card and insert a new one.	Replaces the faulty SD card.
Step 3	Router# **hw-module sm** *slot* **oir-start**	Restarts the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2.
Step 4	***	From the Hyper Terminal or Minicom, enter the *** command to enter the bootloader prompt.
Step 5	ucse-cimc > **boot current recovery**	Boots the E-Series Server from the current image.
Step 6	Recovery-shell # **dedicated-interface** *management-interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the E-Series Server's Management (dedicated) interface.
Step 7	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 8	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote tftp server.
Step 9	Recovery-shell # **reboot**	Reboots CIMC.

This example recovers the CIMC firmware from the current image:

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# dedicated-interface 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
```

```
        IP config: addr: 192.168.0.138 Mask: 255.255.255.0
        Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ...
activating installed image
done
Stage: NONE
Status: SUCCESS
Error: Success
recovery-shell# reboot
```

Recovering from a Corrupted File System

Use this procedure if you see the following error message in the CIMC boot log files.

```
UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY
```

Before You Begin

- Connect the E-Series Server to your PC. Depending on the type of E-Series Server, do one of the following as appropriate:
  - Double-wide—Connect one end of the serial cable to the E-Series Server's serial port and the other end to your PC.
  - Single-wide—First, connect a KVM connector to the E-Series Server's KVM port; and then connect one end of a serial cable to the DB9 port of the KVM connector and the other end to your PC.
- Attach an Ethernet cable into the Management (dedicated) port of the E-Series Server.
- To view the serial output, start the Hyper Terminal or Minicom as appropriate. Do one of the following:
  - Microsoft Windows—Start Hyper Terminal.
  - Linux—Start Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

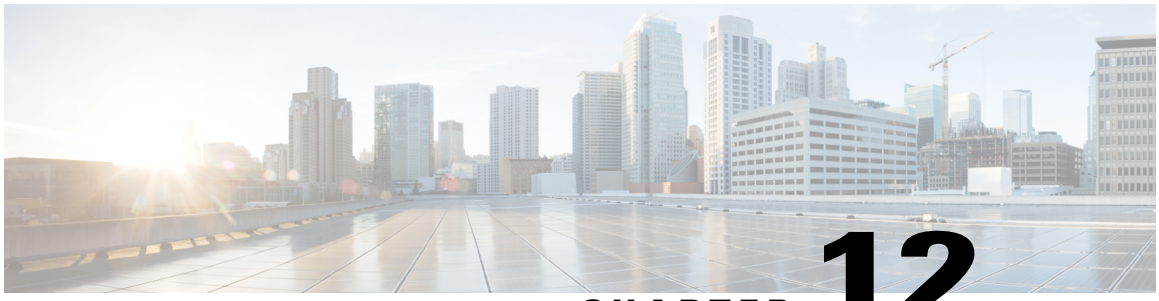
	Command or Action	Purpose
Step 1	Router# **hw-module sm** *slot* **oir-stop**	Shuts down the power to the specified E-Series Server.

	Command or Action	Purpose
		Note The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2.
Step 2	Router# **hw-module sm** *slot* **oir-start**	Restarts the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2.
Step 3	***	From the Hyper Terminal or Minicom, enter the *** command to enter the bootloader prompt.
Step 4	ucse-cimc > **boot current recovery**	Boots the E-Series Server from the current image.
Step 5	To check the file system of the specified partition and recover the corrupted file system, enter these commands.	**1** Recovery-shell # **fs-check [p3 | p4]** **Note** You can only use p3 and p4 partitions with this command. Use this command on the partition that is corrupted. The corrupted partition is the one that displays the **run fsk** error message during CIMC bootup. **2** Do the following: • If the command output displays **clean**, it indicates that the corrupted files are recovered. Enter the **reboot** command to reboot CIMC. **Note** Skip the steps that follow. • If the command output does not display **clean**, proceed to Step 6.
Step 6	(Optional) If the **fs-check [p3 | p4]** command does not recover the corrupted file system, and the output does not display **clean**, enter these commands to format the partitions.	**1** Recovery-shell # **sd-card format [p3 | p4]** Formats the specified corrupted partition on the SD card. **Note** The corrupted partition is the one that displays the **run fsk** error message during CIMC bootup. **2** Recovery-shell # **reboot** Reboots CIMC. **Note** Skip the steps that follow. **Note** When the p3 partition is formatted, the CIMC configuration is lost.

	Command or Action	Purpose
Step 7	(Optional) If the **sd-card format [p3 | p4]** command does not recover the corrupted file system, enter these commands to partition and format the SD card.	**1** Recovery-shell # **sd-card partition** Creates partitions on the SD card. **2** Recovery-shell # **sd-card format p3** Formats the p3 partition on the SD card. **3** Recovery-shell # **sd-card format p4** Formats the p4 partition on the SD card. **4** Recovery-shell # **reboot** Reboots CIMC. **5** (Optional) Recovery-shell # **sd-partition show** Displays the current partition on the SD card. **Note** When you partition the SD card, the contents of the SD card, such as, the configuration and ISO file, are lost.
Step 8	Recovery-shell # **dedicated-interface** *management-interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the E-Series Server's Management (dedicated) interface.
Step 9	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 10	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote tftp server.
Step 11	Recovery-shell # **reboot**	Reboots CIMC.

This example recovers the CIMC firmware from the current image using the **fs-check p3** command:

```
Router# hw-module sm 2 oir-stop
Router# hw-module sm 2 oir-start

***

ucse-cimc > boot current recovery
recovery-shell# fs-check p3
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p4: clean, 51/506912 files, 1880262/2025296 blocks
recovery-shell# reboot
```



CHAPTER 12

Diagnostic Tests

This chapter includes the following sections:

Diagnostic Tests Overview

Diagnostics is a standalone utility that runs on the E-Series Server independent of the operating system or applications running on the server. If you experience problems with the E-Series Server, you can use diagnostics tests to run a preliminary check and isolate the problem. Diagnostic tests can be executed on the server CPU, memory, and block devices. Block devices include hard drive, USB drive, and SD cards.

If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco Technical Assistance Center (TAC) at: http://www.cisco.com/cisco/web/support/index.html to isolate the problem.

If the diagnostic tests fail, open a service request with Cisco TAC for further assistance.

Caution Diagnostic tests are non-destructive, but if there is a power or equipment failure when the tests are running, there is a possibility that the disk data might get corrupted. We highly recommend that you backup the data before running these tests.

Basic Workflow for Executing Diagnostic Tests

1. Backup data.
2. The diagnostics image is pre-installed on the E-Series Server at the time of purchase. You can also choose to download the most current diagnostics image from a specified FTP or HTTP server onto the CIMC internal repository.
3. Mount the diagnostics image onto the HDD virtual drive of a USB controller.

4 Set the boot order to make EFI Shell as the first boot device.

5 Reboot the server.

6 Run diagnostic tests from the EFI Shell.

7 Reset the virtual media boot order to its original setting.

Mapping the Diagnostics Image to the Host

Before You Begin

- Backup data.
- Log in to CIMC as a user with admin privileges.
- The diagnostics image is pre-installed on the E-Series Server at the time of purchase. You can also choose to download the most current diagnostics image from a specified FTP or HTTP server onto the CIMC internal repository. See Obtaining Software from Cisco Systems.

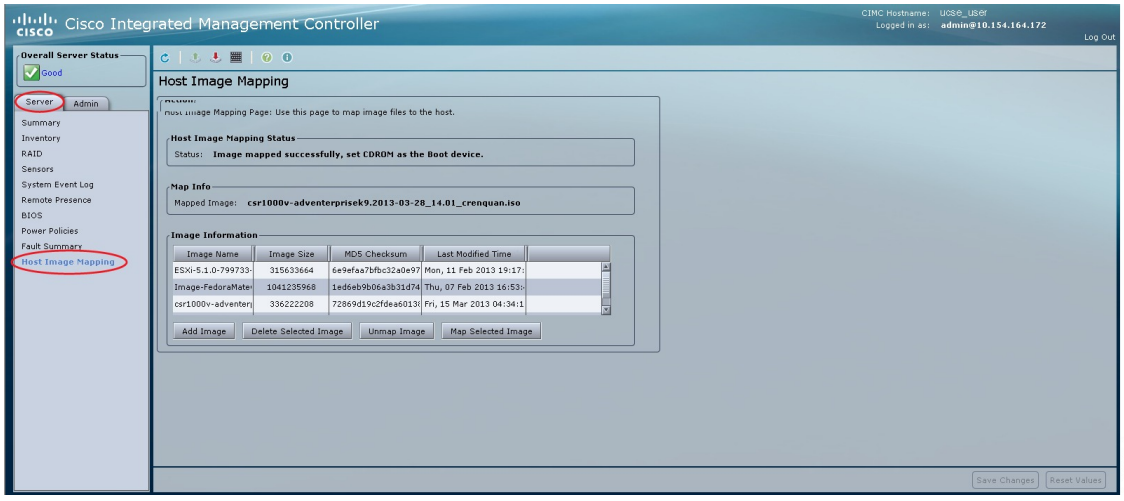
Note If you start an image update while an update is already in process, both updates will fail.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Host Image Mapping**.

Figure 37: Host Image Mapping



Step 3 From the **Host Image Mapping** page, click **Add Image**.
The **Download Image** dialog box opens. Complete the following fields:

Name	Description
Download Image From drop-down list	The type of remote server on which the image is located. This can be one of the following: • **FTP** • **HTTP** **Note** Depending on the remote server that you select, the fields that display change.
FTP or **HTTP Server IP Address** field	The IP address of the remote FTP or HTTP server.
FTP or **HTTP File Path** field	The path and filename of the remote FTP or HTTP server. The path and filename can contain up to 80 characters. • If you are installing a host image, that image must have .iso or .img as the file extension. • If you are installing a diagnostics image, that image must have .diag as the file extension.
Username field	The username of the remote server. The username can contain 1 to 20 characters. **Note** If the username is not configured, enter **anonymous** for the username and any character(s) for the password.
Password field	The password for the username. The password can contain 1 to 20 characters. **Note** If the username is not configured, enter **anonymous** for the username and any character(s) for the password.

Step 4 Click **Download**.
The **Host Image Mapping** page opens. You can view the status of the image download in the **Host Image Mapping Status** area. After the image is downloaded and processed successfully, refresh the page. After the page refreshes, the new image displays in the **Image Information** area.

Step 5 From the **Image Information** area, select the image to map, and then click **Map Selected Image**.
The image is mapped and mounted on the virtual drive of a USB controller.

Step 6 Set the boot order to make **EFI Shell** as the first boot device.
To set the boot order, see Configuring the Server Boot Order.

Step 7 Reboot the server.
The EFI Shell appears.

What to Do Next

Run diagnostic tests.

Running Diagnostic Tests

From the EFI shell, use the following procedure to run diagnostic tests.

Before You Begin

- Back up data. All tests are non-destructive, but if there is power or equipment failure when the tests are running, there is a possibility that the disk data might get corrupted. We highly recommend that you back up data before executing these tests.
- Use the CIMC CLI or the CIMC GUI to download and map the diagnostics image onto the HDD virtual drive of the USB controller.
- Reboot the server. The EFI shell displays.

Procedure

	Command or Action	Purpose
Step 1	Shell > **dir** *virtual-media-drive-name***:**	Displays all the file packages that exist in the specified virtual media drive. The drive name starts with fs0 and can be fs0, fs1, fs2, and so on. **Note** Make sure that you add a colon after the virtual media drive name. For example, **dir fs1:**
Step 2	Shell > *virtual-media-drive-name***:**	Enters the virtual media drive in which the diagnostic file is located.
Step 3	Virtual Media Drive :\> **cp** *package-file-name* **dsh.pkg**	Copies the package file for which you are running diagnostics into the diagnostics shell package file.
Step 4	Virtual Media Drive :\> **dsh**	Enters the Diagnostics Shell. At the confirmation prompt, answer **y**.
Step 5	Server: SRV > **run all**	Executes all available diagnostic tests and displays the progress and status of the tests. Diagnostic tests are run on the server CPU, memory, and block devices. Block devices include hard drive, USB drive, and SD cards. To execute a specific diagnostic test on the server, use the **run** *test-name* command where *test-name* can be one of the following: • **cpux64—**CPU diagnostic test. • **diskx64—**Block devices diagnostic test. Block devices include hard drive, USB drive, and SD cards. • **memoryx64—**Memory diagnostic test.

	Command or Action	Purpose
		Note Diagnostic tests can run for approximately 10 minutes.
Step 6	(Optional) Server: SRV > **results**	Displays a summary of the diagnostic test with **Passed** or **Failed** test status. **Note** The summary report indicates the number of tests that failed and passed. It does not provide information about which tests failed or passed. To determine which tests failed and passed, see the output of the **run all** command.
Step 7	(Optional) Server: SRV > **show**	Displays a list of global parameters and diagnostic test modules that were administered on the server.
Step 8	Server: SRV > **exit**	Exits from Diagnostic Shell.
Step 9	Open a service request with Cisco TAC.	If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco TAC to isolate the problem. If the diagnostic tests fail, open a service request with Cisco TAC for further assistance.

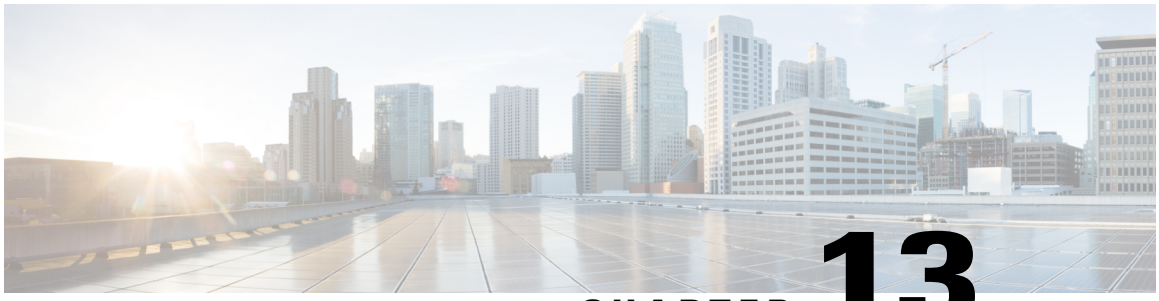
This example runs all diagnostic tests:

```
Shell > dir fs1:
  06/27/12  07:48p            1,435,424  Dsh.efi
  06/27/12  08:03p               10,036  dsh-e140d.pkg
  06/25/12  06:00p               10,140  dsh-e140s.pkg
  06/27/12  08:04p               10,042  dsh-e160d.pkg
          4 File(s)   1,465,642 bytes
Shell > fs1:
fs1:\> cp dsh-e140d.pkg dsh.pkg
copying fs0:\OBD\dsh-e140d.pkg -> fs0:\OBD\dsh.pkg
- [ok]
fs1:\> dsh
Diagnostics is a standalone utility that runs on the server module independent
of the operating system or applications running on the module.All tests are
non-destructive, but there is a possibility of disk datacorruption during
power or equipment failure when the tests are in progress. Therefore, before
executing these tests, we highly recommend that you backup the data.


For questions or concerns with this utility, please open a Service Request
with Cisco TAC at http://www.cisco.com/cisco/web/support/index.html

(Y)es to continue test. (N)o to exit(y/n): Y
Cisco Diagnostics  Shell 1.03(0.3) Thu 06/28/-16:35:08.95-canis-diag@cisco.com
UCS-E140D-M1/K9:SRV>

Server: SRV > run all
Server: SRV > results
Test Name          : all
Test Status        : Passed
Failed/Run History : 0/17
Start Time         : 06/27/12 14:38:19
End Time           : 06/27/12 14:43:36
Diag Version       : 1.03(0.3) Mon 04/02/-17:07:57.19-canis-diag@cisco.com
```

```
Board S/N          : FOC160724BY

Server: SRV > show
Server: SRV > exit
```

What to Do Next

Reset the virtual media boot order to its original setting.



CHAPTER 13

Cisco IOS Software Command Reference—ISR G2

This chapter provides the new Cisco IOS commands that were introduced for the E-Series Servers installed in the ISR G2.

Note The Cisco IOS commands are sometimes updated after original publication; therefore, for updated content, review the *Cisco IOS Interface and Hardware Component Command Reference* at http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-cr-book.html.

This chapter includes the following sections:

imc ip address default-gateway

To configure a static IP address for CIMC and the IP address of the default gateway router that CIMC must use, use the **imc ip address default-gateway** command from interface configuration mode .

imc ip address *i ip_address subnet_mask* **default-gateway** *gateway_address*

no imc ip address *i* **p_address subnet_mask default-gateway** *gateway_address*

Syntax Description

ip_address	IP address of CIMC.
subnet_mask	Subnet mask to append to the IP address; must be in the same subnet as the host router.
gateway_address	IP address of the default gateway router.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

If you do not enable DHCP, you must specify a static IP address and subnet mask.

The following example shows how to configure a static IP address for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
```

imc ip address dhcp

To configure a dynamic IP address for CIMC, use the **imc ip address dhcp** command from interface configuration mode .

imc ip address dhcp

no imc ip address

Syntax Description

This command has no arguments.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

The following example shows how to configure the DHCP ip address for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address dhcp
```

imc vlan

To enter VLAN configuration mode for the specified VLAN number, use the **imc vlan** command from interface configuration mode .

imc vlan *vlan_number*

no imc vlan

Syntax Description

vlan_number	IP address of the remote manager.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

The following example shows how to enter the VLAN configuration mode in CIMC for a specified VLAN:

```
Router(config)# interface ucse 2/0
Router(config-if)# interface vlan 40
```

ucse cmos-reset

To reset the BIOS CMOS of the Cisco E-Series Server, use the **ucse cmos-reset** command in EXEC mode.

ucse *slot* **cmos-reset**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command sets the BIOS (Basic Input Output System) back to the factory defaults. User changes made in the BIOS will be lost.

The following example shows how to reset the BIOS CMOS:

```
Router# ucse 2 cmos-reset
```

ucse password-reset

To reset the BIOS, CIMC, or RAID password, use the **ucse password-reset** command in EXEC mode.

ucse *slot* **password-reset** {**BIOS**| **BMC**| **RAID**}

Syntax Description

slot	Router slot number in which the server module is installed.
BIOS	Resets the BIOS password.
BMC	Resets the CIMC password.
RAID	Resets the RAID password.

Command Modes Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was first introduced in the Cisco UCS E-Series Servers.

Usage Guidelines After this command has been entered, the system requests that a new password be set when accessing the BIOS or BMC.

The following example shows how to reset the BIOS password:

```
Router# ucse 2 password-reset BIOS
Reset command sent
```

ucse session

To start or close a Cisco E-Series Server host or CIMC session, use the **ucse session** command in EXEC mode.

ucse *slot* **session** {**imc [clear]**| **host [clear]**}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
imc	Starts a session with CIMC.
imc clear	Clears the existing CIMC session.
host	Starts a session with the host Cisco E-Series Server.
host clear	Clears the host Cisco E-Series Server session.

Command Modes Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

The **imc clear** and **host clear** commands close the active session of the CIMC or the host. As a result, the system closes the sessions of any other users currently logged in.

Only one active session is allowed in the CIMC or host at any time. If you receive a "connection refused" message when sessioning in, close the current active session by entering the **imc clear** or **host clear** commands.

The following example shows how to clear the CIMC session:

Router# ucse 2 session imc clear

ucse shutdown

To shut down the Cisco E-Series Server system gracefully, use the **ucse shutdown** command in EXEC mode.

ucse *slot* **shutdown**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command when removing or replacing a hot-swappable module during online insertion and removal (OIR).

The following example shows how to gracefully shut down the server:

Router# ucse 2 shutdown

ucse statistics

To display or clear the reset and reload information of the Cisco E-Series Server, use the **ucse statistics** command in EXEC mode.

ucse *slot* **statistics clear**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
clear	Clears the Cisco E-Series Server's reset and reload information.

Command Modes Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines None.

The following example shows how to display the server statistics:

```
Router# ucse 2 statistics

Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 0
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 1
```

ucse status

To display configuration information related to the hardware and software on the Cisco E-Series Server, use the **ucse status** command in EXEC mode.

ucse *slot* **status [detailed]**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
detailed	Displays detail information about the Cisco E-Series Server such as the status of the service module and settings of the reset and heartbeat-reset flags.

Command Modes Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

None.

The following example shows how to display server status:

```
Router# ucse 2 status

Service Module is Cisco ucse 2/0
Service Module supports session via TTY line 131
Service Module is in Steady state
Service Module reset on error is disabled
Service Module heartbeat-reset is enabled
```

ucse stop

To power down the Cisco E-Series Server immediately, use the **ucse stop** command in EXEC mode.

ucse *slot* **stop**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.

Command Modes

Privileged EXEC mode.

Command History

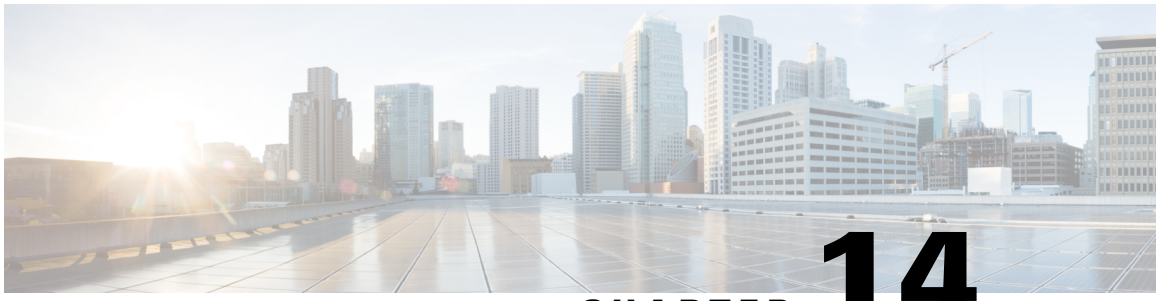
Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

None.

The following example shows how to power down the server:

```
Router# ucse 2 stop

Send server stop command
```



CHAPTER 14

Cisco IOS Software Command Reference—Cisco ISR 4451-X

This chapter provides the new Cisco IOS commands that were introduced for the E-Series Servers installed in the Cisco ISR 4451-X.

Note The Cisco IOS commands are sometimes updated after original publication; therefore, for updated content, review the *Cisco IOS Interface and Hardware Component Command Reference* at http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-cr-book.html.

This chapter includes the following sections:

debug platform software ucse

To debug the Cisco UCS E-Series Server (UCSE) platform software and display debug messages, use the **debug platform software ucse** command in privileged EXEC mode. To disable debug, use the **no** form of this command.

debug platform software ucse {**all**| **error**| **normal**}

no debug platform software ucse {**all**| **error**| **normal**}

Syntax Description

all	Displays all platform debug messages.
error	Displays error debug messages.
normal	Displays normal debug messages.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Usage Guidelines

After you use the **debug platform software ucse all** command, use the appropriate **ucse** command to display debug messages.

The following example shows how to display debug messages for the **ucse subslot imc password-reset** command:

```
Router# debug platform software ucse all
Router#
Router# ucse subslot 2/0 imc password-reset
 ucse2/0/0
Password reset command sent.
Router#
 IMC ACK: UCSE password reset successful for IMC
 ACK received for UCSE: Password Reset Command
```

hw-module subslot session

To start or close a Cisco Integrated Management Controller (CIMC) or host server module session, use the **hw-module subslot session** command in privileged EXEC mode.

hw-module subslot *slot*/*port-adapter* **session** {**imc**| **server**}

Syntax Description

slot/	Number of the router slot in which the server module is installed.

port-adapter	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.
imc	Starts a session with CIMC.
server	Starts a session with the host server module.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Usage Guidelines Only one active session is allowed in the CIMC or server module at any time.

The following example shows how to start a CIMC session:

```
Router# hardware-module subslot 1/0 session imc
```

The following example shows how to start a server module session:

```
Router# hardware-module subslot 1/0 session server
```

imc ip dhcp

To configure a dynamic IP address for the Cisco Integrated Management Controller (CIMC), use the **imc ip dhcp** command in UCSE configuration mode. To unconfigure the dynamic IP address, use the **no** form of this command.

imc ip dhcp

no imc ip dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes UCSE configuration (config-ucse)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

The following example shows how to configure a dynamic IP address for CIMC:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip dhcp
Router(config-ucse)#
 IMC ACK: DHCP enable received for IMC.

 IMC ACK: UCSE setting DHCP enable for IMC successful.
```

show interfaces ucse

To display Cisco UCS E-Series Server (UCSE) interface statistics, use the **show interfaces ucse** command in privileged EXEC mode.

show interfaces ucse *slot*/*port-adapter*/*ucse-interface* [**accounting**| **controller**| **counters**| **crb**| **dampening**| **description**| **etherchannel**| **history**| **irb**| **mac-accounting**| **monitor**| **mpls-exp**| **precedence**| **stats**| **summary**| **switchport**]

Syntax Description

slot/	Number of the router slot in which the server module is installed.
port-adapter/	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.
ucse-interface	Number of the UCSE interface. **Note** For Cisco UCS E-Series Servers, the UCSE interface number can be 0 or 1.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
controller	(Optional) Displays the interface, configuration, and controller status.
counters	(Optional) Displays the interface counters.
crb	(Optional) Displays interface routing or bridging information.

dampening	(Optional) Displays interface dampening information.
description	(Optional) Displays the interface description.
etherchannel	(Optional) Displays interface Ether Channel information.
history	(Optional) Displays interface history.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
monitor	(Optional) Displays interface continuously.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays interface precedence accounting information.
stats	(Optional) Displays the switching path, the packets in and packets out, and the characters in and characters out.
summary	(Optional) Displays the interface summary.
switchport	(Optional) Displays the switch port interface information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

The following example provides sample output from the **show interfaces ucse** *slot*/**0/0 switchport** command.

```
Router# show interfaces ucse 1/0/0 switchport

 Name: ucse 1/0/0
 Switchport: Enabled
 Administrative mode: trunk
```

```
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Disabled
Trunking Native Mode VLAN: 2352
Trunking VLANs Enabled: 1-2349,2450-4094
Voice VLAN: none
```

ucse subslot imc password-reset

To reset the Cisco Integrated Management Controller (CIMC) password, use the **ucse subslot imc password-reset** command in privileged EXEC mode.

ucse subslot *slot*/*port-adapter* **imc password-reset**

Syntax Description

slot/	Number of the router slot in which the server module is installed.
port-adapter	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Usage Guidelines

After you enter this command, at the next login, the system requests that you set a new password to access CIMC.

The following example shows how to reset the CIMC password:

```
Router# ucse subslot 1/0 imc password-reset
Router#
 IMC ACK: UCSE password reset successful for IMC
```

ucse subslot server

To reload, reset, start, or stop the hardware on the server module, use the **ucse subslot server** command in privileged EXEC mode.

ucse subslot *slot*/*port-adapter* **server** {**reload**| **reset**| **start**| **stop**}

Syntax Description

slot/	Number of the router slot in which the server module is installed.
port-adapter	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.
reload	Gracefully shuts down the server module and then powers it on.
reset	Resets the hardware on the server module.
start	Powers on the server module.
stop	Immediately powers down the server module.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Usage Guidelines

Use the **reset** keyword only to recover from a shutdown or failed state.

Caution Using the **reset** keyword does *not* provide an orderly software shutdown and may impact file operations that are in progress.

The following example shows how to reload the server:

```
Router# ucse subslot 1/0 server reload
Router#
 IMC ACK: UCSE Server reload successful.
```

The following example shows how to reset the server:

```
Router# ucse subslot 1/0 server reset
Router#
 IMC ACK: UCSE Server reset successful.
```

The following example shows how to start the server:

```
Router# ucse subslot 1/0 server start
Router#
```

```
 IMC ACK: UCSE Server start successful.
```

The following example shows how to stop the server:

```
Router# ucse subslot 1/0 server stop
Router#
 IMC ACK: UCSE Server stop successful.
```

ucse subslot server password-reset

To reset the BIOS or RAID password, use the **ucse subslot server password-reset** command in privileged EXEC mode.

ucse subslot *slot*/*port-adapter* **server password-reset** {**BIOS**| **RAID**}

Syntax Description

slot/	Number of the router slot in which the server module is installed.
port-adapter	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.
BIOS	Resets the BIOS password.
RAID	Resets the RAID password.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Usage Guidelines

After you enter this command, at the next login, the system requests that you set a new password to access BIOS or configure RAID.

The following example shows how to reset the BIOS password:

```
Router# ucse subslot 1/0 server password-reset BIOS
Router#
 IMC ACK: UCSE password reset successful for BIOS
```

The following example shows how to reset the RAID password:

```
Router# ucse subslot 1/0 server password-reset RAID
Router#
 IMC ACK: UCSE password reset successful for RAID
```

ucse subslot shutdown

To gracefully shut down the server module, use the **ucse subslot shutdown** command in privileged EXEC mode.

ucse subslot *slot*/*port-adapter* **shutdown**

Syntax Description

slot/	Number of the router slot in which the server module is installed.
port-adapter	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

The following example shows how to shut down the server module:

```
Router# ucse subslot 1/0 shutdown
Router#
 IMC ACK: UCSE Server shutdown successful.
```

ucse subslot statistics

To display or clear server module statistics, use the **ucse subslot statistics** command in privileged EXEC mode.

ucse subslot *slot*/*port-adapter* **statistics [clear]**

Syntax Description

slot/	Number of the router slot in which the server module is installed.

port-adapter	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.
clear	(Optional) Clears the server module statistics.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

The following example shows how to display the server module statistics:

```
Router# ucse subslot 1/0 statistics
 Count of number of shutdowns command : 1
 Count of number of status commands : 0
 Count of number of server raid password  : 1
 Count of number of imc password-reset : 2
 Count of number of server bios password reset : 1
 Count of number of server reload : 1
 Count of number of server reset : 1
 Count of number of server start : 1
 Count of number of server stop : 1
 Count of number of vlan commands : 0
 Count of number of access-port commands : 1
 Count of number of IMC configured IP or DHCP commands: 1
```

ucse subslot status

To display configuration information related to the hardware and software on the server module, use the **ucse subslot status** command in privileged EXEC mode.

ucse subslot *slot*/*port-adapter* **status [detailed]**

Syntax Description

slot/	Number of the router slot in which the server module is installed.
port-adapter	Number of the port adapter. **Note** For Cisco UCS E-Series Servers, the port adapter number is 0.
detailed	(Optional) Displays detailed information about the server module, such as its status and settings of the reset and heartbeat-reset flags.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

The following example shows how to display server status:

```
Router#  ucse subslot 1/0 status
CPU info
        Name         Cores    Version
        ------------ -------- --------------------------------------------------
        CPU1         4        Intel(R) Xeon(R) CPU E5-2418L 0 @ 2.00GHz

Memory info
        Name                 Capacity        Channel Speed (MHz) Channel Type
        -------------------- --------------- ------------------- ---------------
        Node0_Dimm0          Not Installed   Unknown             Unknown
        Node0_Dimm1          16384 MB        1333                DDR3
        Node0_Dimm2          8192 MB         1333                DDR3

Hard drive info
        Slot Number Controller Status                 Manufacturer   Model          Drive
Firmware Coerced Size   Type  SED
        ----------- ---------- ---------------------- -------------- --------------
-------------- -------------- ----- -----
        1           SLOT-5     online                 ATA            ST91000640NS   CC02
         952720 MB      HDD   false
        2           SLOT-5     online                 ATA            ST91000640NS   CC02
         952720 MB      HDD   false
        3           SLOT-5     online                 ATA            ST91000640NS   CC02
         952720 MB      HDD   false

Virtual drive info
        Virtual Drive  Status               Name                     Size       RAID Level

        -------------- -------------------- ------------------------ ---------- ----------

        0              Optimal                                       1905440 MB RAID 5


PCI card info
        Name                 Slot       Vendor ID            Device ID            Product
Name
        -------------------- ---------- -------------------- --------------------
-------------------------
        PCIe Adapter1        0          0xe414               0x5716               Broadcom
 5719 1 Gbps 4...
       PCIe Adapter2        2          0x0010              0x7300              LSI 9240-8i
 MegaRAID S...

Network Setting
            IPv4 Address: 10.1.1.2
            IPv4 Netmask: 255.255.255.0
            IPv4 Gateway: 10.1.1.1

            NIC Mode: shared_lom
            NIC Redundancy: none
            NIC Interface: ge1
```

INDEX