Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine

First Published: 2019-10-04

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

CONTENTS

Preface

This preface includes the following sections:

New and Changed Information

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

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

Chapter	Title	Description
Chapter 1	Quick Start Basic Configuration	Provides a list of commands and steps to quickly set up and use the E-Series Server and NCE.

Chapter	Title	Description
Chapter 2	Overview	Provides an overview of the product, hardware and software requirements, and E-Series Server and NCE options.
Chapter 3	Installing the E-Series Server or NCE into the Router	Describes how to install the E-Series Server or NCE into the router.
Chapter 4	Configuring Access to the Management Firmware	Provides options to configure CIMC access.
Chapter 5	Accessing the Management Firmware	Provides an overview of CIMC and describes how to log in to CIMC.
Chapter 6	Managing Storage Using RAID	Describes RAID options and how to configure RAID. **Note** The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.
Chapter 7	Installing the Operating System	Describes how to install the operating system.
Chapter 8	Configuring a Connection Between the Router and the E-Series Server or NCE	Describes how to configure a connection between the router and the E-Series Server or NCE.
Chapter 9	Upgrading Firmware	Provides options for upgrading firmware.
Appendix A	Configuration Differences	
Appendix B	Cisco IOS Software Command Reference—Cisco ISR G2	Provides a list of Cisco IOS commands used to configure the Cisco ISR G2 and the E-Series Server or NCE.
Appendix C	Cisco IOS Software Command Reference—Cisco ISR 4000 series	Provides a list of Cisco IOS commands used to configure the Cisco ISR 4000 series 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 that 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**. Arguments 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.

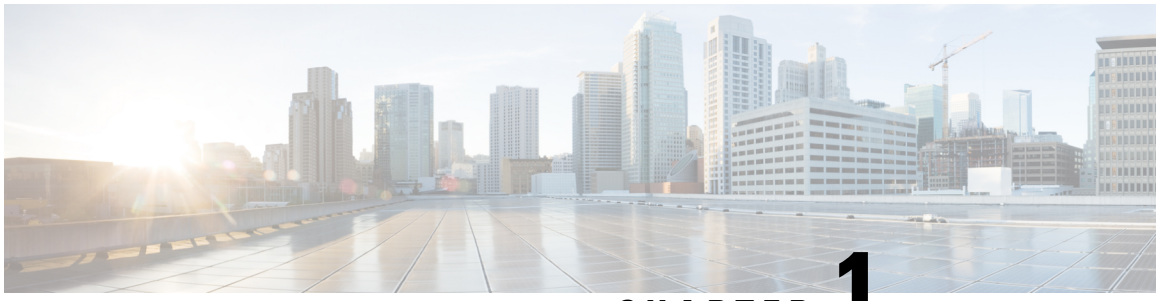
SAVE THESE INSTRUCTIONS

Related Documentation

The Documentation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine provides links to all product documentation.

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

Quick Start Basic Configuration

Note

- Use this "Quick Start Basic Configuration" 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) or the Cisco UCS E-Series Network Compute Engine (NCE).
- For detailed instructions, use subsequent chapters.

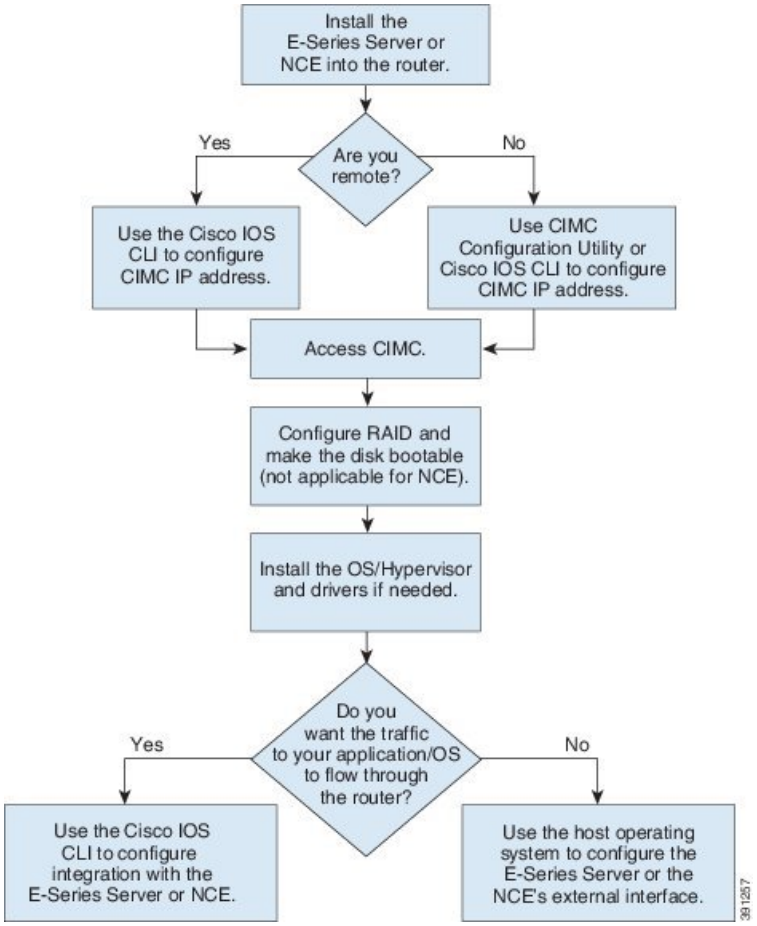
Use this quick start basic configuration chapter if you purchased Option 1 (E-Series Server or NCE without a preinstalled operating system or hypervisor). Some of the configuration steps are different if you purchased Option 2 (E-Series Server or NCE with a preinstalled Microsoft Windows Server), or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

This chapter includes the following sections:

Quick Start Basic Configuration Tasks

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

Figure 1: Basic Workflow—Option 1



Note The CIMC Configuration Utility is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Procedure

Step 1 Install the E-Series Server or NCE 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. This basic configuration shows you how to configure CIMC access using the server's external GE2 interface:

  a. enable

b. **configure terminal**

c. Use one of the following as appropriate:

- **interface ucse** *slot*/*port*—Use for all E-Series Servers or SM E-Series NCE installed in a Cisco ISR G2 or Cisco ISR 4000 series.
- **interface ucse 0**/*subslot*/*port*—Use for an EHWIC E-Series NCE installed in a Cisco ISR G2.
- **interface ucse** *slot*/*subslot*/*port*—Use for a NIM E-Series NCE installed in a Cisco ISR 4000 series.
- **ucse subslot** *slot*/*subslot*—Use for all E-Series Servers and NCEs installed in a Cisco ISR G2 or Cisco ISR 4000 series.

d. **imc ip address** *cimc-ip-address subnet-mask* **default-gateway** *cimc-gateway-ip-address*

e. **imc access-port shared-lom ge2**

f. **no shut**—Not applicable for an E-Series Server installed in a Cisco ISR 4000 series.

g. **end**

Note For detail configuration, see one of the following topics as appropriate:

- Configuring CIMC Access Using the E-Series Server's External GE2 or GE3 Interface—Cisco ISR G2, on page 35
- Configuring CIMC Access Using the E-Series Server's External GE2 or GE3 Interface—Cisco ISR 4000 Series, on page 48
- Configuring CIMC Access Using the EHWIC E-Series NCE's External GE2 Interface, on page 57
- Configuring CIMC Access Using the NIM E-Series NCE's External GE2 Interface—Cisco ISR 4000 Series, on page 68

To use another interface, see Configuring Access to the Management Firmware , on page 23.

- 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 70.

    Note The CIMC Configuration Utility is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

  - Use the Cisco IOS CLI to configure CIMC access (see the configuration for a remote user above).

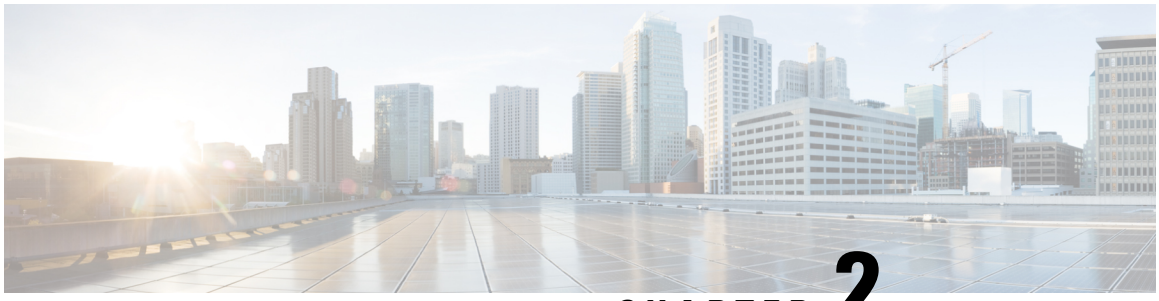
Step 3 In your web browser, enter the IP address that you configured in Step 2 to access CIMC.

Step 4 Configure RAID and make the disk drive bootable. See Managing Storage Using RAID , on page 79.

Step 5 Install the operating system or hypervisor and if needed, install drivers. See Installing the Operating System or Hypervisor, on page 93.

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 or the NCE's external GE2 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 or NCE. See Configuring a Connection Between the Router and the E-Series Server or NCE, on page 115.



CHAPTER 2

Overview

This chapter includes the following sections:

Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Overview

The Cisco UCS E-Series M6 Servers are size-,weight-, and power-efficient blade servers that are housed within the Cisco Catalyst 8300 Series Edge platforms. These servers provide a general-purpose compute platform for branch-office applications deployed either as bare-metal on operating systems, such as Linux, or as virtual machines on hypervisors, such as VMware vSphere Hypervisor.

The UCS E-Series M6 Server is purpose-built with powerful Intel IceLake-D processors for general purpose compute. It comes in the double-wide form factor, that fits into two SM slots.

Note Forinformation about the E-Series M6 Servers,and the maximum number of servers that can be installed per router, see the "Hardware Requirements" section in the *Hardware Installation Guide for Cisco UCS E-Series M6 Servers*.

Server Software

The UCS E-Series M6 Servers require three major software systems:

- CIMC firmware
- BIOS firmware
- Operating system or hypervisor

CIMC Firmware

Cisco Integrated Management Controller (CIMC) is a separate management module built into the motherboard ofthe E-Series M6 Servers. A dedicated 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 M6 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 manageabilityfeatures allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, and manage firmware.

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

Operating System or Hypervisor

Themain server CPU runs on an operating system, such as Linux; or on a hypervisor. You can purchase an E-Series M6 Servers with a preinstalled hypervisor.

Note For information about the platforms that are available on the E-Series M6 Servers, see the "Software Requirements" section in the *Release Notes for Cisco UCS E-Series M6 Servers.*

Managing E-Series Servers and the NCE

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

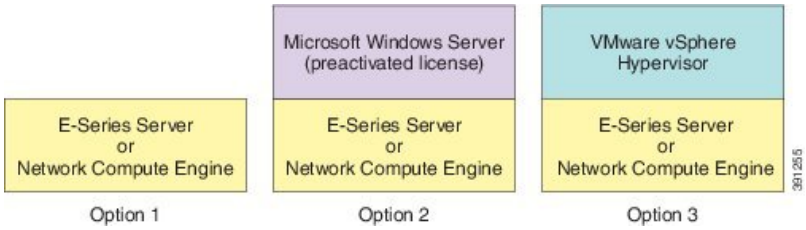
Table 1: E-Series Server and NCE Management Interfaces

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

E-Series Server and NCE Options

The following figure shows the E-Series Server and NCE options.

Figure 2: E-Series Server or NCE Options



- Option 1—E-Series Server or NCE without a preinstalled operating system or hypervisor
- Option 2—E-Series Server or NCE 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 or NCE 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.

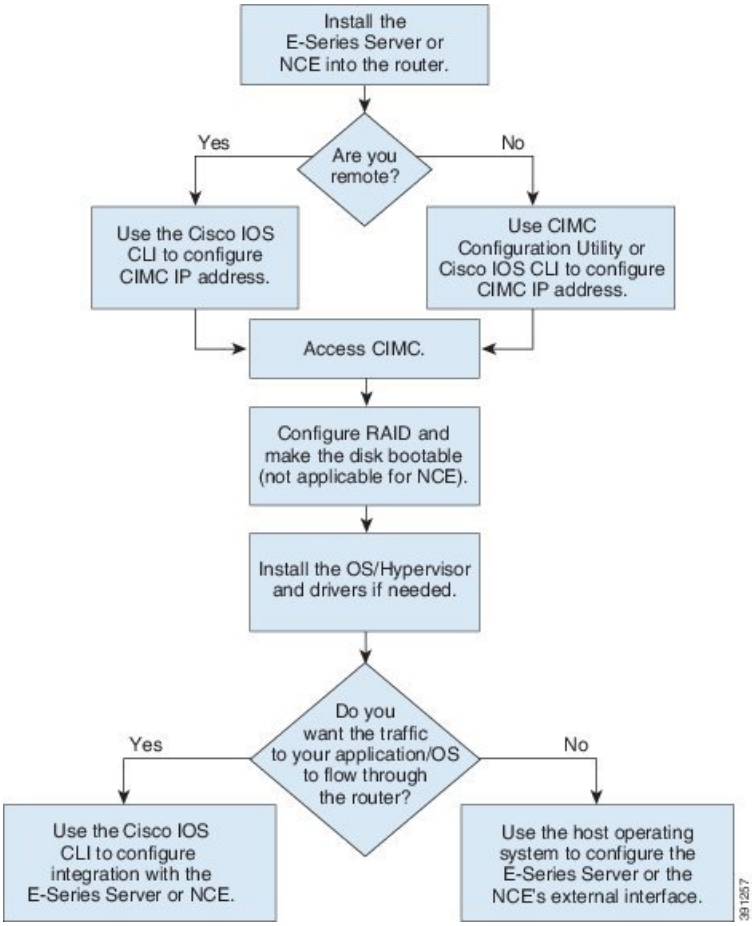
Note The default username for the preinstalled VMware vSphere Hypervisor is **root**, which cannot be changed, and the default password is **password**. After you log in, we recommend that you change the password.

Important The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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

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

Figure 3: Basic Workflow—Option 1



Note The CIMC Configuration Utility is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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

Procedure

	Command or Action	Purpose
Step 1	Install the E-Series Server or NCE into the router.	See Installing the E-Series Server or NCE into the Router, on page 13.

	Command or Action	Purpose
Step 2	Configure the CIMC IP address for CIMC access.	See Configuring Access to the Management Firmware , on page 23.
Step 3	Access CIMC.	See Accessing the Management Firmware, on page 75.
Step 4	Configure RAID and make the disk drive bootable.	See Managing Storage Using RAID , on page 79. **Important** The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.
Step 5	Install the operating system, and if needed, install the drivers.	See Installing the Operating System or Hypervisor, on page 93.
Step 6	Configure an internal connection between the router and the E-Series Server or NCE.	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 or NCE's external 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 or NCE. See Configuring a Connection Between the Router and the E-Series Server or NCE, on page 115.

Basic Workflow for Option 2—E-Series Server or NCE 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 or NCE with a preinstalled Microsoft Windows Server.

Procedure

	Command or Action	Purpose
Step 1	Install the E-Series Server or NCE into the router.	See Installing the E-Series Server or NCE into the Router, on page 13.
Step 2	Configure the CIMC IP address for CIMC access.	See Configuring Access to the Management Firmware , on page 23.
Step 3	Configure an internal connection between the router and the E-Series Server or NCE.	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 or NCE's external 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 or NCE. See Configuring a Connection Between the Router and the E-Series Server or NCE, on page 115.
Step 4	Access CIMC, and then access the Microsoft Windows Server from CIMC.	See Accessing the Management Firmware, on page 75.

Basic Workflow for Option 3—E-Series Server or NCE 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 or NCE with a preinstalled VMware vSphere Hypervisor.

Procedure

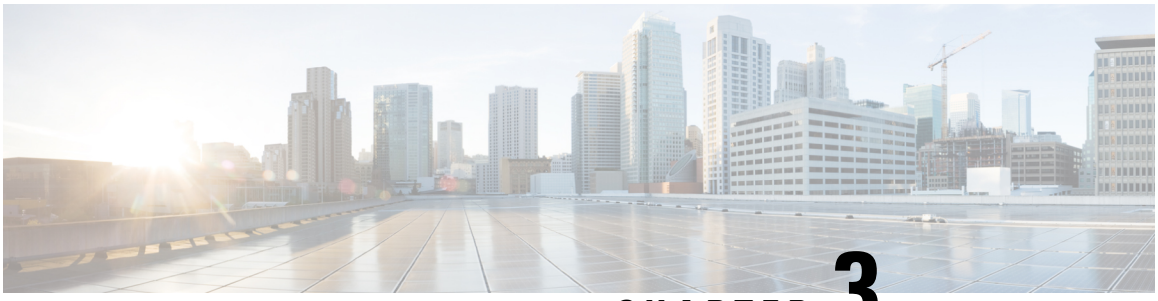
	Command or Action	Purpose
Step 1	Install the E-Series Server or NCE into the router.	See Installing the E-Series Server or NCE into the Router, on page 13.
Step 2	Configure the CIMC IP address for CIMC access.	See Configuring Access to the Management Firmware , on page 23.
Step 3	Configure an internal connection between the router and the E-Series Server or NCE.	Depending on whether you want the traffic to flow through the router or not, do one of the following:

	Command or Action	Purpose
		• 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 or NCE's external 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 or NCE. See Configuring a Connection Between the Router and the E-Series Server or NCE, on page 115.
Step 4	Access CIMC, and then access the VMware vSphere Hypervisor from CIMC.	See Accessing the Management Firmware, on page 75.

Common Terms Used in This Guide

Table 2: Common Terms

Term	Description
BMC	Board Management Controller. BMC is used in the Cisco IOS commands to configure CIMC.
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.
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 or NCE into the Router

This chapter includes the following sections:

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

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

Important If you are migrating the E-Series Server from a Cisco ISR G2 into a Cisco ISR 4000 series, 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 Cisco ISR G2—and then migrate it into the Cisco ISR 4000 series. For CIMC firmware installation instructions, see the "CIMC Firmware Management" chapter in the *GUI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine* on Cisco.com.

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

Verifying Compatibility

Verifying the Cisco ISR G2, E-Series Server, NCE, and Cisco IOS Software Release Compatibility

Table 3: Router, E-Series Server, NCE, and Cisco IOS Release Compatibility

Router	Cisco IOS Software Release for Single-Wide E-Series Servers and the SM E-Series NCE	Cisco IOS Software Release for Double-Wide E-Series Servers	Cisco IOS Software Release for the EHWIC E-Series NCE
1921	—	—	15.4(3)M and later releases
1941	—	—	15.4(3)M and later releases
2911	15.2(4)M and later releases	—	15.4(3)M and later releases
2921	15.2(4)M and later releases	15.2(4)M and later releases	15.4(3)M and later releases
2951	15.2(4)M and later releases	15.2(4)M and later releases	15.4(3)M and later releases
3925	15.2(4)M and later releases	15.2(4)M and later releases	15.4(3)M and later releases
3925e	15.2(4)M and later releases	15.2(4)M and later releases	15.4(3)M and later releases
3945	15.2(4)M and later releases	15.2(4)M and later releases	15.4(3)M and later releases
3945e	15.2(4)M and later releases	15.2(4)M and later releases	15.4(3)M and later releases

Verifying the Cisco ISR 4000 Series, E-Series Server, NIM, CIMC, and Cisco IOS Software Release Compatibility

Table 4: Cisco ISR 4000 Series, E-Series Server, NIM, CIMC, and Cisco IOS Release Compatibility

Router	Cisco IOS Software Release for Single-Wide E-Series Servers and the SM E-Series NCE	Cisco IOS Software Release for Double-Wide E-Series Servers	Cisco IOS Software Release for NIM E-Series NCE	CIMC
4400 Series	XE 3.12S	XE 3.12S	_	2.2.2 and later releases
	XE 3.13S and later releases	XE 3.13S and later releases	_	2.3.1 and later releases
	_	_	XE 3.15S and later releases	3.0.1 and later releases
	XE 16.2.1 [1]	XE 16.2.1	XE 16.2.1	3.0.1 and later releases
4300 Series	XE 3.13S and later releases	XE 3.13S and later releases	_	2.3.1 and later releases
	_	_	XE 3.15S and later releases	3.0.1 and later releases
	XE 16.2.1	XE 16.2.1	XE 16.2.1	3.0.1 and later releases

[1] Do not downgrade the release version from XE 16.2.1. If you downgrade the release version from XE 16.2.1, the UCS-E module will not come up due to CSCux77048. To bring the UCS-E module up, do an OIR using the **hw-module subslot x/y reload** command.

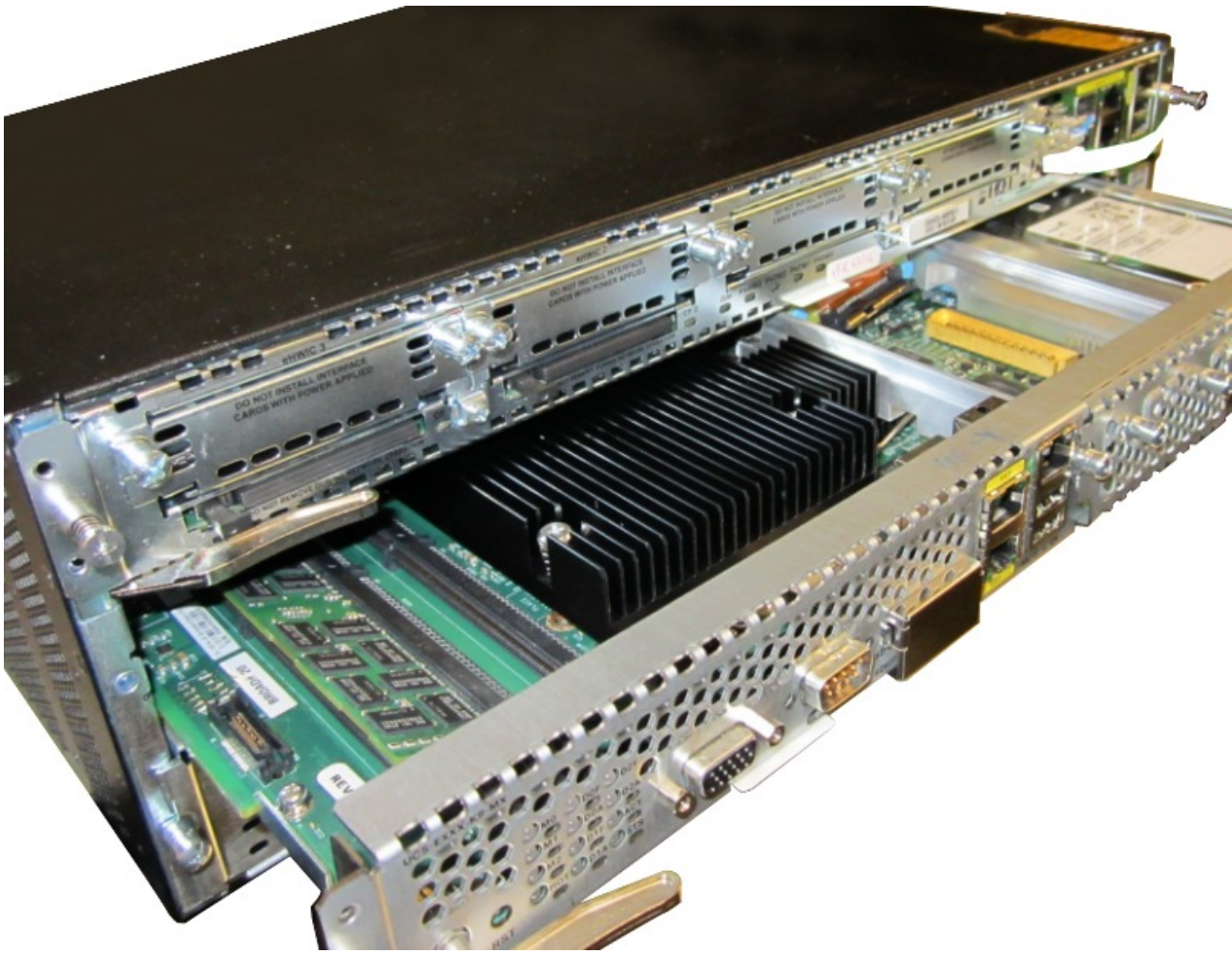
Installing the E-Series Server and the NCE into a Router

The following figures show how to install the E-Series Server and the EHWIC E-Series NCE into a router. For detailed information, see the *Hardware Installation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine* on Cisco.com.

Double-Wide E-Series Server in a Cisco 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 server.

Figure 4: Double-Wide E-Series Server in a Cisco ISR G2



Double-Wide E-Series Server in a Cisco ISR 4000 Series

Important If you are migrating the E-Series Server from a Cisco ISR G2 into a Cisco ISR 4000 series, you must first upgrade the CIMC and the BIOS firmware image to the latest version—while the E-Series Server is still installed in the Cisco ISR G2—and then migrate it into the Cisco ISR 4000 series. We strongly recommend that you upgrade both the CIMC and the BIOS firmware images.

You can use either the Cisco Host Upgrade Utility (HUU) to upgrade the firmware components or you can upgrade the firmware components manually. For firmware upgrade information, see Upgrading Firmware, on page 139 .

If you migrate the E-Series Server into the Cisco ISR 4000 series without first updating the CIMC firmware, the E-Series Server might continuously reset. To stop the reset and install the firmware, see Stopping the E-Series Server from Resetting and Updating the CIMC Firmware—Cisco ISR 4000 Series, on page 21.

Figure 5: Double-Wide E-Series Server in a Cisco ISR 4000 series

EHWIC E-Series NCE in a Cisco ISR G2

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

Figure 6: EHWIC E-Series NCE in a Cisco ISR G2

NIM E-Series NCE in a Cisco ISR 4000 Series

Figure 7: NIM E-Series NCE in a Cisco ISR 4000 Series

Verifying Installation

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:

Procedure

- 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
```

Verifying the EHWIC E-Series NCE Installation

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Router> **show inventory**	Verifies that the router detects the presence of the newly installed EHWIC E-Series NCE.

Example

```
Router> show inventory

NAME: "CISCO3945-CHASSIS", DESCR: "CISCO3945-CHASSIS"
PID: CISCO3945-CHASSIS , VID: V02, SN: FGL1539100Q

NAME: "Cisco Services Performance Engine 150 for Cisco 3900 ISR on Slot 0", DESCR: "Cisco
Services Performance Engine 150 for Cisco 3900 ISR"
PID: C3900-SPE150/K9   , VID: V05 , SN: FOC15367HAZ

NAME: "Enhanced WAN Interface Card UCS Server on Slot 0 SubSlot 3", DESCR: "Enhanced WAN
```

```
Interface Card UCS Server"
PID: UCS-EN120E-M2/K9  , VID: V01, SN: FOC17462K2A

NAME: "C3900 AC Power Supply 1", DESCR: "C3900 AC Power Supply 1"
PID: PWR-3900-AC       , VID: V03, SN: SNI1511C8SM
```

Verifying NIM E-Series NCE Installation

Before You Begin

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

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

Procedure

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

```
Router# show platform
Chassis type: ISR4351/K9

0/1       UCS-EN140N-M2/K9    ok                  3w5d
1/0       UCS-E140DP-M1/K9    ok                  4w6d
2         ISR4351/K9          ok                  5w2d
R0        ISR4351/K9          ok, active          5w2d
F0        ISR4351/K9          ok, active          5w2d
P0        PWR-4450-AC         ok                  5w2d
P2        ACS-4450-FANASSY    ok                  5w2d

Slot      CPLD Version        Firmware Version
--------- ------------------- ------------------------------------
0         14080523            15.4(3r)S1
1         14080523            15.4(3r)S1
2         14080523            15.4(3r)S1
R0        14080523            15.4(3r)S1
F0        14080523            15.4(3r)S1
```

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

```
Router# show hw-module subslot all oir
Module        Model               Operational Status
------------- ------------------- ------------------------
subslot 0/0   ISR4351-3x1GE       ok
subslot 0/1   UCS-EN140N-M2/K9     ok
subslot 1/0   UCS-E140DP-M1/K9    ok
```

Stopping the E-Series Server from Resetting and Updating the CIMC Firmware—Cisco ISR 4000 Series

If you migrate the E-Series Server into the Cisco ISR 4000 series 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.

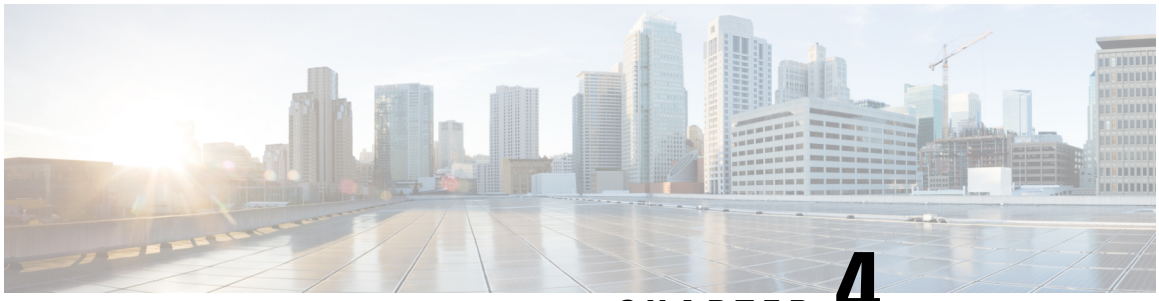
Procedure

	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.
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	Press **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.

	Command or Action	Purpose
Step 10	Router# **hw-module subslot** *slot/subslot* **reload**	Reloads the E-Series Server. **Note** This reload power-cycles the E-Series Server.

What to Do Next

Configure the CIMC IP address for CIMC access. See Configuring Access to the Management Firmware , on page 23.



CHAPTER 4

Configuring Access to the Management Firmware

This chapter provides an overview of the E-Series Server and NCE interfaces and provides procedures to configure access to the CIMC management firmware when the E-Series Server or NCE is installed in the router. It contains the following sections:

Configuring CIMC Access

If you are a remote user, use the Cisco IOS CLI to configure CIMC access.

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.

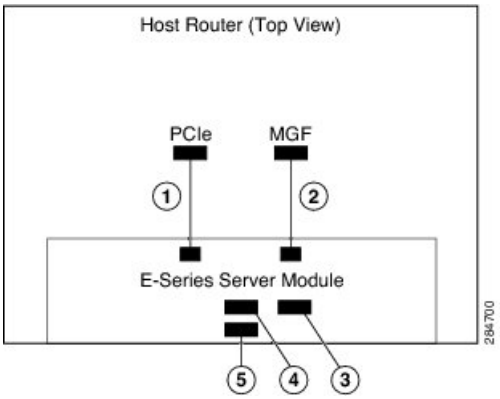
Note The CIMC Configuration Utility is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

- Use the Cisco IOS CLI to configure CIMC access. See one of the following as appropriate:
  - CIMC Access Configuration Options—Cisco ISR G2, on page 25
  - CIMC Access Configuration Options—Cisco ISR 4000 Series, on page 38
  - CIMC Access Configuration Options—EHWIC E-Series NCE, on page 51
  - CIMC Access Configuration Options—NIM E-Series NCE, on page 60

Understanding the Interfaces in an E-Series Server and the Cisco ISR G2

The following figure shows the interfaces in a double-wide E-Series Server and the Cisco 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—Cisco ISR G2

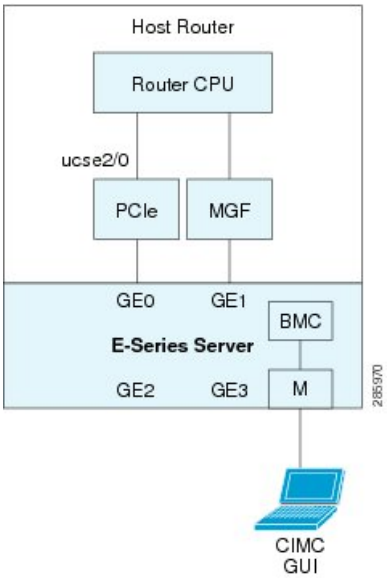
Depending on whether you are a remote user or a local user, do one of the following to configure CIMC access.

- 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—Cisco 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 or subslot and port number of the E-Series Server or NCE.

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 dedicated**	Configures CIMC access through the server's external Management (dedicated) interface. See # 3 in Understanding the Interfaces in an E-Series Server and the Cisco ISR G2.
Step 6	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 7	Router (config-if)# **end**	Exits interface configuration mode.

Example

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
```

Configuring CIMC Access Using Shared LOM—Cisco ISR G2

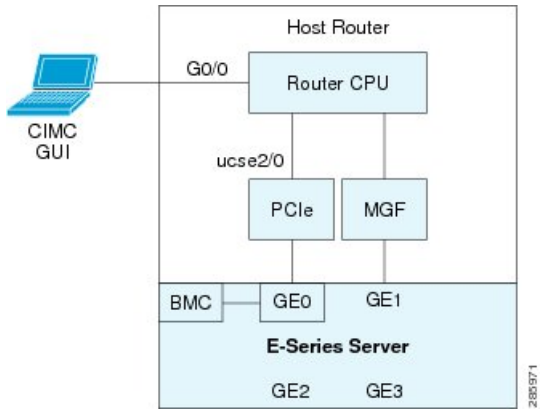
Use one of the following shared LOM interfaces to configure CIMC access:

- 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—Cisco 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 or subslot and port number of the E-Series Server or NCE.

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 interface 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

	Command or Action	Purpose
		Understanding the Interfaces in an E-Series Server and the Cisco ISR G2.
Step 12	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 13	Router (config-if)# **end**	Exits interface 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. • *slot/port*—Slot and port where the E-Series Server is installed.
Step 16	Router (config-if)# **end**	Exits interface 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.

Example

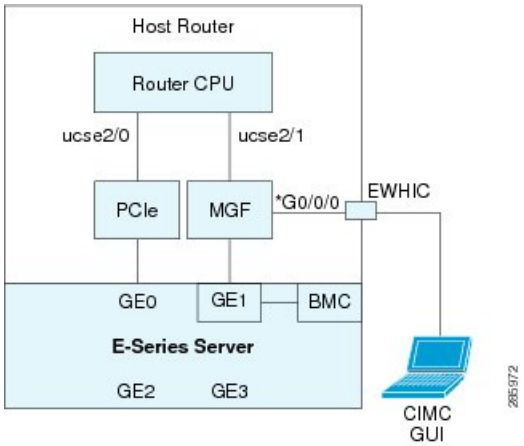
This example shows how to configure CIMC access using the server's internal PCIe *slot*/**0** console interface:

```
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
```

Configuring CIMC Access Using the Router's Internal MGF slot/1 VLAN Interface—Cisco 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



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 or subslot and port number of the E-Series Server or NCE.

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.
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.

	Command or Action	Purpose
Step 6	Router (config-if)# **end**	Exits interface 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 Understanding the Interfaces in an E-Series Server and the Cisco ISR G2.
Step 11	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 12	Router (config-if)# **end**	Exits interface 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.

Example

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

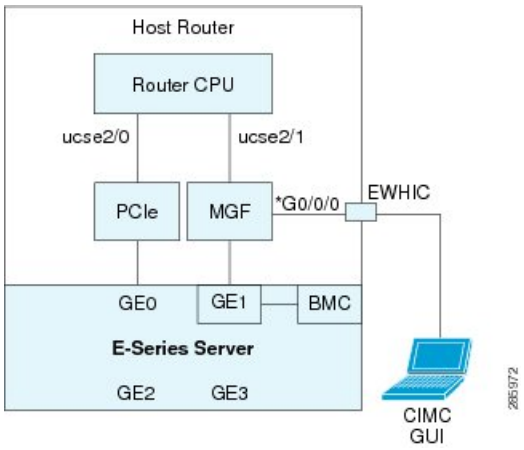
```
Router> enable
Router> password
Router> show vlan-switch
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0/0, Gi0/0/1, Gi0/0/2
                                                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
```

Configuring CIMC Access Using the Router's Internal MGF slot/1 Interface Using a Non-Native VLAN—Cisco ISR G2

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

Figure 12: Configuring CIMC Access Using the Router's Internal MGF slot/1 Interface Using a Non-Native VLAN



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 or subslot and port number of the E-Series Server or NCE.

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)# **vlan** *vlan-number*	Configures the specified VLAN.
Step 5	Router (config)# **end**	Exits VLAN configuration.
Step 6	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 7	Router (config)# **interface vlan** *vlan-number*	Enters VLAN configuration mode for the specified VLAN number.
Step 8	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 9	Router (config-if)# **end**	Exits interface configuration mode.
Step 10	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 11	Router (config)# **interface ucse** *slot/port*	Enters interface configuration mode for the slot and port where the E-Series Server is installed.
Step 12	Router (config)# **imc vlan** *vlan-id*	Configures the specified VLAN ID for CIMC.
Step 13	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 14	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 Understanding the Interfaces in an E-Series Server and the Cisco ISR G2.
Step 15	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 16	Router (config-if)# **end**	Exits interface configuration mode.
Step 17	Router# **configure terminal**	Enters global configuration mode on the host router.

	Command or Action	Purpose
Step 18	Router (config)# **interface ucse** *slot*/**1**	Enters interface configuration mode for the router's MGF *slot*/**1** VLAN interface.
Step 19	Router (config-if)# **switchport mode trunk**	Puts the port into permanent trunking mode. The default configuration is access mode.
Step 20	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 21	Router (config-if)# **end**	Exits interface configuration mode.
Step 22	Router# **ping** *cimc-ip-address*	Verifies connection from the router to CIMC through the router's internal MGF *slot*/**1** VLAN interface.

Example

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

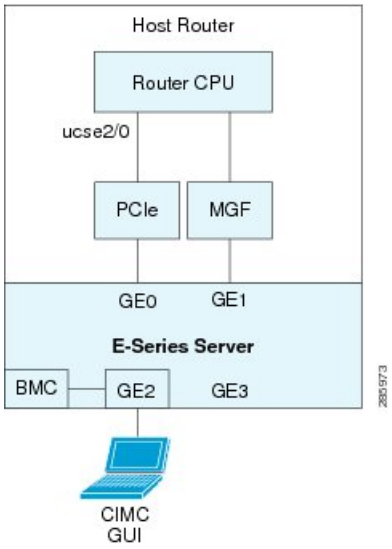
```
Router> enable
Router> password
Router> show vlan-switch
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0/0, Gi0/0/1, Gi0/0/2
                                                Gi0/0/3, uc2/1

Router# configure terminal
Router(config)# vlan 2
Router(config)# end

Router# configure terminal
Router(config)# interface vlan 2
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 vlan 2
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# configure terminal
Router(config)# interface ucse 2/1
Router(config-if)# switchport mode trunk
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
```

Configuring CIMC Access Using the E-Series Server's External GE2 or GE3 Interface—Cisco 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 13: 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 or subslot and port number of the E-Series Server or NCE.

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.

	Command or Action	Purpose
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 the E-Series Server's external GE2 or GE3 interface. See # 4 and 5 in Understanding the Interfaces in an E-Series Server and the Cisco ISR G2.
Step 6	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 7	Router (config-if)# **end**	Exits interface configuration mode.

Example

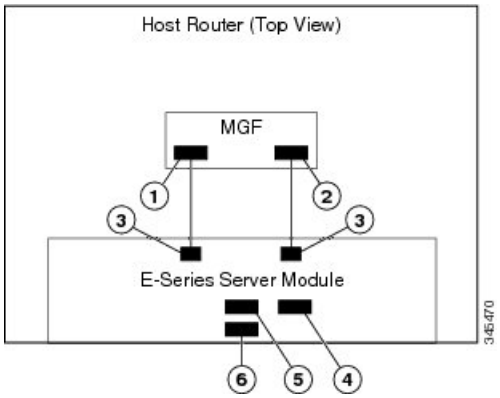
This example shows how to configure CIMC access using the server's external GE2 interface:

```
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
```

Understanding the Interfaces in an E-Series Server and the Cisco ISR 4000 Series

The following figure shows the interfaces in a double-wide E-Series Server and the Cisco ISR 4000 series host router.

Figure 14: 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 4000 Series

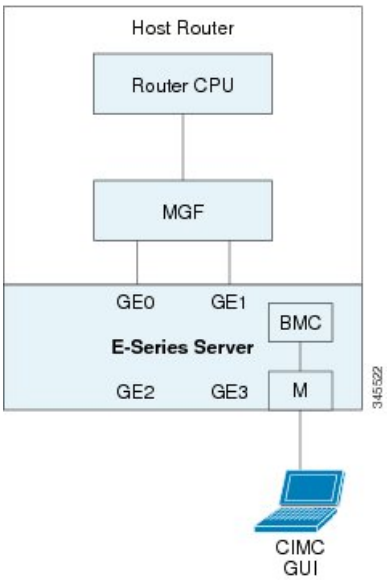
Depending on whether you are a remote user or a local user, do one of the following to configure CIMC access.

- 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 4000 Series

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

Figure 15: 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 or subslot and port number of the E-Series Server or NCE.

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/subslot*	Enters ucse interface configuration mode for the slot and subslot 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.

	Command or Action	Purpose
		• *cimc-gateway-ip-address*—IP address for the default gateway.
Step 5	Enter one of the following commands: • Router (config-ucse)# **imc access-port mgmt** • Router (config-ucse)# **imc access-port dedicated**	Configures CIMC access through the server's external Management (dedicated) interface. See # 4 in Understanding the Interfaces in the NIM E-Series NCE and the Cisco ISR 4000 Series, on page 59. • 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.

Example

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
```

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
```

Configuring CIMC Access Using the E-Series Server's NIC Interfaces—Cisco ISR 4000 Series

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

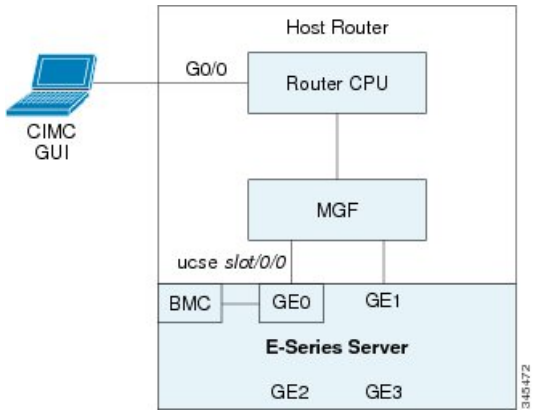
- E-Series Server's internal GE0 and the router's **ucse** *slot*/**0/0** interface

- 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 4000 Series 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 16: 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 or subslot and port number of the E-Series Server or NCE.

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.

	Command or Action	Purpose
Step 7	Router (config)# **interface ucse** *slot*/**0/0**	Enters ucse interface configuration mode for the slot, subslot, and port 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*/*subslot*	Enters ucse interface configuration mode for the slot and subslot 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.

	Command or Action	Purpose
Step 13	Enter one of the following commands: • Router (config-ucse)# **imc access-port ge0** • 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 Understanding the Interfaces in an E-Series Server and the Cisco ISR 4000 Series, on page 36. • 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/subslot/port*	Creates a static route. • *cimc-ip-address*—IP address of CIMC. • *slot/subslot/port*—Slot, subslot, and port 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.

Example

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
```

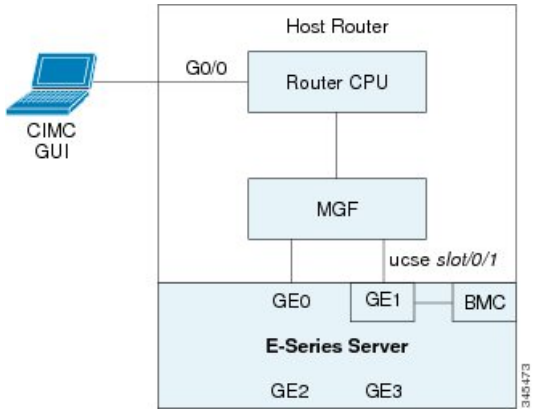
This example shows how to configure CIMC access using the E-Series Server's internal console interface and the router's ucse *slot*/**0/0** interface—Applicable with Cisco IOS XE Release 3.10S and later versions:

```
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
```

*Configuring CIMC Access Using the E-Series Server's Internal GE1 Interface and the Cisco ISR 4000 Series 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 17: 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 or subslot and port number of the E-Series Server or NCE.

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*/**0/1**	Enters ucse interface configuration mode for the slot, subslot, and port 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.

	Command or Action	Purpose
		• *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/subslot*	Enters ucse interface configuration mode for the slot and subslot 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	Enter one of the following commands: • Router (config-ucse)# **imc access-port ge1** • Router (config-ucse)# **imc access-port shared-lom ge1**	Configures CIMC access using the E-Series Server's internal GE1 interface. See # 3 in Understanding the Interfaces in an E-Series Server and the Cisco ISR 4000 Series, on page 36. • Use the **imc access-port ge1** command if you installed the Cisco IOS XE Release 3.9S.

	Command or Action	Purpose
		• Use the **imc access-port shared-lom ge1** 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/subslot/port*	Creates a static route. • *cimc-ip-address*—IP address of CIMC. • *slot/subslot/port*—Slot, subslot, and port 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.

Example

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
```

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:

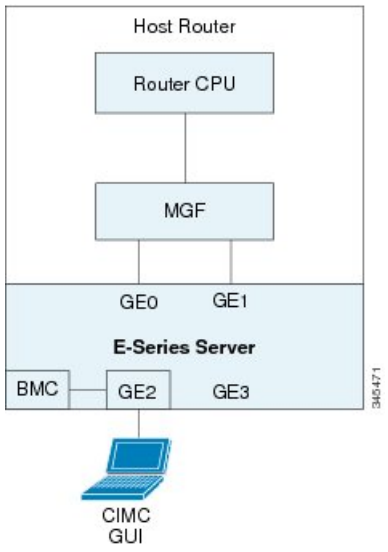
```
Router> enable
Router> password
Router# configure terminal

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
```

Configuring CIMC Access Using the E-Series Server's External GE2 or GE3 Interface—Cisco ISR 4000 Series

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 18: 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/subslot*	Enters ucse interface configuration mode for the slot and subslot 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** {**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 Understanding the Interfaces in an E-Series Server and the Cisco ISR 4000 Series, on page 36. • 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.

Example

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
```

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:

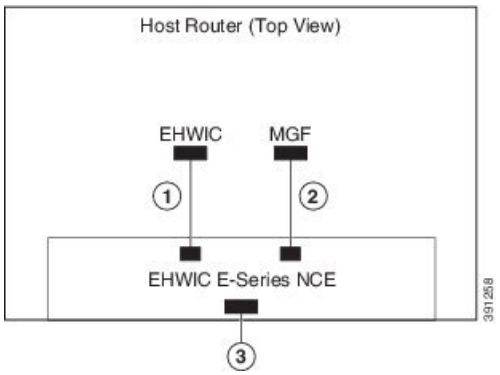
```
Router> enable
Router> password
Router# configure terminal

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
```

Understanding the Interfaces in the EHWIC E-Series NCE and the Cisco ISR G2

Note This section is applicable to the EHWIC E-Series NCE. This section is not applicable to the SM E-Series NCE.

The following figure shows the interfaces in the EHWIC E-Series NCE and the Cisco ISR G2 host router.

Figure 19: Interfaces in the EHWIC E-Series NCE and the Cisco ISR G2 Host Router



	Interface	Interface Location	Description
1	Router's EHWIC **0**/*subslot*/**0** Interface	Internal Interface	Also called Console interface. This interface connects the router's EHWIC interface to the EHWIC E-Series NCE. The EHWIC interface provides an internal Layer 3 GE link between the router and the EHWIC E-Series NCE. It can be used both for CIMC configuration and for host operating system configuration.
2	Router's MGF **0**/*subslot*/**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 EHWIC E-Series NCE. This interface can be used both for CIMC configuration and for host operating system configuration. **Note** This interface is not applicable to the Cisco 1921 ISR G2.
3	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—EHWIC E-Series NCE

Do one of the following to configure CIMC access.

- Use one of the following shared LOM interfaces to configure CIMC access:
  - Router's internal EHWIC **0**/*subslot*/**0** Console interface
  - Router's internal MGF **0**/*subslot*/**1** VLAN interface

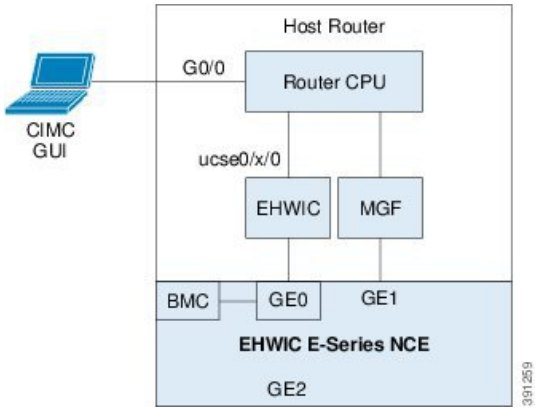
Note This interface is not applicable to the Cisco ISR 1921.

  - NCE's external GE2 interface
- Use the Cisco IOS CLI to configure CIMC access.

Configuring CIMC Access Using the Router's Internal EHWIC 0/subslot/0 Console Interface—EHWIC E-Series NCE

See the following figure and the procedure that follows to configure CIMC access using the router's internal EHWIC **0**/*subslot*/**0** console interface.

Figure 20: Configuring CIMC Access Using the Router's Internal EHWIC 0/subslot/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 or subslot and port number of the E-Series Server or NCE.

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.
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **end**	Exits interface configuration mode.
Step 7	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 8	Router (config)# **interface ucse 0**/*subslot*/*port*	Enters interface configuration mode for the subslot and port where the NCE 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.

	Command or Action	Purpose
		• *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 EHWIC **0**/*slot*/**0** (console) interface. See # 1 in Understanding the Interfaces in the EHWIC E-Series NCE and the Cisco ISR G2, on page 50.
Step 12	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 13	Router (config-if)# **end**	Exits interface 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 0**/*subslot*/*port*	Creates a static route. • *cimc-ip-address*—IP address of CIMC. • *subslot/port*—Subslot and port where the NCE is installed.

	Command or Action	Purpose
Step 16	Router (config-if)# **end**	Exits interface configuration mode.
Step 17	Router# **ping** *cimc-ip-address*	Verifies connection from the router to CIMC through the router's internal EHWIC **0**/*subslot*/**0** console interface.

Example

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

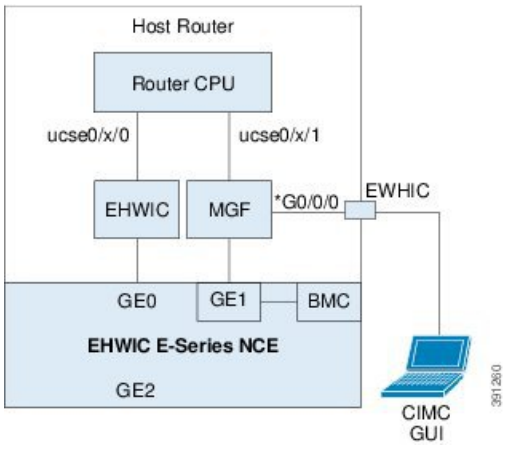
```
Router> enable
Router> password
Router# configure terminal

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 0/3/0
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 0/3/0
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
```

Configuring CIMC Access Using the Router's Internal MGF 0/subslot/1 VLAN Interface—EHWIC E-Series NCE

Important This procedure is not applicable to the Cisco 1921 ISR G2.

See the following figure and the procedure that follows to configure CIMC access using the router's internal MGF **0**/*subslot*/**1** VLAN interface.

Figure 21: Configuring CIMC Access Using the Router's Internal MGF 0/subslot/1 VLAN 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 or subslot and port number of the E-Series Server or NCE.

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.
Step 4	Router (config)# **interface vlan** *vlan-number*	Enters interface 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 interface configuration mode.
Step 7	Router# **configure terminal**	Enters global configuration mode on the host router.

	Command or Action	Purpose
Step 8	Router (config)# **interface ucse 0/***subslot***/0**	Enters ucse interface configuration mode for the subslot and port where the NCE 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 **0/***subslot***/1** MGF VLAN interface. See # 2 in Understanding the Interfaces in the EHWIC E-Series NCE and the Cisco ISR G2, on page 50.
Step 11	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 12	Router (config-if)# **end**	Exits interface configuration mode.
Step 13	Router# **configure terminal**	Enters global configuration mode on the host router.
Step 14	Router (config)# **interface ucse 0/***subslot***/1**	Enters ucse interface configuration mode for the subslot and port where the NCE is installed.
Step 15	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 16	Router (config-if)# **end**	Exits interface configuration mode.
Step 17	Router# **ping** *cimc-ip-address*	Verifies connection from the router to CIMC through the router's internal MGF **0/***subslot***/1** VLAN interface.

Example

This example shows how to configure CIMC access using the router's internal MGF **0/***subslot***/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, uc0/3/1
```

```
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 0/3/0
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# configure terminal
Router(config)# interface ucse 0/3/1
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
```

Configuring CIMC Access Using the EHWIC E-Series NCE's External GE2 Interface

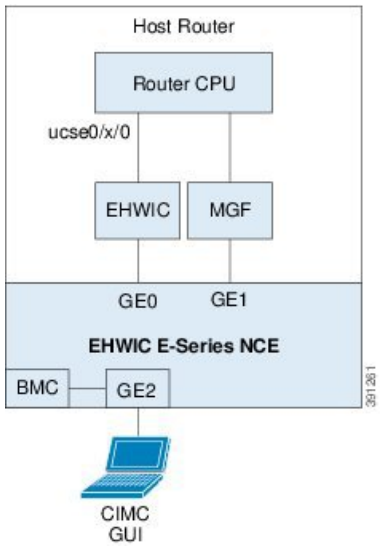
Important If you are using the external GE2 interface on an EHWIC E-Series NCE or the NIM E-Series NCE to configure CIMC access, to configure CIMC access, you might lose connectivity with CIMC during server reboot. This is expected behavior. If you must maintain connectivity with CIMC during a reboot, we recommend that you use one of the other network interfaces to configure CIMC access. See CIMC Access Configuration Options—EHWIC E-Series NCE, on page 51.

If you want to use the external GE2 interface to configure CIMC access, we recommend that you use the **spanning-tree portfast** command. For details, see the CSCup50049 caveat in the *Release Notes for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*

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

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

Figure 22: Configuring CIMC Access Using the EHWIC E-Series NCE'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 or subslot and port number of the E-Series Server or NCE.

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 0/***subslot/port*	Enters ucse interface configuration mode for the subslot and port where the NCE 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.

	Command or Action	Purpose
Step 5	Router (config-if)# **imc access-port shared-lom GE2**	Configures CIMC access through the EHWIC E-Series NCE's external GE2 interface. See # 3 in Understanding the Interfaces in the EHWIC E-Series NCE and the Cisco ISR G2, on page 50.
Step 6	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 7	Router (config-if)# **end**	Exits interface configuration mode.

Example

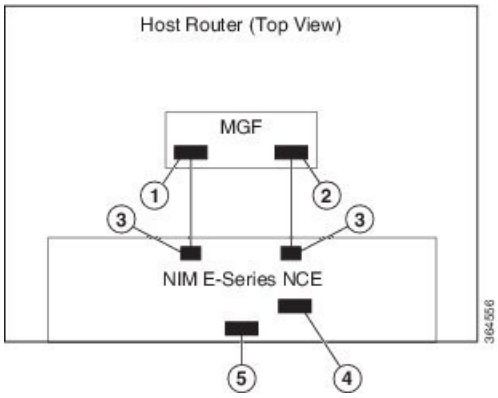
This example shows how to configure CIMC access using the EHWIC E-Series NCE external GE2 interface:

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

Router(config)# interface ucse 0/3/0
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
```

Understanding the Interfaces in the NIM E-Series NCE and the Cisco ISR 4000 Series

The following figure shows the interfaces in a NIM E-Series NCE and the Cisco ISR 4000 series host router.

Figure 23: Interfaces in a NIM E-Series NCE



	Interface	Interface Location	Description

1	Router's **ucse 0**/*subslot*/**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 NIM E-Series NCE. This interface can be used both for CIMC configuration and for host operating system configuration. **Note** This interface is used to access the NIM E-Series NCE's internal GE0 interface.
2	Router's **ucse 0**/*subslot*/**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 NIM E-Series NCE. This interface can be used both for CIMC configuration and for host operating system configuration. **Note** This interface is used to access the NIM E-Series NCE's internal GE1 interface.
3	GE0 and GE1 Interfaces	Internal Interfaces	NIM E-Series NCE's internal NIC interfaces.
4	Management (Dedicated) Interface	External Interface	Used for CIMC configuration and management.
5	GE2 Interface	External Interface	Can be used both for CIMC configuration and for host operating system configuration.

CIMC Access Configuration Options—NIM E-Series NCE

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

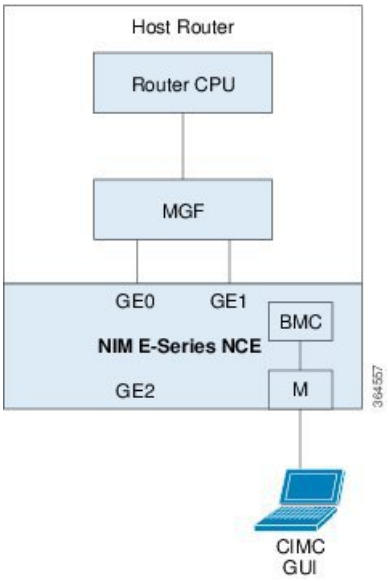
- If you are a remote user, use the Cisco IOS CLI to configure CIMC access by using one of the following interfaces:
  - CIMC Management (dedicated) interface
  - NIM E-Series NCE's internal GE0 and the router's ucse **0**/*subslot*/**0** interface
  - NIM E-Series NCE's internal GE1 interface and the router's ucse **0**/*subslot*/**1** interface
  - NIM E-Series NCE's external GE2 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 NIM E-Series NCE's External Management (Dedicated) Interface—Cisco ISR 4000 Series

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

Figure 24: Configuring CIMC Access Using the NIM E-Series NCE'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 or subslot and port number of the E-Series Server or NCE.

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/subslot*	Enters ucse interface configuration mode for the slot and subslot where the NIM E-Series NCE 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 dedicated**	Configures CIMC access through the server's external Management (dedicated) interface. See # 4 in Understanding the Interfaces in the NIM E-Series NCE and the Cisco ISR 4000 Series, on page 59.
Step 6	Router (config-ucse)# **end**	Returns to privileged EXEC mode on the host router.

Example

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

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

Router(config)# ucse subslot 0/1
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
```

Configuring CIMC Access Using the NIM E-Series NCE's NIC Interfaces—Cisco ISR 4000 Series

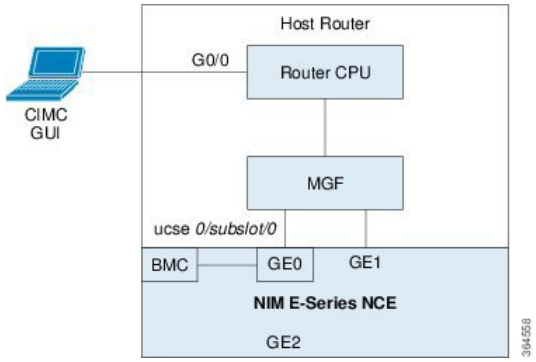
Use one of the following NIM E-Series NCE's NIC interfaces to access CIMC:

- NIM E-Series NCE's internal GE0 and the router's **ucse 0**/*subslot*/**0** Interface interface
- NIM E-Series NCE's internal GE1 interface and the router's **ucse 0**/*subslot*/**1** interface
- NIM E-Series NCE's external GE2 interface

Configuring CIMC Access Using the NIM E-Series NCE's Internal GE0 Interface and the Cisco ISR 4000 Series ucse 0/*subslot*/0 Interface

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

Figure 25: Configuring CIMC Access Using the NIM E-Series NCE's Internal GE0 Interface and the Router's ucse 0/subslot/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 or subslot and port number of the E-Series Server or NCE.

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 0/***subslot***/0**	Enters ucse interface configuration mode for the slot, subslot, and port where the NIM E-Series NCE 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.

	Command or Action	Purpose
		• *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/subslot*	Enters ucse interface configuration mode for the slot and subslot where the NIM E-Series NCE 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 shared-lom console**	Configures CIMC access using the NIM E-Series NCE's internal GE0 interface. See # 3 in Understanding the Interfaces in the NIM E-Series NCE and the Cisco ISR 4000 Series, on page 59.
Step 14	Router (config-ucse)# **exit**	Exits ucse interface configuration mode.
Step 15	Router (config)# **ip route** *cimc-ip-address subnet-mask* **ucse** *slot/subslot/port*	Creates a static route. • *cimc-ip-address*—IP address of CIMC. • *slot/subslot/port*—Slot, subslot, and port where the NIM E-Series NCE is installed.

	Command or Action	Purpose
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 0**/*subslot*/**0** interface.

Example

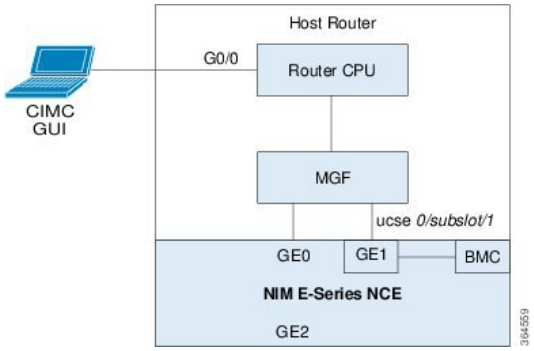
This example shows how to configure CIMC access using the NIM E-Series NCE's internal console interface and the router's **ucse 0**/*subslot*/**0** interface:

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

Router(config)# ucse subslot 0/1
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 0/1/0
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
```

Configuring CIMC Access Using the NIM E-Series NCE's Internal GE1 Interface and the Cisco ISR 4000 Series ucse 0/*subslot*/1 Interface

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

Figure 26: Configuring CIMC Access Using the NIM E-Series NCE's Internal GE1 Interface and the Router's ucse 0/subslot/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 or subslot and port number of the E-Series Server or NCE.

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 0/***subslot***/1**	Enters ucse interface configuration mode for the slot, subslot, and port where the NIM E-Series NCE 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.

	Command or Action	Purpose
		• *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/subslot*	Enters ucse interface configuration mode for the slot and subslot where the NIM E-Series NCE 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 shared-lom ge1**	Configures CIMC access using the NIM E-Series NCE's internal GE1 interface. See # 3 in Understanding the Interfaces in the NIM E-Series NCE and the Cisco ISR 4000 Series, on page 59.
Step 14	Router (config-ucse)# **exit**	Exits ucse interface configuration mode.
Step 15	Router (config)# **ip route** *cimc-ip-address subnet-mask* **ucse** *slot/subslot/port*	Creates a static route. • *cimc-ip-address*—IP address of CIMC. • *slot/subslot/port*—Slot, subslot, and port where the NIM E-Series NCE is installed.

	Command or Action	Purpose
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 0**/*subslot*/**1** interface.

Example

This example shows how to configure CIMC access using the NIM E-Series NCE's internal GE1 interface and the router's ucse **0**/*subslot*/**1** interface:

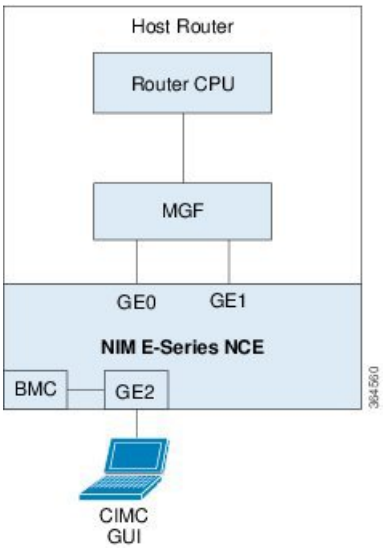
```
Router> enable
Router> password
Router# configure terminal

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

Router(config)# ucse subslot 0/1
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 0/1/1
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
```

Configuring CIMC Access Using the NIM E-Series NCE's External GE2 Interface—Cisco ISR 4000 Series

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

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

Figure 27: Configuring CIMC Access Using the NIM E-Series NCE'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 or subslot and port number of the E-Series Server or NCE.

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/subslot*	Enters ucse interface configuration mode for the slot and subslot where the NIM E-Series NCE 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.

	Command or Action	Purpose
		• *cimc-gateway-ip-address*—IP address for the default gateway.
Step 5	Router (config-ucse)# **imc access-port shared-lom** {**GE2**}	Configures CIMC access through the NIM E-Series NCE's external GE2 interface. See # 5 and 6 in Understanding the Interfaces in the NIM E-Series NCE and the Cisco ISR 4000 Series, on page 59.
Step 6	Router (config-ucse)# **end**	Returns to privileged EXEC mode on the host router.

Example

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

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

Router(config)# ucse subslot 0/1
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
```

Configuring CIMC Access Using the CIMC Configuration Utility

Note This procedure is applicable to E-Series Servers and the SM E-Series NCE. This procedure is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

If you are a local user, you can use either the Cisco IOS CLI or the CIMC Configuration Utility to configure CIMC access.

Note When you use the CIMC Configuration Utility to configure CIMC access, the configuration is not reflected as a 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.

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 username to log in to 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 and the Cisco UCS E-Series Network Compute Engine* or the *CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.

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.

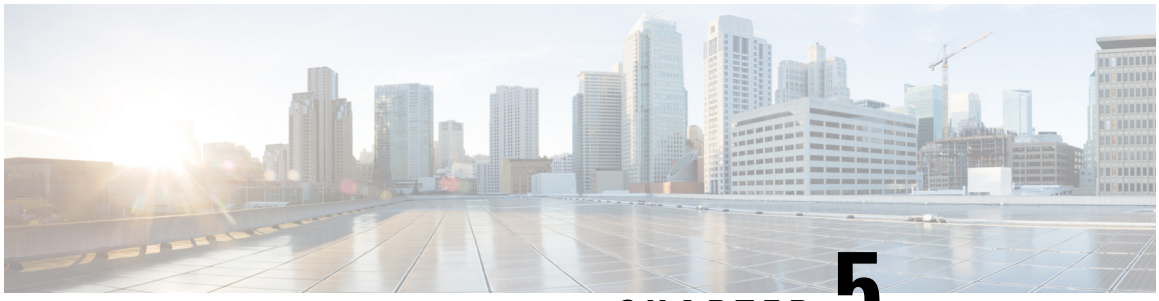
Step 9 Remove the USB thumb drive, alter the **network.cfg** file with your next IP address, and then insert the USB thumb drive into the next server that you want to configure.

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.

What to Do Next

Do one of the following as appropriate:

- If you purchased an E-Series Server or NCE Option 1 (E-Series Server or NCE without a preinstalled operating system or hypervisor), log in to the CIMC GUI or the CIMC CLI to access CIMC. See Accessing the Management Firmware, on page 75.
- If you purchased an E-Series Server or NCE Option 2 (E-Series Server or NCE with a preinstalled Microsoft Windows Server) or Option 3 (E-Series Server or NCE with a preinstalled VMware vSphere Hypervisor), configure an internal connection between the router and the E-Series Server or NCE. 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 or NCE's external 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 or NCE. See Configuring a Connection Between the Router and the E-Series Server or NCE, on page 115.



CHAPTER 5

Accessing the Management Firmware

This chapter includes the following sections:

CIMC Overview

The Cisco Integrated Management Controller (CIMC) is the management service for the E-Series M6 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
- View server properties, router information, and chassis status.
- 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, SNMP, and Redfish.
- Manage certificates
- Configure platform event filters
- Monitor power supply, fan, temperature, voltage, current, LED and storage sensors.
- Update CIMC firmware
- Update BIOS firmware
- Install the host image from an internal repository
- Monitor faults, alarms, and server status

- Set time zone and view local time.
- Collect technical support data in the event of server failure

Most 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 and the NCE. 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

TheCIMC CLI is a command-line management interface for E-Series M6 Servers. You can launch the CIMC CLI in the following ways:

- By the serial port.
- Over the network by SSH.
- From the router. Use one of the following commands as appropriate:
  - **hw-module subslot** *slot/subslot* **session imc**—Use for E-Series Servers installed in a Cisco Catalyst 8300 Edge Series platform.

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.

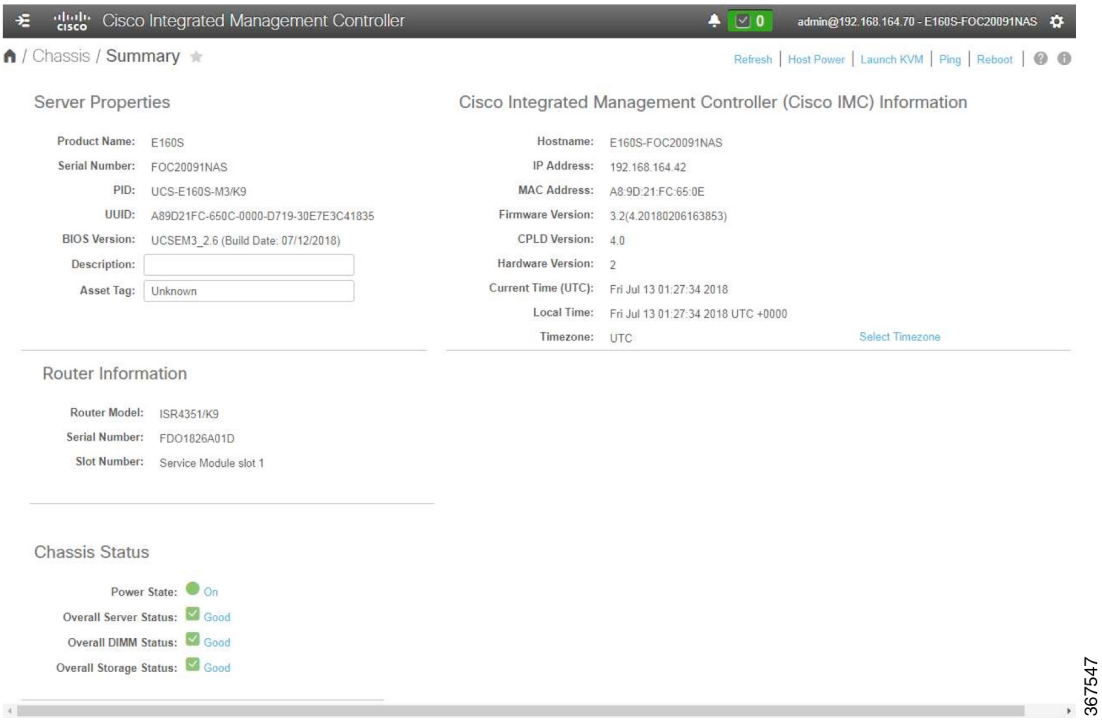
Step 6 In the **Confirm Password** field, enter the password again to confirm it.

Step 7 Click **Save Changes**.

The **Server Summary** page appears, which is the CIMC home page. See CIMC Home Page, on page 78.

CIMC Home Page

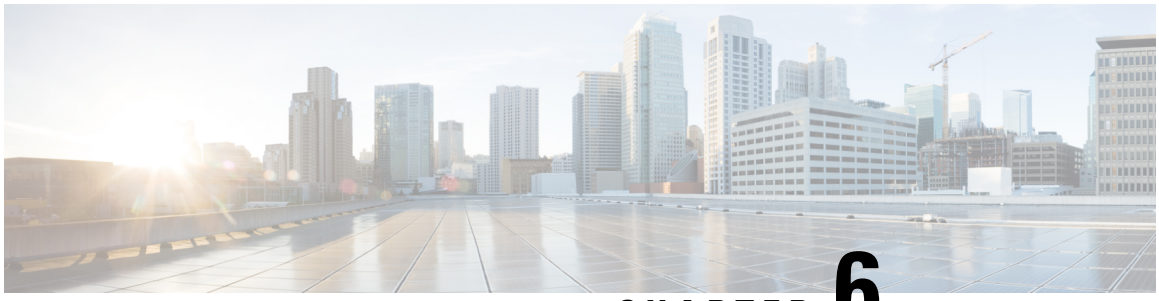
Figure 28: CIMC Home Page



What to Do Next

If you purchased E-Series Server Option 1 (E-Series Server without a preinstalled operating system or hypervisor), configure RAID. See Managing Storage Using RAID , on page 79.

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.



CHAPTER 6

Managing Storage Using RAID

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

Important The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

This chapter includes the following sections:

RAID Options

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

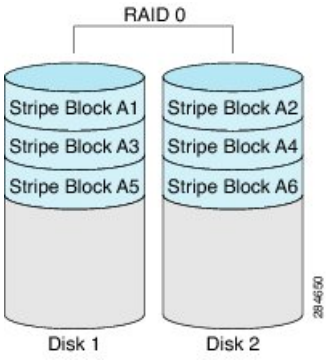
You can choose to store the E-Series Server data files on local Redundant Array of Inexpensive Disks (RAID). The following RAID levels are supported:

- 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 29: 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.

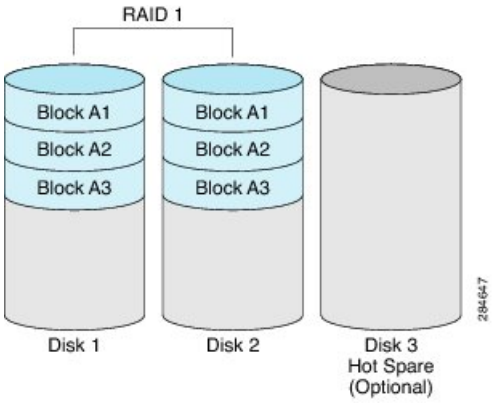
However, there is no fault tolerance, error checking, hot spare, or hot-swapping. If one disk drive fails, the data in the entire array is destroyed. Because there is no error checking or hot-swapping, the array is susceptible to unrecoverable errors.

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 30: RAID 1



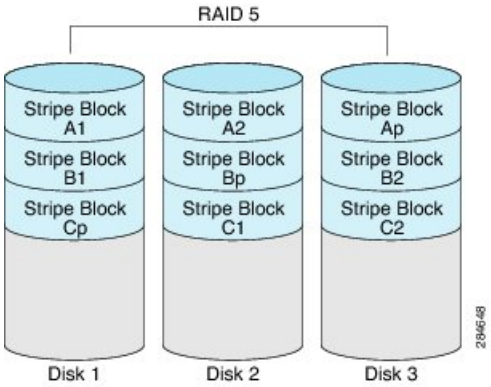
RAID 1 supports fault tolerance and hot-swapping. When one disk drive fails, you can remove the faulty disk drive and replace it with a new disk drive.

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 31: 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.

RAID 10

RAID 10, a combination of RAID 0 and RAID 1, consists of striped data across mirrored spans. A RAID 10 drive group is a spanned drive group that creates a striped set from a series of mirrored drives. RAID 10 allows a maximum of eight spans. You must use an even number of drives in each RAID virtual drive in the span. The RAID 1 virtual drives must have the same stripe size. RAID 10 provides high data throughput and complete data redundancy but uses a larger number of spans.

Note RAID 10 is supported on DoubleWide M3 servers.

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 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.

Note On Cisco UCS M1 and M2 servers, you can use the CIMC GUI or the WebBIOS, which is accessible from the KVM console, to configure RAID. On Cisco UCS M3 servers, you can use the CIMC GUI or the MegaRAID controller, 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** menu.

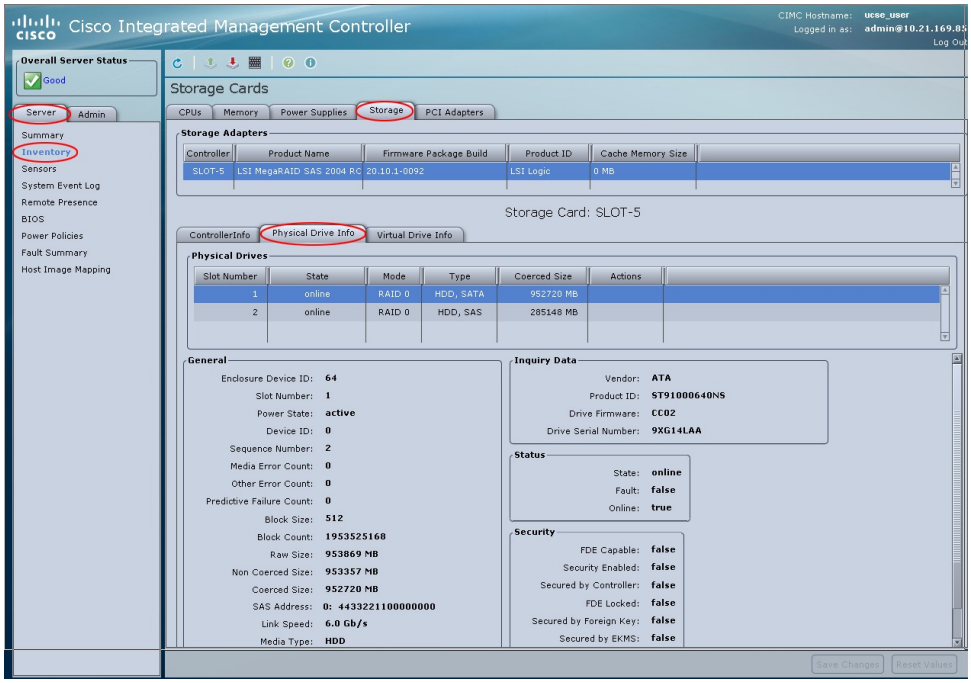
Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Storage** tab.

Step 4 To configure RAID, make sure that the status of each of the physical drives that you want to configure as RAID is **unconfigured good**. To change the physical drive status, do the following:

a) In the tabbed menu of the **Storage Card** area, click the **Physical Drive Info** tab.

Figure 32: Physical Drive Info Tab



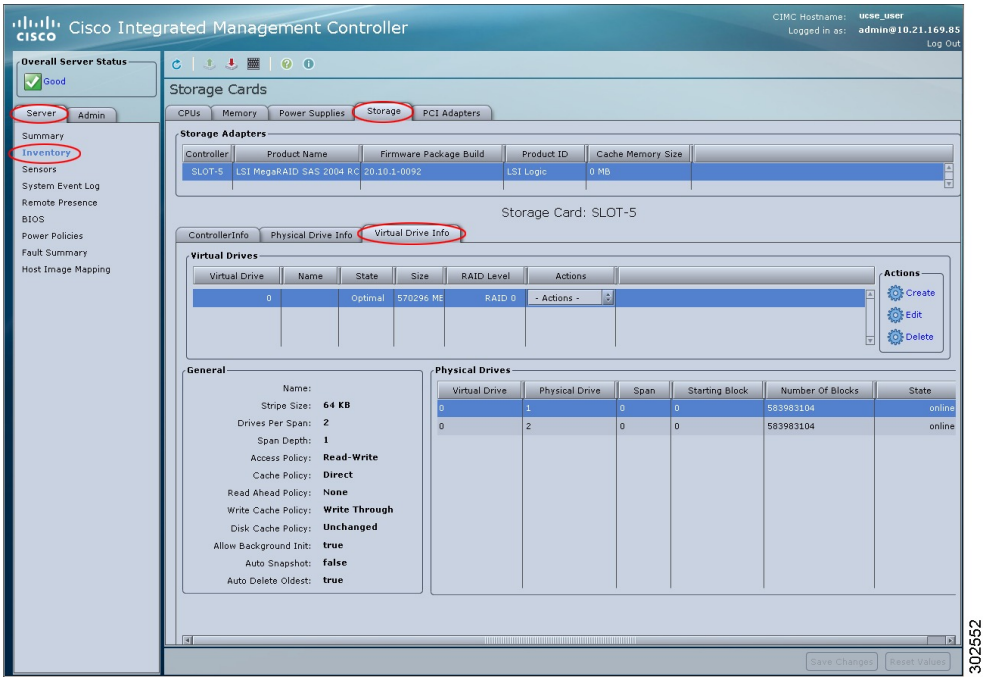
b) From the **Actions** column in the **Physical Drives** pane, choose **Set State** from the drop-down list.

The **Change Physical Drive State** dialog box appears.

c) From the **Change Physical Drive State to** drop-down list, choose **unconfigured good**, and then click **Confirm**.

Step 5 In the tabbed menu of the **Storage Card** area, click the **Virtual Drive Info** tab.

Figure 33: Virtual Drive Info Tab



Step 6 In the **Actions** area of the **Virtual Drive Info** tab, click **Create**.

The **Configure Virtual Drive** dialog box appears. Complete the following fields as appropriate:

Name	Description
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 PCIe option supports RAID 0 and RAID 1 levels.
Unconfigured Drives table	Displays the drives that are unconfigured and available for RAID configuration.
Add >	Moves the selected drives from the **Unconfigured Drives** table to the **Selected Drives** table.
< Remove	Removes the selected drives from the **Selected Drives** table.
Selected Drives table	Displays the drives that are selected for RAID configuration.

Step 7 Click **Next**.

The **Configure RAID Parameters** dialog box appears. Complete the following fields as appropriate:

Name	Description
Strip Size drop-down list	The strip size options. This can be one of the following: • **64 KB** • **32 KB** • **16 KB** • **8 KB** **Caution** The smaller strip sizes have a known problem with VMware vSphere Hypervisor™ installation; therefore, if you are installing the vSphere platform, we recommend that you select the **64 KB** strip size option.
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 only read data from the drive. • **Blocked**—The host cannot access the drive.
Drive Cache drop-down list	How the controller handles drive caching. This can be one of the following: • **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. • **Disable**—Caching is disabled on the drives.

Name	Description
Initialization drop-down list	How the controller initializes the drives. This can be one of the following: • **Quick**—Controller initializes the drive quickly. This is the default and recommended option. **Note** If you are using SSD drives, we recommend that you choose the Quick initialization option. • **Full**—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. • **None**—Controller does not initialize the drives.
HSP check-box	Designates the drive as a hot spare drive. **Note** Applicable for RAID 1 only.
Set Bootable check-box	How the controller boots the drive. This can be one of the following: • **Enable**—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.

Step 8 Click **Next**.

The **Confirm RAID Configuration** dialog box appears.

Step 9 Review the RAID configuration, and then click **Submit** to accept the changes.

Configuring RAID

Note On Cisco UCS M1 and M2 servers, you can use the CIMC GUI or the WebBIOS, which is accessible from the KVM console, to configure RAID. On Cisco UCS M3 servers, you can use the CIMC GUI or the MegaRAID controller, which is accessible from the KVM console, to configure RAID.

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** menu.

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.

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

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 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**

Name	Description
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.
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.

Name	Description
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

Important The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Note Use WebBIOS to configure RAID on M1 and M2 servers. Use MegaRAID controller to configure RAID on M3 servers. See Configuring RAID Using the MegaRAID Controller, on page 89

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

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.

Configuring RAID Using the MegaRAID Controller

Important The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

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 **R** during bootup to access the MegaRAID Controller.

The **Virtual Drive Management** page appears, which allows you to configure MegaRAID Controller.

Configuring RAID Using the Cisco IOS CLI

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# **ucse** *slot* **server raid level {none | 0 | 1 | 5} use** *hard drive list*	Configures the RAID level on the specified hard drive. **Caution** When you use this command, all existing data in the hard drive is lost.
Step 3	At the confirmation prompt, enter **y**.	Proceeds with the RAID configuration process.
Step 4	Router# **show ucse** *slot* **server raid level**	(Optional) Displays the RAID configuration.

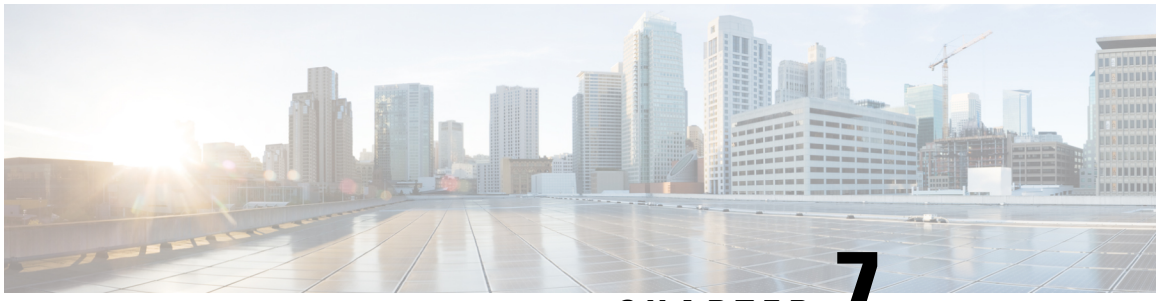
Example

This example shows how to configure RAID using the Cisco IOS CLI.

```
Router> enable
Router> password
Router# ucse 1 server raid level 1 use HDD1 HDD2
You are about to change RAID configuration.
It will destroy all data on the hard drives
Are you sure [y/n] y

RAID reconfigured
Router# show ucse 1 server raid level
md0 : active raid1 HDD1 [1] HDD2 [0]
      10337728 blocks [2/2] [UU]
JBOD: HDD3
```

What to Do Next

If you purchased E-Series Server or NCE Option 1 (E-Series Server or NCE without a preinstalled operating system or hypervisor), install the operating system. See Installing the Operating System or Hypervisor, on page 93.



CHAPTER 7

Installing the Operating System or Hypervisor

Note If you purchased E-Series Server or NCE Option 1 (E-Series Server or NCE without a 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 and NCE 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.

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 The VMware vSphere Hypervisor requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 103.

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.

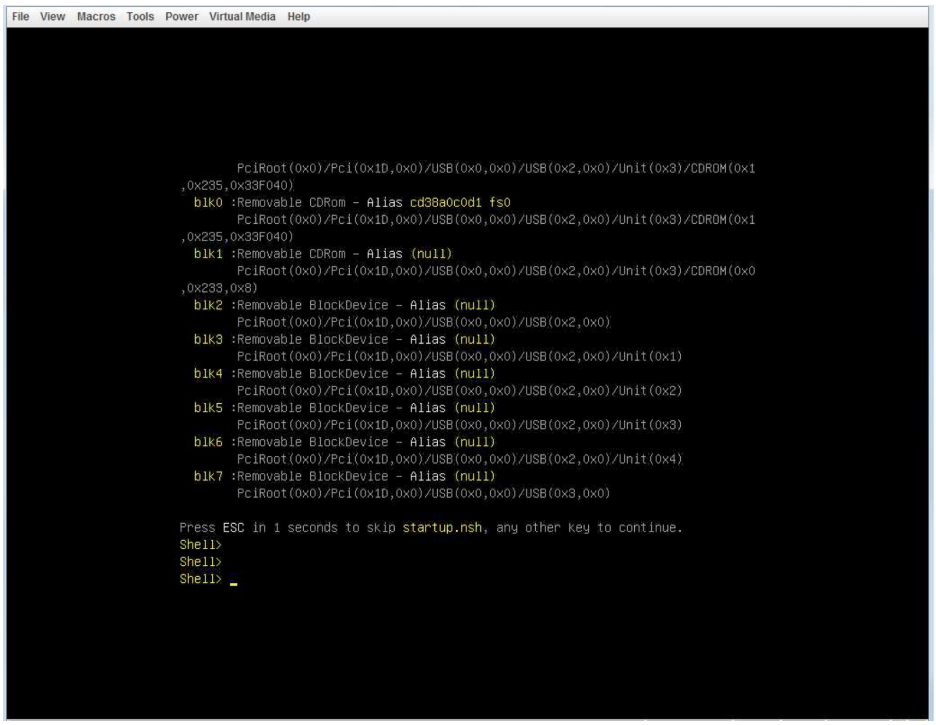
Step 2 If CIMC is not open, log into the CIMC GUI.

Step 3 From the top menu, click **Launch KVM**.

Step 4 From the **Launch KVM** menu, click **Java Based KVM**.

The **KVM Console** opens in a separate window.

Step 5 From the KVM console, click the **Virtual Media** tab.



Step 6 In the **Virtual Media** tab,click **Activate Virtual Devices**

Step 7 Select **Accept this Session** and then click **Apply** .

Step 8 Click the **Virtual Media** tab and click **Map CD/DVD**.

Step 9 Click **Browse**, 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 in the **Virtual Media** tab.

Step 10 Set the boot order to make the virtual CD/DVD drive as the boot device.

Step 11 Reboot the server.

When the server reboots, it begins the installation process from the virtual CD/DVD drive. Refer to the platform installation guide for the installation process.

Step 12 If the 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 99.

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.

Procedure

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

Step 2 Reboot the server.

Caution If you are using the shared LOM interfaces to access CIMC, make sure that you do not use the CIMC GUI during the server reboot process. If you use the CIMC GUI, the GUI will disconnect during PXE installation as the boot agent overrides the IP address that was previously configured on the Ethernet ports.

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

TheHost Image Mapping feature allows you to download, map, unmap, or delete a host image. Download a host image, such as 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 M6 Servers. 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.

Mapping the Host Image

Before you begin

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

Note The VMware vSphere Hypervisor requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 103.

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** menu.

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

Name	Description
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.

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 99.

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 101.

Installing Drivers for the Microsoft Windows Server

Note If you purchased an E-Series Server or NCE Option 1 (E-Series Server or NCE 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 the following 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
- Intel Server Chipset Driver for Windows
- Intel Network Adapter Driver for Windows Server 2012 R2

Note The driver 'Intel Network Adapter Driver for Windows Server 2012 R2' is applicable only for the following servers:

- UCS-E160S-M3 Server
- UCS-EN140N-M2 Server
- UCS-EN120E-M2 Server
- UCS-E180D-M3/K9 Server
- UCS-E1120D-M3/K9 Server

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 100.

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.

This step is applicable to E-Series Servers and the SM E-Series NCE. This step is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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

Obtaining Software from Cisco Systems

Use this procedure to download BIOS and CIMC firmware.

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 Firmware**—Contains the Host Upgrade Utility.

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.

Unmapping the Host Image

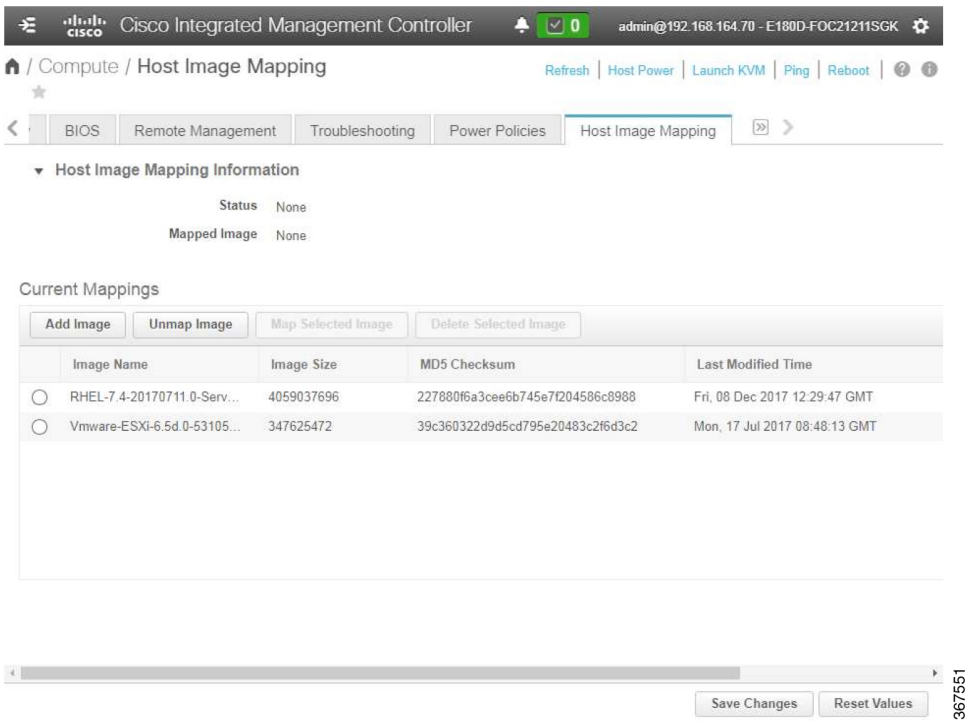
Before you begin

Log in to CIMC as a user with admin privileges.

Procedure

Step 1 In the Navigation pane, click the **Compute** menu.

Step 2 On the **Compute** tab, click **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 the VMware FL-SRE-V-HOST license (equivalent to VMware vSphere Hypervisor 5.X), make sure that the RAM that you are using is 32 GB or less. If the RAM is more than 32 GB, you will get an error message, and you will not be able to apply the license. If you want to use 48 GB of RAM, upgrade your license to FL-SRE-V-HOSTVC.

1. Download the customized VMware vSphere Hypervisor image.
2. Install the VMware vSphere Hypervisor image.
3. Assign a static IP address to the VMware vSphere Hypervisor.
4. 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 Click **Downloads**, and then select **All Products** from the drop-down list.

Step 4 Do one of the following as appropriate:

- To download the VMware vSphere Hypervisor 5.1 image, enter **ESXi-5.1.0-799733-custom-Cisco-2.1.0.3.iso** in the **Search** field, and then click the **Search** icon. From the **Search Results**, click **VMware vSphere > Drivers & Tools > Cisco Custom Image for ESXi 5.1.0 GA Install CD**, and then click **Download**.
- To download the VMware vSphere Hypervisor 5.5 image, enter **ESXi-5.5.0-1331820-custom-Cisco-5.5.0.1.iso**, in the **Search** field, and then click the **Search** icon. From the **Search Results**, click **VMware vSphere > Drivers & Tools > CISCO Custom Image for ESXi 5.5.0 GA Install CD**, and then click **Download**.

What to do next

Install the VMware vSpere Hypervisor 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 103.

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

- Install the image onto the E-Series Server or NCE. For installation instructions, see Mapping the Host Image, on page 97.

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 105. From the vSphere Client, use the host IP address to log in to the VMware vSphere Hypervisor.

Downloading and Installing the vSphere Client

Before you begin

- Make sure that you have assigned a static IP address to the VMware vSphere Hypervisor. See Assigning a Static IP Address to the VMware vSphere Hypervisor, on page 103.
- 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** (for VMware 6.7 version, the default password is **password@123**; for VMWare 7.0 version, the default password is **Password1$**). After you log in, we recommend that you change the password.

Downloading and Installing the Operating System Using the Cisco IOS CLI

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# **ucse slot imc file download URL ftp|ftps|http|https:** *server-ip-address/path/filename.iso*	Downloads the ISO image file from a remote FTP, FTPS, HTTP, or HTTPS server onto the local file system.

	Command or Action	Purpose
Step 3	Router# **show ucse** *slot* **imc download progress**	(Optional) Displays the progress of the download.
Step 4	Router# **ucse** *slot* **server start boot url imc-file:** *filename.iso*	Installs and boots the image file from a local file system.

Example

This example downloads and installs the operating system:

```
Router> enable
Router# ucse 2 imc file download URL ftp 10.20.34.56 pub/hostimage.iso
Started downloading file from ftp 10.20.34.56 pub/hostimage.iso
Router# show ucse 2 imc file download progress
Downloaded 23%
Router# ucse 2 server start boot url imc-file: hostimage.iso
```

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

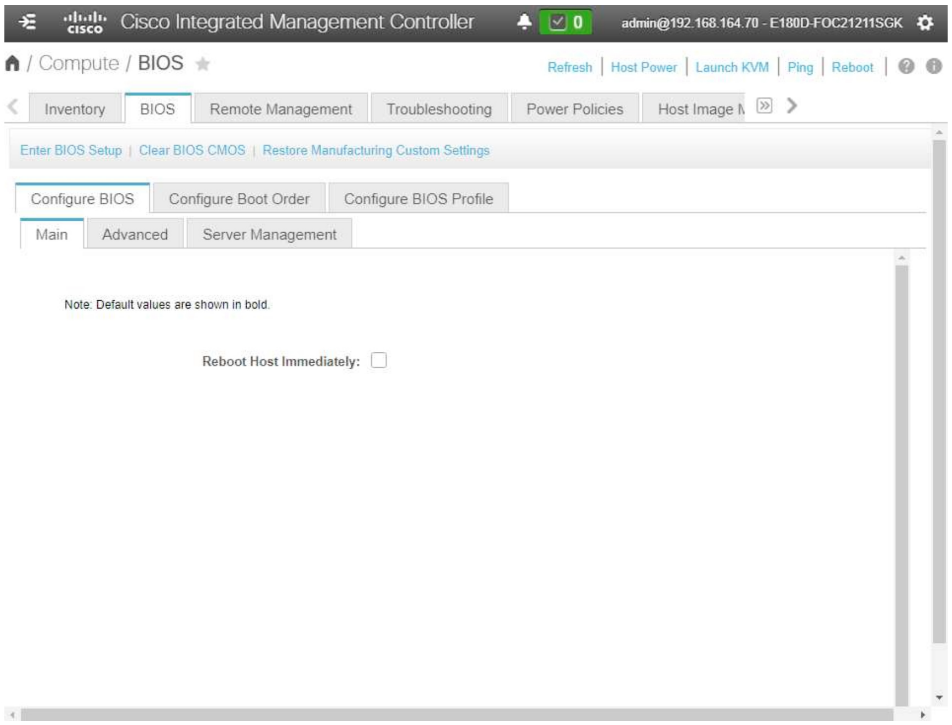
Before you begin

Log into CIMC as a user with admin privileges.

Procedure

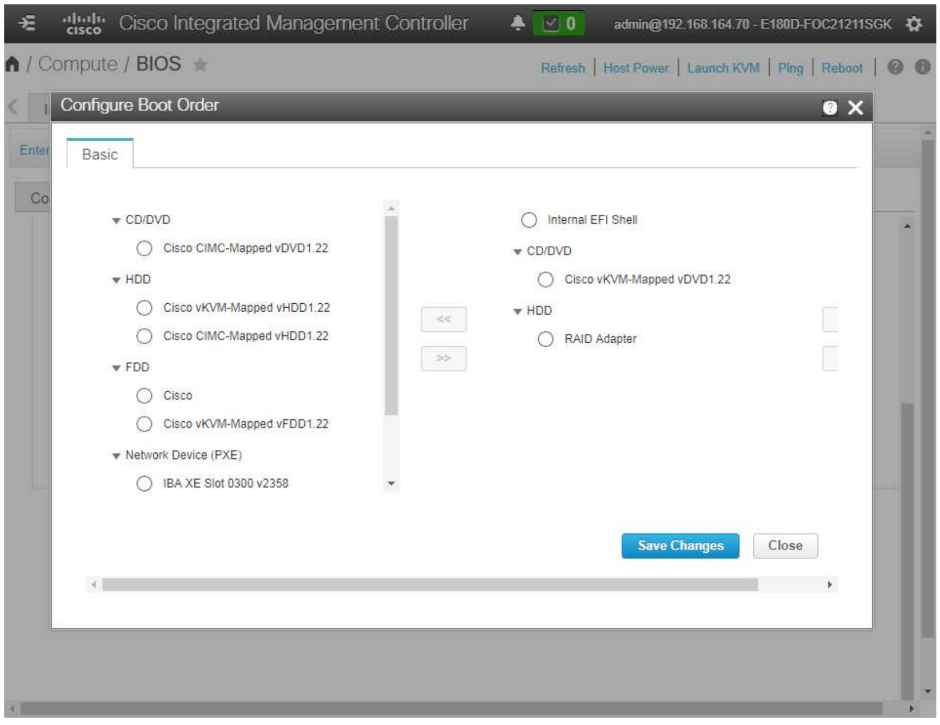
Step 1 In the Navigation pane, click the **Compute** menu.

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



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

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



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. • **FDD**—Floppy disk drive. • **CDROM**—Bootable CD-ROM. • **PXE**—PXE boot. • **EFI** —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 Server Boot Order Using the CIMC GUI

Before you begin

Log into CIMC as a user with admin privileges.

Procedure

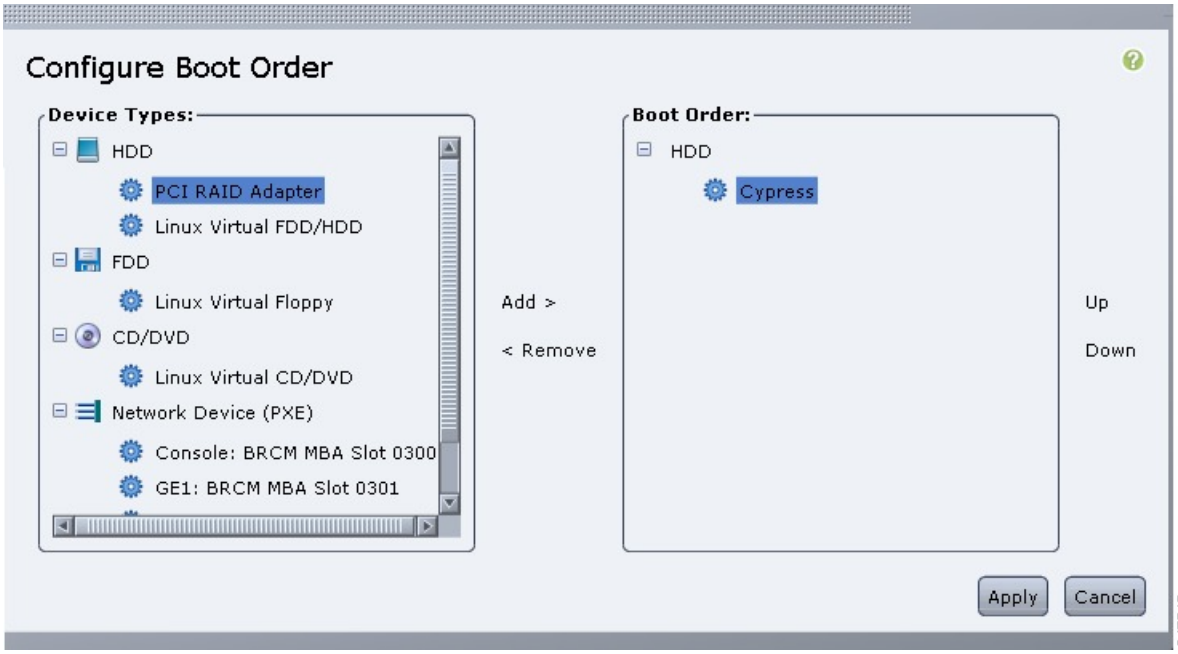
Step 1 In the **Navigation** pane, click the **Server** menu.

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

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

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

Figure 34: 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** • **SSD Hard Drive** • **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** • **GE1** • **GE2** • **GE3** • **TE2** • **TE3** **Note** The PXE boot options vary depending on the platform. For instance, the M3 servers use TE2 and TE3 instead of GE2 and GE3. • **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 a USB or an external CD-ROM drive that is directly connected to the E-Series Server or NCE.

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

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.

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.

Configuring the Server Boot Order Using the Cisco IOS CLI

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 ucse** *slot* **server boot devices**	Displays the devices available from which you can boot the server.
Step 3	Router# **ucse** *slot* **server boot order device_1 [device_2] [device_3] [device_4]**	Specifies the devices from which to boot the server. **Note** The name of the devices must exactly match the names displayed by the output of the **show ucse***slot* **server boot devices** command. The device can be any of the following, but you can only use each device name once: • **PXE**—PXE boot • **FDD**—Floppy disk drive • **HDD**—Hard disk drive • **CDROM**—Bootable CD-ROM
Step 4	Router# **show ucse** *slot* **server boot order**	(Optional) Displays the order in which the device boot is attempted.

Example

This example configures the boot order:

```
Router> enable
Router# show ucse 2 server boot devices
PXE
FDD
HDD:HDD3
HDD:RAID-MD0
HDD:USB-FF5D6CC3DAA67F12-1
CDROM:USB-CD
Router# ucse 2 boot order PXE CDROM:USB-CD FDD HDD:RAID-MD0
Router# show ucse 2 server boot order
Currently booted from CDROM:USB-CD
Boot order:
1) PXE
2) CDROM:USB-CD
3) FDD
```

```
4) HDD:RAID-MD0
```

Verifying Operating System and Hypervisor Installation

Accessing the Microsoft Windows Server from CIMC

Before you begin

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

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

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

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

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

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 103.

Step 5 Make sure that you have installed vSphere Client. If not, install it. See Downloading and Installing the vSphere Client, on page 105.

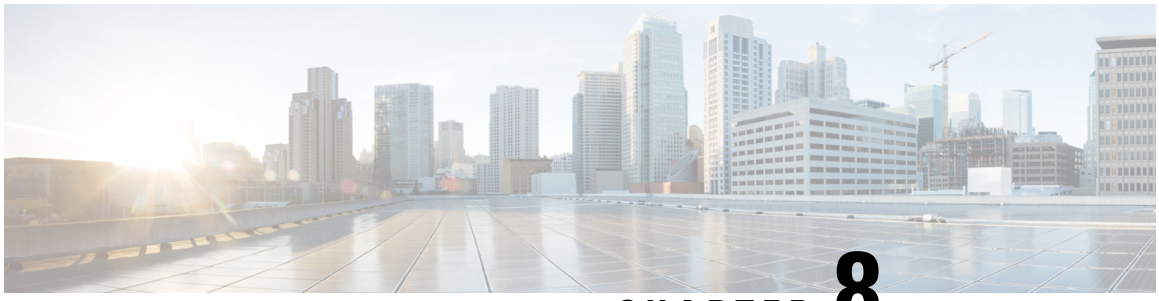
Step 6 From the vSphere Client, log in to the VMware vSphere Hypervisor.

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** (For VMware version 7.0, the default password is **Password1$**). After you log in, we recommend that you change the password.

What to Do Next

Configure a connection between the router and the server. See Configuring a Connection Between the Router and the E-Series Server or NCE, on page 115.



CHAPTER 8

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

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 or NCE's external interface.
- If you *want* the traffic to your application or operating system to flow through the router, use the procedures provided in this chapter to configure an internal connection between the router and the E-Series Server or NCE.

This chapter includes the following sections:

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

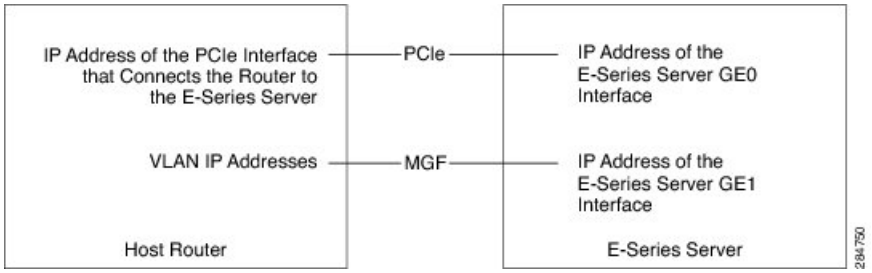
Use this configuration if you want the traffic to your application or operating system to flow through the Cisco ISR G2. To configure an internal connection between the Cisco ISR G2 and the E-Series Server, you must configure these IP addresses:

- 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 35: Internal Connection Between the Cisco 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 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 the 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.

	Command or Action	Purpose
		Caution The **ip unnumbered** command creates a point-to-point interface between devices. Broadcasting is not supported.
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **end**	Exits interface configuration mode.
Step 7	Use the server's operating system to configure the E-Series Server's **GE0** interface. See the figure above.	—
Step 8	Router (config)# **interface ucse** *slot*/**1**	Enters interface configuration mode for the router's MGF *slot*/**1** VLAN interface. See the 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 interface 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 the 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 interface configuration mode.
Step 17	Use the server's operating system to configure the E-Series Server's **GE1** interface. See figure above.	—

Example

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.
```

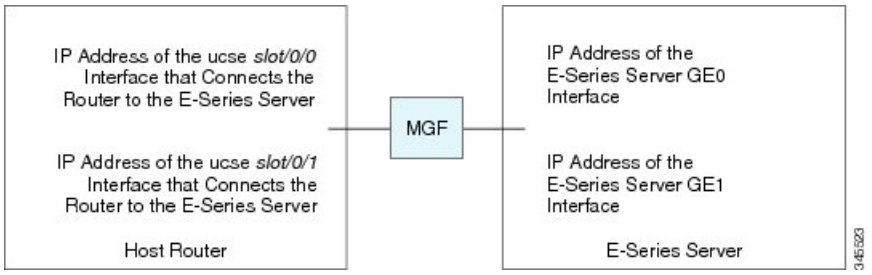
Configuring an Internal Connection Between the Cisco ISR 4000 Series and the E-Series Server

Use this configuration if you want the traffic to your application or operating system to flow through the Cisco ISR 4000 series. To configure an internal connection between the Cisco ISR 4000 series 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 36: Internal Connection Between the Cisco ISR 4000 Series 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 the 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.
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.

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

Example

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.
```

Creating an Ethernet Virtual Circuit Between the E-Series Server and the Cisco ISR 4000 Series Using the Native VLAN

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 4000 series 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	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.	—

Example

This example shows how to create an Ethernet Virtual Circuit using the native VLAN between the E-Series Server and the Cisco ISR 4000 series.

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)# 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.
```

Creating an Ethernet Virtual Circuit Between the E-Series Server and the Cisco ISR 4000 Series Using a Non-Native VLAN

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 E-Series Server and the Cisco ISR 4000 series.

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	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.
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:	• The **rewrite egress tag push dot1q** command specifies the encapsulation

	Command or Action	Purpose
	• 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*	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)# **exit**	Exits interface configuration mode.
Step 13	Router (config)# **interface BDI** *bridge-id*	Enters the bridge domain interface.
Step 14	Router (config-if)# **ip address** *bdi-interface-ip-address*	Specifies the IP address of the BDI interface.
Step 15	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 16	Router (config-if)# **end**	Returns to global configuration mode on the host router.
Step 17	Use the server's operating system to configure the E-Series Server's **NIC** interface.	—
Step 18	Router# **ping** *server's-NIC-interface*	Shows if connection is established with the E-Series Server's **NIC** interface.
Step 19	Router# **show arp**	Displays the Access Resolution Protocol (ARP) cache.
Step 20	Router# **show bridge-domain** *bridge-id*	Displays bridge domain information.

Example

This example shows how to create an Ethernet virtual circuit using a non-native VLAN between the E-Series Server and the Cisco ISR 4000 series.

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)# exit

Router(config)# 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.

Configuring an Internal Connection Between the Cisco ISR G2 and the EHWIC E-Series NCE

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

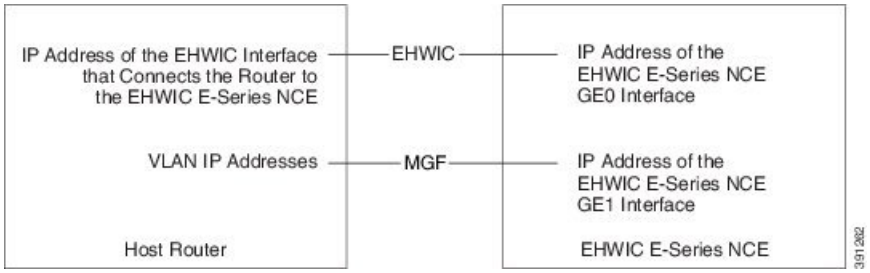
- For traffic to flow through the EHWIC connection (see next figure), configure the following:
  - IP address of the router's internal EHWIC interface that connects the router to the EHWIC E-Series NCE's GE0 interface.
  - IP address of the EHWIC E-Series NCE's GE0 interface.
- For traffic to flow through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

Important The MGF connection option is not applicable to the Cisco 1921 ISR G2.

- IP address of the router's internal MGF VLAN interface.
- IP address of the EHWIC E-Series NCE's GE1 interface.

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

Figure 37: Internal Connection Between the Cisco ISR G2 and the EHWIC E-Series NCE



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 0**/*subslot*/**0**	Enters interface configuration mode for the router's EHWIC **0**/*subslot*/**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 EHWIC E-Series NCE's GE0 interface. See the 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.

	Command or Action	Purpose
		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.
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **end**	Exits interface configuration mode.
Step 7	Use the server's operating system to configure the EHWIC E-Series NCE's **GE0** interface. See the figure above.	—
Step 8	Router (config)# **interface ucse 0/***subslot***/1**	Enters interface configuration mode for the router's MGF **0/***subslot***/1** VLAN interface. See the figure above. **Important** This step is not applicable to the Cisco ISR 1921.
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)# **end**	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 interface 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 the 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.

	Command or Action	Purpose
Step 16	Router (config-if)# **end**	Exits interface configuration mode.
Step 17	Use the server's operating system to configure the EHWIC E-Series NCE's **GE1** interface. See the figure above.	**Important** This step is not applicable to the Cisco 1921 ISR G2.

Example

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

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 0/1/0
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 0/1/1
Router(config-if)# switchport mode trunk
Router(config-if)# end

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.
```

Configuring an Internal Connection Between the Cisco ISR 4000 Series and the NIM E-Series NCE

Use this configuration if you want the traffic to your application or operating system to flow through the Cisco ISR 4000 series. To configure an internal connection between the Cisco ISR 4000 series and the NIM E-Series NCE, you must configure these IP addresses:

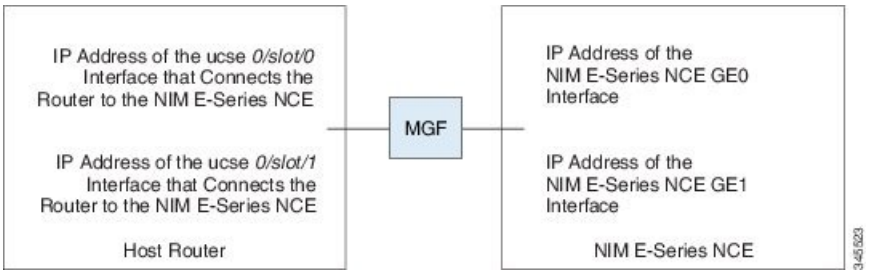
- For traffic to flow through the router's **ucse 0**/*subslot*/**0** and the server's internal GE0 interface (see next figure), configure the following:
  - IP address of the router's **ucse 0**/*subslot*/**0** interface that connects the router to the server's GE0 interface.

- IP address of the server's GE0 interface.

- For traffic to flow through the router's **ucse 0/***subslot***/1** and the server's internal GE1 interface (see next figure), configure the following:
  - IP address of the router's **ucse 0/***subslot***/1** interface.
  - IP address of the server's GE1 interface.

The following figure shows the internal connection between the router and the server.

Figure 38: Internal Connection Between the Cisco ISR 4000 Series and the NIM E-Series NCE



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 0/***subslot***/0**	Enters interface configuration mode for the router's ucse **0/***subslot***/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 0/***subslot***/0** interface that connects the router to the server's GE0 interface. See the 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.

	Command or Action	Purpose
		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.
Step 5	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 6	Router (config-if)# **end**	Exits interface configuration mode.
Step 7	Use the server's operating system to configure the server's **GE0** interface. See the figure above.	—
Step 8	Router (config)# **interface ucse 0/***subslot***/1**	Enters interface configuration mode for the router's ucse **0/***subslot***/1** interface.
Step 9	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 10	Router (config-if)# **end**	Exits interface configuration mode.
Step 11	Use the server's operating system to configure the server's **GE1** interface. See the figure above.	—

Example

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

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 0/1/0
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 NIM E-Series NCE's GE0 interface.

Router(config)# interface ucse 0/1/1
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 NIM E-Series NCE's GE1 interface.
```

Creating an Ethernet Virtual Circuit Between the NIM E-Series NCE and the Cisco ISR 4000 Series Using the Native VLAN

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 4000 series and the NIM E-Series NCE.

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 0/***subslot***/0**	Enters interface configuration mode for the router's **0/***subslot***/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 NIM E-Series NCE's **GE0** interface.	—

Example

This example shows how to create an Ethernet Virtual Circuit using the native VLAN between the NIM E-Series NCE and the Cisco ISR 4000 series.

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

```
Router> enable
Router# configure terminal

Router(config)# interface ucse 0/1/0
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)# 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 NIM E-Series NCE's GE0 interface.
```

Creating an Ethernet Virtual Circuit Between the NIM E-Series NCE and the Cisco ISR 4000 Series Using a Non-Native VLAN

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 NIM E-Series NCE, or to the virtual machines created on the installed hypervisor.

Before you begin

Configure an internal connection between the Cisco ISR 4000 series and the NIM E-Series NCE.

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 0/***subslot***/0**	Enters interface configuration mode for the router's ucse **0/***subslot***/0** interface.
Step 4	Router (config-if)# **no ip address**	Removes an IP address or disables IP processing.

	Command or Action	Purpose
Step 5	Router (config-if)# **no negotiation auto**	Disables automatic negotiation on the interface.
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)# **exit**	Exits interface configuration mode.
Step 13	Router (config)# **interface BDI** *bridge-id*	Enters the bridge domain interface.
Step 14	Router (config-if)# **ip address** *bdi-interface-ip-address*	Specifies the IP address of the BDI interface.
Step 15	Router (config-if)# **no shut**	Causes the interface to be administratively up.
Step 16	Router (config-if)# **end**	Returns to global configuration mode on the host router.
Step 17	Use the server's operating system to configure the NIM E-Series NCE's **NIC** interface.	—
Step 18	Router# **ping** *server's-NIC-interface*	Shows if connection is established with the NIM E-Series NCE's **NIC** interface.
Step 19	Router# **show arp**	Displays the Access Resolution Protocol (ARP) cache.
Step 20	Router# **show bridge-domain** *bridge-id*	Displays bridge domain information.

Example

This example shows how to create an Ethernet virtual circuit using a non-native VLAN between the NIM E-Series NCE and the Cisco ISR 4000 series.

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

```
Router> enable
Router# configure terminal
Router(config)# interface ucse 0/1/0
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)# exit

Router(config)# 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 NIM E-Series NCE'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 GE0, GE1, GE2, and GE3 interfaces—Cisco ISR G2
- E-Series Server's GE0, GE1, GE2, and GE3 interfaces—Cisco ISR 4000 series
- EHWIC E-Series NCE's GE0, GE1, and GE2 interfaces—Cisco ISR G2
- NIM E-Series NCE's GE0, GE1, and GE2 interfaces—Cisco ISR 4000 series
- NetXtreme II 1 Gigabit Server (PCIe Card)
- NetXtreme II 10 Gigabit Server (PCIe Card)

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

- The lowest numbered MAC address corresponds to the E-Series Server's GE0 interface.
- The second lowest MAC address corresponds to the E-Series Server's GE1 interface.
- The third lowest MAC address corresponds to the E-Series Server's GE2 interface.
- The 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 136 section, or the appropriate platform documentation.

Determining Network Interface Mapping for the E-Series Server's GE0, GE1, GE2, and GE3 Interfaces—Cisco ISR 4000 series

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

- The lowest numbered MAC address corresponds to the E-Series Server's GE0 interface.
- The second lowest MAC address corresponds to the E-Series Server's GE1 interface.
- The third lowest MAC address corresponds to the E-Series Server's GE2 interface.
- The 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 136 section, or the appropriate platform documentation.

Determining Network Interface Mapping for the EHWIC E-Series NCE's GE0, GE1, and GE2 Interfaces—Cisco ISR G2

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

- The lowest numbered MAC address corresponds to the EHWIC E-Series NCE's GE0 interface.
- The second lowest MAC address corresponds to the EHWIC E-Series NCE's GE1 interface.
- The third lowest MAC address corresponds to the EHWIC E-Series NCE's GE2 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 136 section, or the appropriate platform documentation.

Determining Network Interface Mapping for the NIM E-Series NCE's GE0, GE1, and GE2 Interfaces—Cisco ISR 4000 series

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

- The lowest numbered MAC address corresponds to the NIM E-Series NCE's GE0 interface.
- The second lowest MAC address corresponds to the NIM E-Series NCE's GE1 interface.
- The third lowest MAC address corresponds to the NIM E-Series NCE's GE2 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 136 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

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.

UCS E Series M3 Servers:Reordering ESXi VMNIC Interface Number to Start with Server's Lowest MAC Address

On Cisco UCS E Series M3 servers, the VMware vSphere Hypervisor DCUI VMNIC interface ordering does not map to server's lowest MAC address. After installing ESXi on M3 servers, the default DCUI VMNIC interface ordering and server's NIC interface mappings are:

```
~ Name    MAC Address        UCS-E160S-M3 NIC   Description
------  -------------      ----------------
-------------------------------------------------------
vmnic0  a8:9d:21:fc:61:12  TE2                Intel(R) Ethernet Connection X552/X557-AT
10GBASE-T
vmnic1  a8:9d:21:fc:61:13  TE3                Intel(R) Ethernet Connection X552/X557-AT
10GBASE-T
vmnic2  a8:9d:21:fc:61:10  GE0              Broadcom Corporation NetXtreme BCM5719 Gigabit
 Ethernet
vmnic3  a8:9d:21:fc:61:11  GE1              Broadcom Corporation NetXtreme BCM5719 Gigabit
 Ethernet
```

To make VMNIC interface ordering to start with the server's lowest MAC address, follow these procedures:

1. Enable SSH and Shell Access in ESXi.
2. SSH into ESXi .
3. Use **esxcli network nic list** command to display VMNIC number and its correpsonding MAC address.
4. Use **localcli --plugin-dir /usr/lib/vmware/esxcli/int/deviceInternal alias list** command to display the Bus address and VMNIC number mappings.
5. Use **localcli** command to remap VMNIC number to Bus address that has the lowest MAC address.
6. Reboot ESXi.
7. SSH into ESXi and verify changes.

The following example shows how to display VMNIC number and its MAC address:

```
~ # esxcli network nic list
Name    PCI Device     Driver  Link  Speed  Duplex  MAC Address         MTU  Description
------  -------------  ------  ----  -----  ------  -----------------  ----
-------------------------------------------------------
vmnic0  0000:004:00.0  ixgbe   Up     1000  Full    a8:9d:21:fc:61:12  1500  Intel(R)
Ethernet Connection X552/X557-AT 10GBASE-T
vmnic1  0000:004:00.1  ixgbe   Up     1000  Full    a8:9d:21:fc:61:13  1500  Intel(R)
Ethernet Connection X552/X557-AT 10GBASE-T
vmnic2  0000:008:00.0  tg3     Up     1000  Full    a8:9d:21:fc:61:10  1500  Broadcom
Corporation NetXtreme BCM5719 Gigabit Ethernet
vmnic3  0000:008:00.1  tg3     Up     1000  Full    a8:9d:21:fc:61:11  1500  Broadcom
Corporation NetXtreme BCM5719 Gigabit Ethernet
```

The following example shows how to display Bus address and VMNIC name mapping:

```
~ # localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias list
Bus type  Bus address          Alias
--------------------------------
```

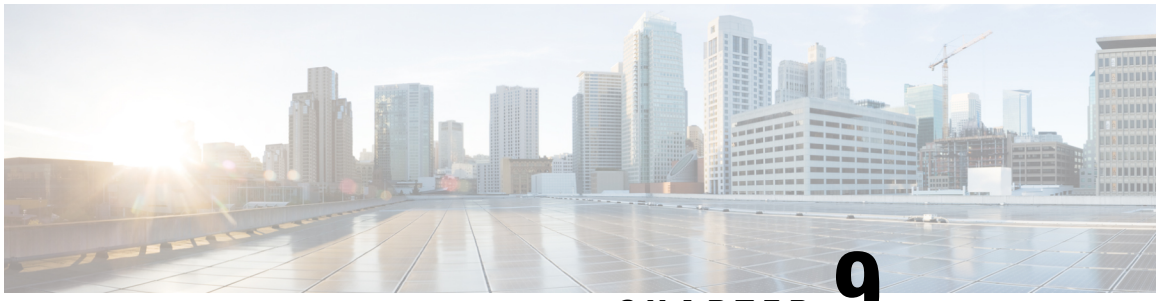
```
pci       p0000:06:00.0        vmhba0
pci       p0000:08:00.0        vmnic2
pci       p0000:08:00.1        vmnic3
pci       p0000:04:00.1        vmnic1
pci       p0000:04:00.0        vmnic0
logical   pci#p0000:06:00.0#0  vmhba0
```

The following example shows how to remap VMNIC number to the Bus address that has the lowest MAC adddress:

```
~ # localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --alias
vmnic0 --bus-address p0000:08:00.0 --bus-type pci
~ # localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --alias
vmnic1 --bus-address p0000:08:00.1 --bus-type pci
~ # localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --alias
vmnic2 --bus-address p0000:04:00.0 --bus-type pci
~ # localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --alias
vmnic3 --bus-address p0000:04:00.1 --bus-type pci
~ # reboot
```

The following example shows how the VMNIC interface ordering looks like after the reboot. The VMNIC interface number begins with the lowest MAC address.:

```
~ # esxcli network nic list
Name    PCI Device     Driver  Link  Speed  Duplex  MAC Address         MTU  Description
------  -------------  ------  ----  -----  ------  -----------------  ----
-------------------------------------------------------
vmnic0  0000:008:00.0  tg3     Up     1000  Full    a8:9d:21:fc:61:10  1500  Broadcom
Corporation NetXtreme BCM5719 Gigabit Ethernet
vmnic1  0000:008:00.1  tg3     Up     1000  Full    a8:9d:21:fc:61:11  1500  Broadcom
Corporation NetXtreme BCM5719 Gigabit Ethernet
vmnic2  0000:004:00.0  ixgbe   Up     1000  Full    a8:9d:21:fc:61:12  1500  Intel(R)
Ethernet Connection X552/X557-AT 10GBASE-T
vmnic3  0000:004:00.1  ixgbe   Up     1000  Full    a8:9d:21:fc:61:13  1500  Intel(R)
Ethernet Connection X552/X557-AT 10GBASE-T
~ # localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias list
Bus type  Bus address          Alias
------------------------------------
pci       p0000:06:00.0        vmhba0
pci       p0000:08:00.0        vmnic0
pci       p0000:08:00.1        vmnic1
pci       p0000:04:00.1        vmnic3
pci       p0000:04:00.0        vmnic2
logical   pci#p0000:06:00.0#0  vmhba0
~ #
```



CHAPTER 9

Upgrading Firmware

This chapter includes the following sections:

Options for Upgrading Firmware

You can use either the Cisco Host Upgrade Utility (HUU) to upgrade the firmware components or you can upgrade the firmware components manually.

- **HUU**—We recommend that you use the HUU ISO file to upgrade all firmware components, which include the CIMC and BIOS firmware.
- **Manual Upgrade**—To manually upgrade the CIMC and BIOS firmware, you must first obtain the firmware from Cisco Systems, and then use the CIMC GUI or the CIMC CLI to upgrade it. After you upgrade the firmware, reboot the system.

Cisco Host Upgrade Utility Overview

The Cisco Host Upgrade Utility (HUU) is a tool that you can use to upgrade the firmware on the Cisco UCS E-Series Servers (E-Series Servers) and the Cisco UCS E-Series Network Compute Engine (NCE). The HUU provides a web-based GUI where you can choose all or specific firmware components to upgrade.

The following firmware components are available for upgrade:

- Cisco Integrated Management Controller (CIMC)
- System BIOS
- LAN on motherboard (LOM)
- RAID controllers
- Broadcom PCI adapters:
  - 5709 Dual and Quad port adapters
  - 57712 Dual port adapter
- LSI
  - LSI MegaRAID SAS 9240-4i

Note Cisco UCS E Series servers do not support saving HUU logs to RAID_SD0_1.

You cannot use the HUU to upgrade the Programmable Logic Devices (PLD) firmware. You must use the Cisco IOS CLI to upgrade the PLD firmware. For details, see the "Upgrading Programmable Logic Devices Firmware on the E-Series EHWIC NCE" section in the *CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.

Minimum CIMC and BIOS Firmware Releases Required to Use HUU

The HUU is supported on CIMC, release 2.1.0 and later releases. To use HUU, make sure that you upgrade both the CIMC and BIOS firmware to the release specified in the table below.

Note The HUU is *not* supported on CIMC, releases 1.0 and 1.0(2). If you try to use the HUU on a server that has an older release of CIMC, you will get an error message asking you to upgrade the firmware.

The following table provides information about the minimum CIMC and BIOS releases required to use the HUU.

Table 5: Minimum CIMC and BIOS Firmware Releases Required to Use HUU

Minimum Compatible CIMC Release	Minimum Compatible BIOS Release
2.1.0	1.5.0.2

CIMC and BIOS Firmware Releases Available With HUU ISO Images

The following table provided the CIMC and BIOS firmware releases that are available for upgrade when you install a specific HUU ISO image.

Table 6: CIMC and BIOS Firmware Releases Available With HUU ISO Images

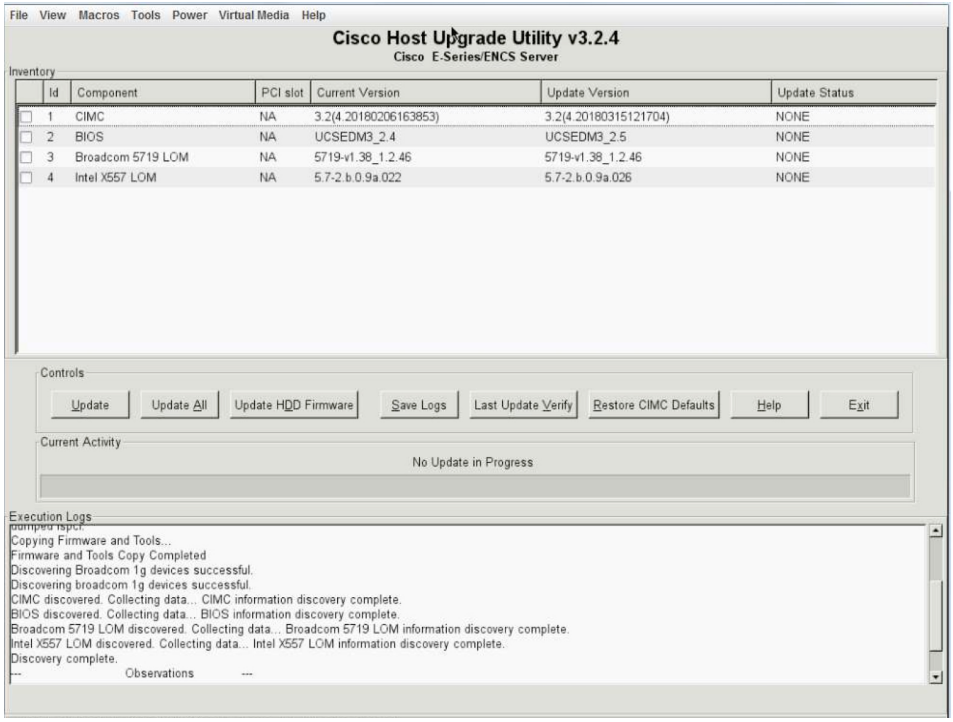
HUU ISO Image	Contains CIMC Release	Contains BIOS Release
3.1.1	3.1.1	UCSEN.1.5.0.3—Applicable to the EHWIC E-Series NCE and the NIM E-Series NCE (UCS-EN120E and UCS-EN140N-M2) UCSES.1.5.0.2—Applicable to the single-wide E-Series Server (UCS-E140S-M1, UCS-EN120S-M2 and UCS-E140S-M2) UCSED.2.5.0.3—Applicable to the double-wide E-Series Servers (UCS-E140D-M1, UCS-E160D-M1, UCS-E160D-M2 and UCS-E180D-M2)
3.1.2	3.1.2	UCSEN.1.5.0.3—Applicable to the EHWIC E-Series NCE and the NIM E-Series NCE (UCS-EN120E and UCS-EN140N-M2) UCSES.1.5.0.2—Applicable to the single-wide E-Series Server (UCS-E140S-M1, UCS-EN120S-M2 and UCS-E140S-M2) UCSED.2.5.0.3—Applicable to the double-wide E-Series Servers (UCS-E140D-M1, UCS-E160D-M1, UCS-E160D-M2 and UCS-E180D-M2)
3.1.3	3.1.3	UCSEN.1.5.0.3—Applicable to the EHWIC E-Series NCE and the NIM E-Series NCE (UCS-EN120E and UCS-EN140N-M2) UCSES.1.5.0.2—Applicable to the single-wide E-Series Server (UCS-E140S-M1) UCSES.1.5.0.5—Applicable to the single-wide E-Series Server (UCS-EN120S-M2 and UCS-E140S-M2) UCSED.2.5.0.3—Applicable to the double-wide E-Series Servers (UCS-E140D-M1, UCS-E160D-M1, UCS-E160D-M2 and UCS-E180D-M2)

HUU ISO Image	Contains CIMC Release	Contains BIOS Release
3.1.4	3.1.4	UCSEN.1.5.0.3—Applicable to the EHWIC E-Series NCE and the NIM E-Series NCE (UCS-EN120E and UCS-EN140N-M2) UCSES.1.5.0.2—Applicable to the single-wide E-Series Server (UCS-E140S-M1) UCSES.1.5.0.5—Applicable to the single-wide E-Series Server (UCS-EN120S-M2 and UCS-E140S-M2) UCSED.2.5.0.3—Applicable to the double-wide E-Series Servers (UCS-E140D-M1, UCS-E160D-M1, UCS-E160D-M2 and UCS-E180D-M2) UCSEM3.1.0—Applicable to the single-wide E-Series Server (UCS-E160S-M3)
3.2.2	3.2.2	UCSEN.1.5.0.5—Applicable to the EHWIC E-Series NCE and the NIM E-Series NCE (UCS-EN120E and UCS-EN140N-M2) UCSES.1.5.0.2—Applicable to the single-wide E-Series Server (UCS-E140S-M1) UCSES.1.5.0.6—Applicable to the single-wide E-Series Server (UCS-EN120S-M2 and UCS-E140S-M2) UCSED.2.5.0.4—Applicable to the double-wide E-Series Servers (UCS-E140D-M1, UCS-E160D-M1, UCS-E160D-M2 and UCS-E180D-M2) UCSEM3.2.4—Applicable to the single-wide E-Series Server (UCS-E160S-M3) UCSEDM3.2.4—Applicable to the single-wide E-Series Server (UCS-E180D-M3 and UCS-E1120D-M3)

HUU ISO Image	Contains CIMC Release	Contains BIOS Release
3.2.3	3.2.3	UCSEN.1.5.0.5—Applicable to the EHWIC E-Series NCE and the NIM E-Series NCE (UCS-EN120E and UCS-EN140N-M2) UCSES.1.5.0.2—Applicable to the single-wide E-Series Server (UCS-E140S-M1) UCSES.1.5.0.6—Applicable to the single-wide E-Series Server (UCS-EN120S-M2 and UCS-E140S-M2) UCSED.2.5.0.4—Applicable to the double-wide E-Series Servers (UCS-E140D-M1, UCS-E160D-M1, UCS-E160D-M2 and UCS-E180D-M2) UCSEM3.2.4—Applicable to the single-wide E-Series Server (UCS-E160S-M3) UCSEDM3.2.4—Applicable to the single-wide E-Series Server (UCS-E180D-M3 and UCS-E1120D-M3)
3.2.4	3.2.4	UCSEN.1.5.0.5—Applicable to the EHWIC E-Series NCE and the NIM E-Series NCE (UCS-EN120E and UCS-EN140N-M2) UCSES.1.5.0.2—Applicable to the single-wide E-Series Server (UCS-E140S-M1) UCSES.1.5.0.7—Applicable to the single-wide E-Series Server (UCS-EN120S-M2 and UCS-E140S-M2) UCSED.2.5.0.5—Applicable to the double-wide E-Series Servers (UCS-E140D-M1, UCS-E160D-M1, UCS-E160D-M2 and UCS-E180D-M2) UCSEM3.2.5—Applicable to the single-wide E-Series Server (UCS-E160S-M3) UCSEDM3.2.5—Applicable to the single-wide E-Series Server (UCS-E180D-M3 and UCS-E1120D-M3)

Understanding the HUU User Interface

Figure 39: HUU User Interface



User Interface Name	Description
Id column	Displays the serial number of the component row.
Component column	Lists the firmware components that are available for upgrade.
PCI Slot column	Display the PCI slot information for the PCI adapter components.
Current Version column	Displays the current firmware version number that is installed for each of the listed components.
Update Version column	Displays the firmware version number that is available for upgrade for each of the listed components.
Update Status column	Displays the status of the update for each of the listed components while the update is in progress.
Update button	Initiates the firmware update for a selected component.
Update All button	Initiates the firmware update for all available components.

User Interface Name	Description
Save Logs button	Saves the log files. If an error occurs while updating the firmware, you are prompted to save the error log. Click the **Save Logs** button to save the error logs to an externally connected USB. This log can be used to identify the cause of the error and for troubleshooting.
Last Update Verify button	Verifies if the update was successful. **Note** You must first reboot HUU by clicking the **Exit** button, and then click the **Last Update Verify** button to verify the last update.
Restore CIMC Defaults button	Restores the CIMC settings to factory default settings.
Exit button	Exits the HUU. Click **Yes** at the confirmation prompt to exit. • If you update the CIMC and not the BIOS, when you click the **Exit** button, the CIMC will get activated but you will lose connectivity to the CIMC and KVM. • If you select LOM for update and you are in shared LOM mode, when you click the **Exit** button, you will lose connectivity to the CIMC and KVM.
Usage area	Lists keyboard shortcuts that you can use to perform specific tasks.
Current Activity area	Provides the status of an update.
Execution Logs area	Provides a log of activities and their status while an update is in progress.

Upgrading the Firmware

Basic Workflow for Using the HUU

1. Download the HUU ISO image from Cisco.com.
2. Use the KVM console or the CIMC CLI to map the HUU ISO image.
3. Set the boot order to make the virtual CD/DVD drive as the boot device.
4. From the HUU GUI, select all or specific firmware components to update.
5. After the firmware updates, click **Exit** to reboot the HUU.

6. Unmap the HUU ISO image.
7. Reboot the server.

Upgrading the Firmware Using the HUU

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 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 **Servers—Unified Computing**.

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.

Step 9 Click **Unified Computing System (UCSE) Server Firmware**.

Step 10 Click the **Download** button associated with the **Cisco UCS Host Upgrade Utility** ISO image to download the image onto your PC.

The **End User License Agreement** dialog box appears.

Step 11 Click **Accept License Agreement**.

Step 12 The **Opening** *ucse-server-platform-huu***.iso** dialog box appears.

Either open the file or browse to the location where you want to save the HUU ISO image, and then click **OK**.

Step 13 You can use either the KVM Console or the CIMC CLI to map the HUU ISO image:

- To use the KVM Console, do the following:
  a. Use a browser to connect to the CIMC GUI on the server that you are upgrading.
  b. In the address field of the browser, enter the CIMC IP address for that server, and then enter your username and password to log in to the CIMC GUI.
  c. Click the **Launch KVM Console** icon on the toolbar. The KVM Console opens in a separate window.
  d. From the KVM Console, click the **Virtual Media** tab.
  e. Click **Add Image**, navigate to and select the Host Upgrade Utility ISO image, and then click **Open** to mount the image.

f. In the **Client View** area, in the Mapped column, check the check box for the mounted ISO image.

- To use the CIMC CLI, download the ISO image on to an FTP or TFTP server, and then use the following commands:

  a. Server# **scope host-image-mapping**.

  b. Server/host-image-mapping # **download-image** *protocol server-ip-address huu-ISO-filename*

  c. Server/host-image-mapping # **map-image** *huu-ISO-filename*.

```
Server# scope host-image-mapping
Server/host-image-mapping # download-image ftp 10.20.34.56 2.1.1.iso
Username: anonymous
Password:
Image download has started.
Please check the status using "show detail".
Server/host-image-mapping # map-image 2.1.1.iso
```

Step 14 After the image is mapped, set the boot order to make the virtual CD/DVD drive as the boot device.

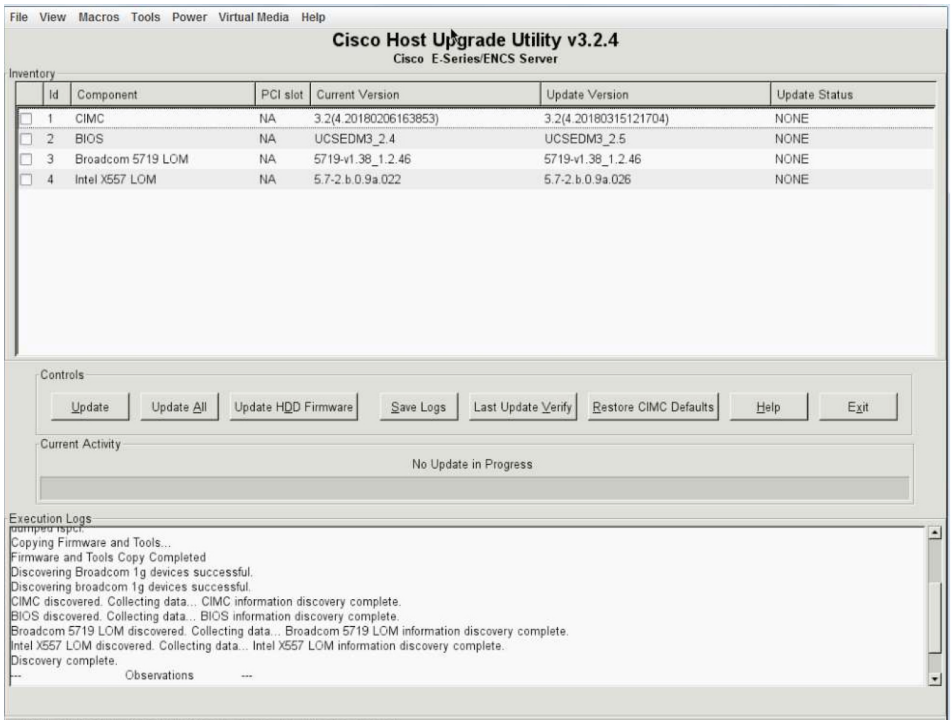
Step 15 Reboot the server.

Step 16 From the CIMC GUI, click the **Launch KVM Console** icon on the toolbar.

The HUU and the **Cisco Software License Agreement** page appears.

Step 17 Click **I Agree** to accept the licensing terms and conditions.

The **Cisco Host Upgrade Utility** GUI appears with a list of components that are available for update.



Step 18 Do one of the following:

- To update all the listed components, click **Update all**.
- To update specific components, select the components, and then click **Update**.

The status of the update is displayed in the **Update Status** column. To view details about the update status, see the **Execution Logs** area.

Note We recommend that you always update the BIOS and the CIMC firmware at the same time.

Step 19 After the firmware is updated, click **Exit**, and then click **Ok** at the confirmation prompt.

The HUU reboots.

Important
- If the BIOS firmware is selected for update, it will be the last one to update because it requires the host to be powered off. You can check the progress of the BIOS update from the CIMC GUI or CIMC CLI. After the BIOS update completes, you must use the CIMC GUI or the CIMC CLI to manually power on the host.
- If the CIMC firmware is selected for update—after you click the **Exit** button from the HUU GUI—the new CIMC firmware gets automatically activated. However, if both the BIOS and CIMC firmwares are selected for update, the CIMC firmware does not get automatically activated. You must use the CIMC GUI or the CIMC CLI to manually activate the new CIMC firmware.
- When the new CIMC firmware gets activated, you will lose network connectivity to the CIMC GUI, CIMC CLI, and virtual KVM. Also, the mapped HUU ISO image gets unmapped. To run the HUU, you must map the HUU ISO image again.
- When the LOM firmware is updated, you might lose network connectivity to the CIMC GUI and virtual KVM.

Step 20 Unmap the HUU ISO image. Do one of the following:

- From the CIMC GUI, click the **Launch KVM Console** icon on the toolbar, from the Mapped column, check the check box for the mounted HUU ISO image, and then click **Remove Image**.
- From the CIMC CLI, use the **unmap-image** command:
- `Server/host-image-mapping # unmap-image`

Step 21 Reboot the server.

Troubleshooting

Problem	Solution
Connection to the CIMC is lost after an update and reboot, and the KVM session ends.	This is expected behavior after a firmware update. Log back in to the CIMC, and then re-establish your KVM session.

Problem	Solution
Error Message: *PID, Board-Part-Number, Product-Part-Number* is not supported by this HUU image. HUU will not boot on this machine. Press any key to reboot the server.	This error message displays when the HUU ISO image is not supported by the server. To resolve this problem, use the HUU ISO image that is supported by the server. See Minimum CIMC and BIOS Firmware Releases Required to Use HUU, on page 140.
After using the HUU to update the Broadcom NCSI firmware, the warning prompt to update the Broadcom firmware still displays in the CIMC GUI and the CIMC CLI.	To resolve this problem, power cycle the E-Series Server to allow the new Broadcom NCSI firmware to take effect.

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.

Obtaining Software from Cisco Systems

Use this procedure to download BIOS and CIMC firmware.

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 Firmware**—Contains the Host Upgrade Utility.

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.

Upgrading Firmware Manually

You can upgrade the firmware manually, through the browser or from a TFTP server. For details, see the *Firmware Management* chapter in the *GUI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine* or the *CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.

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 "Upgrading Firmware" chapter in the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*. This chapter 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 100.
- Unzip the proper upgrade file to your local machine.

Procedure

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

Step 2 On the **Server** tab, click **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 "Upgrading Firmware" chapter in the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*. This chapter 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 100.
- Unzip the proper upgrade file on your TFTP server.

Procedure

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

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 From the **Actions** area, click **Launch KVM Console**.

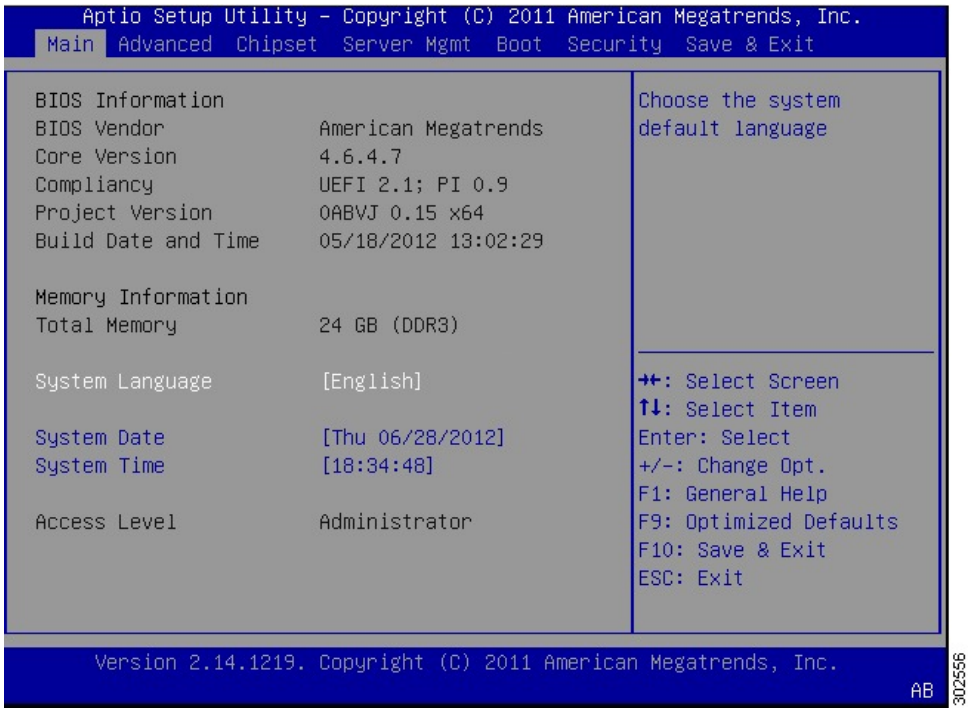
The **KVM Console** opens in a separate window.

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 40: 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** menu.

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 From the **Actions** area, click **Launch KVM Console**.

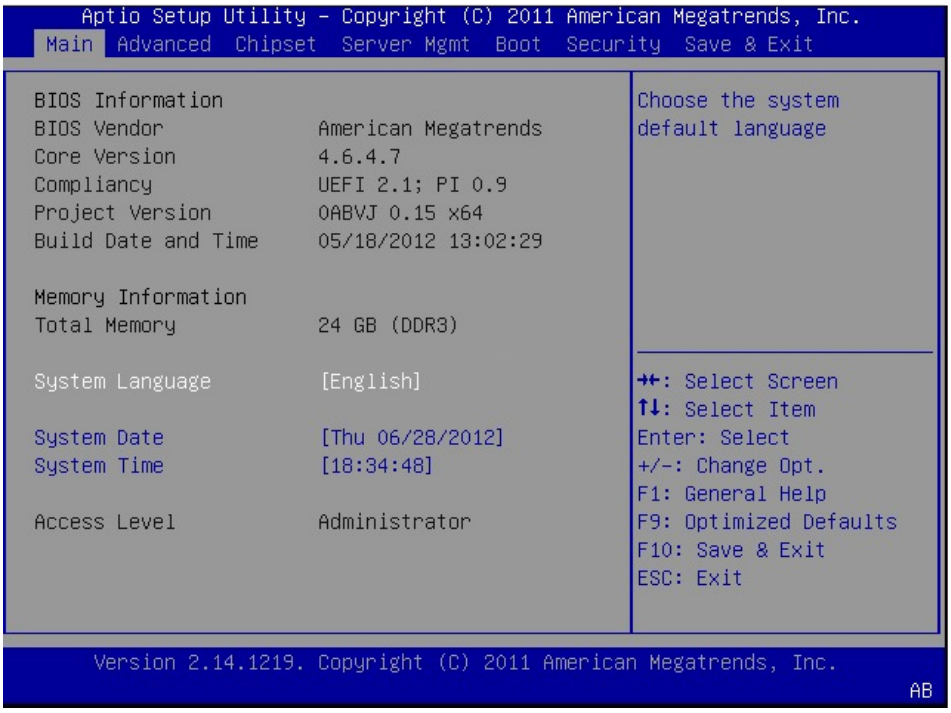
The **KVM Console** opens in a separate window.

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 41: BIOS Setup Menu



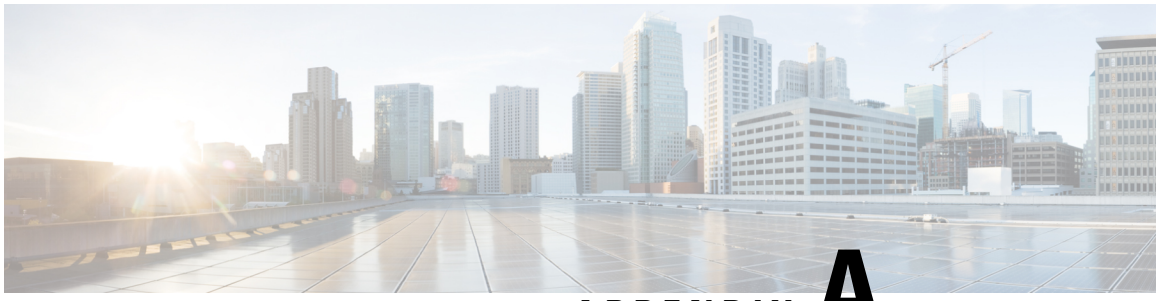
Step 6 To navigate between menu items, use the **right** or **left arrow keys** on your keyboard.

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.



APPENDIX A

Configuration Differences

This appendix includes the following sections:

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

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

Table 7: Differences in Router Configuration Between the Cisco SRE-V and the E-Series Server—Cisco 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 Access to the Management Firmware , on page 23.

  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:

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

Router Configuration Differences Between the Cisco ISR G2 and the Cisco ISR 4000 Series

The examples in the following table provide the key differences between the Cisco ISR G2 configuration and the Cisco ISR 4000 series configuration.

Table 8: Differences in Router Configuration Between the Cisco ISR G2 and the Cisco ISR 4000 Series

Cisco ISR G2 Configuration	Cisco ISR 4000 Series 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 shared-lom console`
	` 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 4000 series, the **interface ucse** *slot*/*port* command is replaced by the **ucse subslot** *slot*/*subslot* and the **interface ucse** *slot*/*subslot*/*port* commands.
- In the Cisco 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 4000 series, you can use either the management interface or one of the NIC interfaces to configure CIMC access. See Configuring Access to the Management Firmware , on page 23.

  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 Cisco ISR G2, you use the **ucse** *slot* **session {imc | host}** command to session into the server.
- In the Cisco ISR 4000 series, you use the **hw-module subslot** *slot*/**0 session {imc | server}** command to session into the server.

Router Configuration Differences Between the E-Series Server and the EHWIC E-Series NCE—Cisco ISR G2

The examples in the following table provide the key differences between the E-Series Server configuration and the EHWIC E-Series NCE configuration.

Table 9: Differences in Router Configuration Between the E-Series Server and the EHWIC E-Series NCE

E-Series Server Configuration	EHWIC E-Series NCE 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 ucse 1/1`
` switchport mode trunk`
 	
`ip route 10.0.0.2 255.255.255.255 ucse 1/0`
	`interface GigabitEthernet0/0`
	` ip address 10.0.0.1 255.0.0.0`
	
	`interface ucse 0/1/0`
	` 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 ucse 0/1/1`
	` switchport mode trunk`
	
	`ip route 10.0.0.2 255.255.255.255 ucse 0/3/0`

Note the following differences:

- In the EHWIC E-Series NCE, the **interface ucse** *slot*/*port* command is replaced by the **interface ucse 0/***subslot*/*port* command.

- In the EHWIC E-Series NCE, the **ip route** *cimc-ip-address subnet-mask* **ucse** *slot*/*port* command is replaced by the **ip route** *cimc-ip-address subnet-mask* **ucse 0**/*subslot*/*port* command.
- In Cisco IOS Release 15.4(3)M, for both the E-Series Servers and NCEs, all **ucse** *slot x* commands are replaced by the **ucse subslot** *slot*/*subslot x* command.

Router Configuration Differences Between the E-Series Server and the NIM E-Series NCE—Cisco ISR 4000 Series

The examples in the following table provide the key differences between the E-Series Server configuration and the NIM E-Series NCE configuration.

Table 10: Differences in Router Configuration Between the E-Series Server and the NIM E-Series NCE

E-Series Server Configuration	NIM E-Series NCE Configuration

`interface GigabitEthernet 0/0/0`
` ip address 10.0.0.1 255.0.0.0`
 	
`ucse subslot 1/0`
` imc access-port shared-lom console`
` 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`
	`interface GigabitEthernet 0/0/0`
	` ip address 10.0.0.1 255.0.0.0`
	
	`ucse subslot 0/1`
	` imc access-port shared-lom console`
	` imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1`
	
	`interface ucse0/1/0`
	` ip unnumbered GigabitEthernet0/0/0`
	` no negotiation auto`
	` switchport mode trunk`
	
	`ip route 10.0.0.2 255.255.255.255 ucse0/1/0`

Note the following differences:

- In the NIM E-Series NCE, the **ucse subslot** *slot*/*port* command is replaced by the **ucse subslot** *port*/*slot* command.
- In the NIM E-Series NCE, the **interface ucse** *slot*/*port*/*subport* command is replaced by the **interface ucse** *port*/*slot*/*subport* command.

The command to session into the server has also changed:

- For the E-Series Server installed in the Cisco ISR 4000 series, you use the **hw-module subslot** *slot*/**0 session {imc | server}** command to session into the E-Series Server.
- For the NIM E-Series NCE installed in the Cisco ISR 4000 series, you use the **hw-module subslot 0**/*slot* **session {imc | server}** command to session into the NIM E-Series NCE.

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.

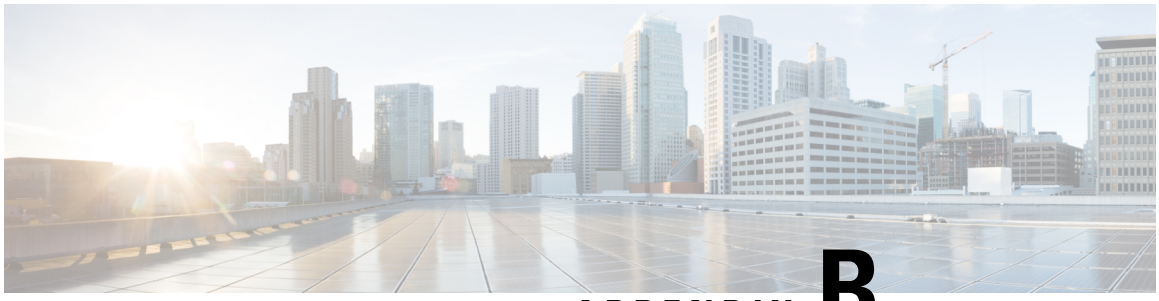
Table 11: Differences in Router Configuration Between the Cisco SRE-V and the E-Series Server—ISR G2

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 103.



APPENDIX B

Cisco IOS Software Command Reference—Cisco ISR G2

This appendix provides the new Cisco IOS commands that were introduced for the E-Series Servers and NCE installed in the Cisco 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 appendix 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 in interface configuration mode. To remove the static IP address, use the **no** form of this command.

imc ip address *ip-address subnet-mask* **default-gateway** *gateway-address*
no imc ip address *ip-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 (config-if)

Command History

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

Usage Guidelines

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

Examples

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 DHCP IP address for CIMC, use the **imc ip address dhcp** command in interface configuration mode. To remove the DHCP IP address, use the **no** form of the this command.

imc ip address dhcp
no imc ip address dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example shows how to configure a 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 in interface configuration mode. To remove the VLAN configuration, use the **no** form of this command.

imc vlan *vlan-number*
no imc vlan *vlan-number*

Syntax Description

vlan-number	IP address of the remote manager.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example shows how to enter 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, use the **ucse cmos-reset** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **cmos-reset**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **cmos-reset**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.

subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

This command sets the BIOS CMOS back to the factory defaults. User changes made in the BIOS will be lost.

Examples

The following example shows how to reset the BIOS CMOS in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

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

Examples

The following example shows how to reset the BIOS CMOS in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 cmos-reset
```

ucse password-reset

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

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

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

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

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

Cisco IOS Software Command Reference—Cisco ISR G2

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
BIOS	Resets the BIOS password.
BMC	Resets the CIMC password.
RAID	Resets the RAID password. **Note** RAID is not applicable for the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series NCE installed in an ISR G2.

Usage Guidelines

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

RAID is not applicable for the EHWIC E-Series NCE.

Examples

The following example shows how to reset the BIOS password in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 password-reset BIOS

Reset command sent
```

Examples

The following example shows how to reset the BIOS password in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 password-reset BIOS

Reset command sent
```

ucse session

To start or close a host or CIMC session, use the **ucse session** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

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

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

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

Note The **ucse** *slot* **session imc** command will work only if you have configured a router-side IP address (for instance, ip unnumbered GigabitEthernet0/0) on the interface.

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
imc	Starts a session with CIMC.
imc clear	Closes the existing CIMC session.
host	Starts a session with the host Cisco E-Series Server.
host clear	Closes the host Cisco E-Series Server session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

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.

Examples

The following example shows how to clear the CIMC session in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 session imc clear
```

Examples

The following example shows how to clear the CIMC session in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 session imc clear
```

ucse shutdown

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

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **shutdown**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **shutdown**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.

Release	Modification
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

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

Examples

The following example shows how to gracefully shut down an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 shutdown
```

Examples

The following example shows how to gracefully shut down an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 shutdown
```

ucse statistics

To display or clear the reset and reload server information, use the **ucse statistics** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **statistics [clear]**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **statistics [clear]**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
clear	(Optional) Clears the E-Series Server's reset and reload information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to display the server statistics in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
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
```

Examples

The following example shows how to display the server statistics in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 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 of a server, use the **ucse status** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

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

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **status** [**detailed**]

Cisco IOS Software Command Reference—Cisco ISR G2

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
detailed	(Optional) 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 (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to display server status in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
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
```

Examples

The following example shows how to display server status in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 status

Service Module is Cisco ucse 0/3
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 immediately power down the server, use the **ucse stop** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **stop**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **stop**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to power down an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 stop

Send server stop command
```

Examples

The following example shows how to power down an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 stop

Send server stop command
```

Installation Commands

Commands	Description
ucse *slot* **imc config {restore | save}** *url*	Saves the CIMC configuration to a file on the router's flash drive or restores the CIMC configuration from a file on the router's flash drive. • *slot*—Router slot number in which the E-Series Server is installed. • **restore**—Restores the CIMC configuration from a file. • **save**—Saves the CIMC configuration to a file. • *url*—The url where the configuration file is located.
ucse *slot* **imc file delete** *file_name*	Deletes the CIMC image file. The file must have .iso as the file extension. • *slot*—Router slot number in which the E-Series Server is installed. • *file_name*—Name of the CIMC image file to delete. **Note** The name of the file must exactly match the name of the file as displayed by the output of the **show ucse** *slot* **imc files** command.
ucse *slot* **imc file download {URL***url* **| abort}**	Downloads the CIMC image file in the background to an internal storage device. The file must have .iso as the file extension. • *slot*—Router slot number in which the E-Series Server is installed. • *url*—Downloads the file from the specified location. • **abort**—Aborts the file download operation.
imc config file *file_name*	Stores the CIMC configuration file into the running configuration. • *file_name*—The name of the CIMC configuration file that you want to store.
show ucse *slot* **imc download progress**	Displays the status of the CIMC firmware download. • *slot*—Router slot number in which the E-Series Server is installed.
show ucse *slot* **imc files**	Displays the CIMC installable images that are available on the local file system. • *slot*—Router slot number in which the E-Series Server is installed.

Password Reset Command

Session Command

IP Address Configuration Commands

CIMC Access Commands

VLAN Command

Commands	Description
imc vlan *vlan_number*	Enters VLAN configuration mode for the specified VLAN.
no imc vlan	The **no** command removes the configuration.

Reload, Reset, Start, Stop, Shutdown Commands

RAID Commands

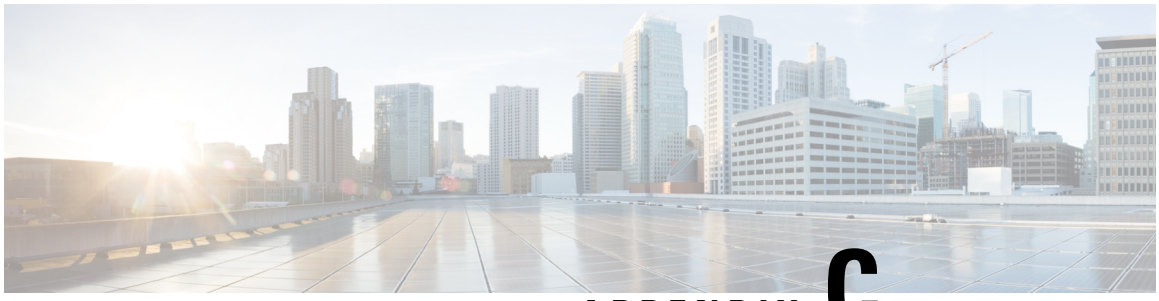
Commands	Description
ucse *slot* **server raid level {0 | 1 | 5 | NONE} [use** *hard_drive_list***}**	Configures the specified RAID level on the E-Series Server. • *slot*—Router slot number in which the E-Series Server is installed. • **0**—Data is stored evenly in stripe blocks across two or more disks without redundancy (mirroring). **1**—Data is stored in mirrored set of disk drives with an optional hot spare disk drive. **5**—Data is stored in stripe blocks with parity data staggered across all disk drives. **NONE**—Disk drives of a computer are not configured as RAID and are put in a JBOD configuration. • **use** *hard_drive_list*— Allows you to specify the hard disk drives (HDD) on which you want to configure RAID. Enter the list of HDDs in a comma-separated list, such as HDD1, HDD2, HDD3. This command only applies to the internal hard drives, which are named according to their physical location. If you do not use the **use** *hard_drive_list* command, the system combines all of the drives into a RAID array. **Note** The names of the hard drives must exactly match the names displayed by the output of the **show ucse** *slot* **server boot devices** command.
show ucse *slot* **server raid level**	Displays the current RAID configuration.

Statistics and Status Commands

Boot Commands

Erase Hard Drive Commands

Commands	Description
ucse *slot* **server erase device hdd {ALL | use** *hard_drive_list***}**	Erases all existing data from the E-Series Server's hard disk drives. • *slot*—Router slot number in which the E-Series Server is installed. • *hard_drive_list*—Erases the data from the specified hard disk drives. **Note** The names of the hard disk drives must exactly match the names displayed by the output of the **show ucse** *slot* **server boot devices** command.
show ucse *slot* **server erase device status**	Displays the status of devices that are erased.



APPENDIX C

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

This chapter provides the new Cisco IOS commands that were introduced for the E-Series Servers installed in the Cisco ISR 4000 series.

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 appendix includes the following sections:

debug platform software ucse

To debug the Cisco UCS E-Series Server 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.

Examples

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) session or host server module session, use the **hw-module subslot session** command in privileged EXEC mode.

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

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot 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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 series.

Usage Guidelines

Only one active session is allowed on the CIMC or server module at any time.

Examples

The following example shows how to start a CIMC session in an E-Series Server installed in a Cisco ISR 4000 series:

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

The following example shows how to start a server module session in an E-Series Server installed in a Cisco ISR 4000 series:

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

imc ip dhcp

To configure a DHCP IP address for the Cisco Integrated Management Controller (CIMC), use the **imc ip dhcp** command in UCSE configuration mode. To remove the DHCP 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).

Examples

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.
```

platform switchport

To enable the Switch Virtual Interface (SVI) configuration on a UCS E series server, use the **platform switchport svi** command in privileged EXEC mode. To disable the configuration, use the **no** form of this command.

platform switchport *ucse interface* **svi**

Syntax Description

ucse interface	Number of the UCSE interface. For Cisco UCS E-Series Servers, the UCSE interface number can be 0 or 1.

Command Modes

UCSE Config Mode (config-ucse)#

Command History

Release	Modification
Cisco IOS XE Release 3.15S	This command was introduced on Cisco ISR4000 Series Routers.

Usage Guidelines

Enabling or disabling the SVI configuration on a UCS-E subslot interface requires a module OIR or router reload after you save the configuration.

Examples

Before you use this command, you have to set the spanning tree mode. The following example shows how to set the spanning tree mode:

```
spanning-tree vlan 1-4094 priority 24576
```

The following example shows how to enable Switch Virtual Interface (SVI) configuration on a UCS E series server:

```
ISR4k(config-ucse)#platform switchport 1 svi
Ena/Dis SVI on UCSE needs a OIR or Router reload
```

Examples

After you use this command, the UCS-E interface shows up in the show spanning-tree command output:

```
SR4451-1#show spanning-tree

G0:VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
             Address     f07f.06bc.c0b1
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     f07f.06bc.c0b1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
uc1/0/0             Desg FWD 4         128.257  P2p
uc1/0/1             Desg FWD 4         128.258  P2p


G0:VLAN0003
  Spanning tree enabled protocol rstp
  Root ID    Priority    24579
             Address     f07f.06bc.c0b1
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24579  (priority 24576 sys-id-ext 3)
             Address     f07f.06bc.c0b1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
uc1/0/0             Desg FWD 4         128.257  P2p
uc1/0/1             Desg FWD 4         128.258  P2p

ISR4451-1#
```

show interfaces ucse

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

show interfaces ucse *slot/subslot/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. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot 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.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example provides sample output from the **show interfaces ucse** *slot*/**0/0 switchport** command in an E-Series Server installed in a Cisco ISR 4000 series:

```
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/subslot* **imc password-reset**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot 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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

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

Examples

The following example shows how to reset the CIMC password in an E-Series Server installed in a Cisco ISR 4000 series:

```
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/subslot* **server** {**reload** | **reset** | **start** | **stop**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
reload	Powers down the server module and then powers it on. **Note** The **reload** keyword is not supported on the NIM E-Series-NCE. Instead, we recommend that you use the following commands from the router: **1.** Router # **ucse subslot** *slot/subslot* **shutdown** **2.** Router # **ucse subslot** *slot/subslot* **start** If a reload is necessary, use the following command: Router # **hw-module subslot 0/***NIM-slot-number* **reload** **Note** This command power-cycles the module. The CIMC and server reboot.
reset	Resets the hardware on the server module.
start	Powers on the server module.
stop	Immediately powers down the server module. **Note** The **stop** keyword is not supported on the NIM E-Series-NCE. Instead, we recommend that you use the following command from the router: Router # **ucse subslot** *slot/subslot* **shutdown** If it is necessary to do an immediate power down of the server, use the following command: Router # **hw-module subslot 0/***NIM-slot-number* **stop** **Note** This command powers down the module. The CIMC and server power off.

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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

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.

Examples

The following example shows how to reload the E-Series Server installed in a Cisco ISR 4000 series:

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

The following example shows how to reset the E-Series Server installed in a Cisco ISR 4000 series:

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

The following example shows how to start the E-Series Server installed in a Cisco ISR 4000 series:

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

The following example shows how to stop the E-Series Server installed in a Cisco ISR 4000 series:

```
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/subslot* **server password-reset** {**BIOS** | **RAID**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
BIOS	Resets the BIOS password.
RAID	Resets the RAID password. **Note** RAID is not supported on the NIM E-Series NCE.

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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

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.

Examples

The following example shows how to reset the BIOS password in an E-Series Server installed in a Cisco ISR 4000 series:

```
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 in an E-Series Server installed in a Cisco ISR 4000 series:

```
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/subslot* **shutdown**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot 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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

The NIM E-Series NCE might take up to 60 seconds to shut down. After two or three shut down attempts, if the NIM E-Series NCE does not shut down, enter the following commands from the router:

1. Router # **hw-module subslot 0/***NIM-slot-number* **stop**
2. Router # **hw-module subslot 0/***NIM-slot-number* **start**

Examples

The following example shows how to shut down an E-Series Server installed in a Cisco ISR 4000 series:

```
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/subslot* **statistics** [**clear**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.

subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot 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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example shows how to display the statistics of an E-Series Server:

```
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*/*subslot* **status** [**detailed**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example shows how to display the status of an E-Series Server:

```
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
```

Commands Modified to Support Cisco ISR 4451-X

imc access-port

To configure Cisco Integrated Management Controller (CIMC) access through the server module's dedicated, management, or host ports, use the **imc access-port** command in interface configuration mode or UCSE configuration mode.

Cisco UCS E-Series Server Installed in Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X
imc access-port {**dedicated** | **shared-lom** [{**GE1** | **GE2** | **GE3** | **console** | **failover** [*option*]}]}
no imc access-port {**dedicated** | **shared-lom** [{**GE1** | **GE2** | **GE3** | **console** | **failover** [*option*]}]}

Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S
imc access-port {**MGMT** | [{**GE0** | **GE1** | **GE2** | **GE3**[*failover-option*]}]}
no imc access-port {**MGMT** | [{**GE0** | **GE1** | **GE2** | **GE3**[*failover-option*]}]}

Syntax Description

Table 12: Cisco UCS E-Series Server Installed in Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X

dedicated	Configures CIMC access using the IMC dedicated port.
shared-lom	Configures CIMC access using one of the following host ports: • **GE1** • **GE2** • **GE3** • **console** • **failover** **Note** If you enter **failover**, you must also enter one additional parameter: • **GE1 GE1** [**GE2**] | [**GE3**] [**GE2 GE3**] • **GE2 GE2 GE3**

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

Table 13: Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S

MGMT	Configures CIMC access using the Cisco UCS E-Series Server's management port.
GE0, **GE1**, **GE2**, **GE3**	(Optional) Configures CIMC access using one of the following NIC interfaces: • **GE0**—Cisco UCS E-Series Server's internal NIC interface connecting to the router's UCSE *slot*/**0/0** interface. • **GE1**—Cisco UCS E-Series Server's internal NIC interface connecting to the router's UCSE *slot*/**0/1** interface. • **GE2**—Cisco UCS E-Series Server's external NIC interface. • **GE3**—Cisco UCS E-Series Server's external NIC interface. Applicable to double-wide Cisco UCS E-Series Servers. • *failover-option*—To configure failover, enter one additional parameter: • **GE2 backplane**—Applicable to single-wide and double-wide Cisco UCS E-Series Servers. • **GE3 backplane**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE2 GE3**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE3 GE2**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE2 GE3 backplane**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE3 GE2 backplane**—Applicable to double-wide Cisco UCS E-Series Servers.

Command Modes

Interface configuration (config-if) for a Cisco UCS E-Series Server installed in Cisco 2900 and 3900 ISR G2.

UCSE configuration (config-ucse) for a Cisco UCS E-Series Server installed in the Cisco ISR 4451-X.

Command History

Release	Modification
Cisco IOS Release 15.2(4)M	This command was introduced on the Cisco UCS E-Series Servers installed in Cisco 2900 and 3900 Series Integrated Services Routers (ISR G2).
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4451-X Integrated Services Router (Cisco ISR 4451-X).
Cisco IOS XE Release 3.10S	This command was modified so that all platforms—Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X—use the same command.

Usage Guidelines

If the Cisco UCS E-Series Server is installed in Cisco 2900 and 3900 ISR G2, use the **imc access-port** command in interface configuration mode:

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

If the Cisco UCS E-Series Server is installed in Cisco ISR 4451-X, use the **imc access port** command in UCSE configuration mode:

```
Router(config)# ucse subslot 1/0
Router(config-ucse)#
```

Examples

The following example shows how to configure CIMC access using the dedicated port:

```
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 dedicated
Router(config-if)# no shut
Router(config-if)# end
```

Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S

The following example shows how to configure CIMC access using the MGMT port:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ucse subslot 1/0
Router(config-ucse)# imc access-port mgmt
Router(config-ucse)#
 IMC ACK: Access ports received: MGMT

 IMC ACK: UCSE access port operation successful.
```

switchport

Cisco 3550, 4000, and 4500 Series Switches

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface into Layer 3 mode, use the **no** form of this command.

switchport
no switchport

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without keywords). Use the **no** form of this command (without keywords) to return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased. Use the **switchport** commands (with keywords) to configure the switching characteristics.

switchport
switchport {**host** | **nonegotiate**}

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

no switchport
no switchport nonegotiate

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

To configure the server module to communicate with the router over a high-speed Multi Gigabit Fabric (MGF) backplane switch port, use the **switchport** command (with keywords) in interface configuration mode.

switchport {**access** | **mode** | **trunk**}

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

To configure the flex Layer 2 and Layer 3 ports to Layer 2 interface, use the **switchport** command (without keywords). To configure to Layer 3 interface, use the **no switchport** command (without keywords).

switchport
no switchport

Syntax Description

Cisco 3550, 4000, and 4500 Series Switches

This command has no arguments or keywords.

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

Table 14: Syntax Description for Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

host	Optimizes the port configuration for a host connection.
nonegotiate	Specifies that the device will not engage in negotiation protocol on this interface.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Table 15: Syntax Description for Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets the access mode characteristics of the interface.
mode	Sets the interface type: Access or Trunk.
trunk	Sets trunk characteristics when the interface is in Trunk mode. This is the default mode.

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

This command has no arguments or keywords.

Command Default

Cisco 3550, 4000, and 4500 Series Switches

All interfaces are in Layer 2 mode.

Catalyst 6500/6000 Series Switches and 7600 Series Routers

The default access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

The last two ports of the front-panel switch ports (flex ports) are set to Layer 2 interface by default.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
15.1(2)T	Support for IPv6 was added.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).
Cisco IOS XE Release 17.11.1a	This command was implemented to provide flex support on the last two Layer 2 switch ports of the Cisco 1000 Series ISRs with 4 or 8 Front-Panel Switch Ports.

Usage Guidelines

Cisco 3550, 4000, and 4500 Series Switches

Use the **no switchport** command to put the interface into the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port. Entering the **no switchport** command shuts down the port and then reenables it, which might generate messages on the device to which the port is connected.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access, enables spanning tree PortFast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning-tree PortFast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other Cisco 7600 series routers, hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

The no form of the **switchport** nonegotiate command removes nonegotiate status.

When using the **nonegotiate** keyword, Dynamic Inter-Switch Link Protocol and Dynamic Trunking Protocol (DISL/DTP)-negotiation packets are not sent on the interface. The device trunks or does not trunk according to the mode parameter given: access or trunk. This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

You must force a port to trunk before you can configure it as a SPAN-destination port. Use the **switchport nonegotiate** command to force the port to trunk.

Examples

Cisco 3550, 4000, and 4500 Series Switches

The following example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed (Layer 3) port:

```
Router(config-if)#no switchport
```

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

The following example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

```
Router(config-if)#
switchport
Router(config-if)#
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to optimize the port configuration for a host connection:

```
Router(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Router(config-if)#
```

This example shows how to cause a port interface that has already been configured as a switched interface to refrain from negotiating trunking mode and act as a trunk or access port (depending on the mode set):

```
Router(config-if)#
switchport nonegotiate
Router(config-if)#
```

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

The following example shows how to cause an interface to cease operating as a Cisco-routed port and to convert it into a Layer 2 switched interface:

```
Router(config-if)#
switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed (Layer 3) ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

The following example shows how to convert a flex port to a Layer 3 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.0.1 255.255.255.0
Device(config-if)# exit
```

The following example shows how to convert a flex port to a Layer 2 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# exit
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the current operating configuration.
switchport access vlan	Sets the VLAN when the interface is in Access mode.
switchport mode	Sets the interface type: Access or Trunk

Command	Description
switchport trunk	Sets trunk characteristics when the interface is in Trunk mode.

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchport access vlan** command in interface configuration or template configuration mode. To reset the access-mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

switchport access vlan *vlan-id*
no switchport access vlan

Syntax Description

vlan-id	VLAN to set when the interface is in access mode; valid values are from 1 to 4094. Valid values for Cisco UCS E-Series Servers installed in Cisco 4400 Integrated Services Routers are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2

Command Default

The defaults are as follows:

- Access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

The no form of the **switchport access vlan** command resets the access-mode VLAN to the appropriate default VLAN for the device.

Examples

The following example shows how to stop the port interface from operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Device(config-if)# switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to make a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN in interface configuration mode:

```
Device(config-if)# switchport access vlan 2
```

The following example shows how to make a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN, using an interface template in template configuration mode:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# switchport access vlan 2
Device(config-template)# end
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport mode

To set the interface type, use the **switchport mode** command in interface configuration mode. Use the appropriate **no** form of this command to reset the mode to the appropriate default mode for the device.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
switchport mode {**access** | **trunk**}
no switchport mode

Cisco Catalyst 6500/6000 Series Switches
switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}
no switchport mode

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

Cisco 7600 Series Routers
switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **private-vlan** | **trunk**}
no switchport mode
switchport mode private-vlan {**host** | **promiscuous**}
no switchport mode private-vlan

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers
switchport mode {**access** | **trunk**}
no switchport mode {**access** | **trunk**}

Syntax Description

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
dot1q-tunnel	Sets the trunking mode to TUNNEL unconditionally.
dynamic auto	Sets the interface to convert the link to a trunk link.
dynamic desirable	Sets the interface to actively attempt to convert the link to a trunk link.
private vlan host	Specifies that the ports with a valid private VLAN (PVLAN) association become active host private VLAN ports.
private vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.

Table 16: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.

Command Default

The default is **access** mode.

The default mode is dependent on the platform; it should be either **dynamic auto** for platforms that are intended as wiring closets or **dynamic desirable** for platforms that are intended as backbone switches. The default for PVLAN ports is that no mode is set.

The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamic auto** for platforms that are intended for wiring closets or **dynamic desirable** for platforms that are intended as backbone switches.
- No mode is set for PVLAN ports.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Cisco Catalyst 6000 family switches.
12.1(1)E	This command was integrated on the Cisco Catalyst 6000 family switches.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

Release	Modification
12.1(8a)EX	The switchport mode **private-vlan** {**host** | **promiscuous**} syntax was added.
12.2(2)XT	Creation of switchports became available on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for creation of switchports on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

If you enter a forced mode, the interface does not negotiate the link to the neighboring interface. Ensure that the interface ends match.

The **no** form of the command is not supported on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you configure a port as a promiscuous or host-PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a SPAN destination.

If you delete a private-port PVLAN association or mapping, or if you configure a private port as a SPAN destination, the deleted private-port PVLAN association or mapping or the private port that is configured as a SPAN destination becomes inactive.

If you enter **dot1q-tunnel** mode, PortFast Bridge Protocol Data Unit (BPDU) filtering is enabled and Cisco Discovery Protocol (CDP) is disabled on protocol-tunneled interfaces.

Examples

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode trunk
```

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

The following example shows how to set the interface to dynamic desirable mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dynamic desirable
```

The following example shows how to set a port to PVLAN-host mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan host
```

The following example shows how to set a port to PVLAN-promiscuous mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan promiscuous
```

Integrated Series Routers Generation 2 (ISR G2) Platforms with EHWIC-4/8ESG

The following example shows how to configure tunneling on port 4/1 and verify the configuration:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# end
```

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show dot1q-tunnel	Displays a list of 802.1Q tunnel-enabled ports.
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays trunk information.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private vlan host association	Defines a PVLAN association for an isolated or community port.
switchport private vlan mapping	Defines the PVLAN mapping for a promiscuous port.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
switchport trunk {**encapsulation dot1q** | **native vlan** | **allowed vlan**}
no switchport trunk {**encapsulation dot1q** | **native vlan** | **allowed vlan**}

Cisco 7600 Series Routers and Catalyst 6500 Series Switches
{**switchport trunk encapsulation** {**isl** | **dot1q** [**ethertype** *value*] | **negotiate**} | **native vlan** {**tag***vlan-id*} | **allowed vlan** *vlan-list* | **pruning vlan** *vlan-list*}
no switchport trunk {**encapsulation** {**isl** | **dot1q** [**ethertype** *value*] | **negotiate**} | **native vlan** [**tag**] | **allowed vlan** | **pruning vlan**}

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers
switchport trunk {**native vlan** *vlan-id* | **allowed vlan** *vlan-list*}
no switchport trunk {**native vlan** *vlan-id* | **allowed vlan** *vlan-list*}

Syntax Description

encapsulation isl	Sets the trunk encapsulation format to Inter-Switch Link (ISL).
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
native vlan	Sets the native VLAN for the trunk in 802.1Q trunking mode.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

allowed vlan *vlan list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
ethertype *value*	(Optional) Sets the EtherType value; valid values are from 0x0 to 0x5EF-0xFFFF.
encapsulation negotiate	Specifies that if the Dynamic Inter-Switch Link (DISL) protocol and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan tag	Enables the native VLAN tagging state on the interface.
native vlan *vlan id*	The particular native VLAN.
pruning vlan *vlan list*	Sets the list of VLANs that are enabled for VLAN Trunking Protocol (VTP) pruning when the interface is in trunking mode. See the "Usage Guidelines" section for the *vlanlist*argument formatting guidelines.

Table 17: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

native vlan *vlan-id*	The particular native VLAN. Valid values are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2
allowed vlan *vlan-list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode. **Note** For *vlan-list* format, see **Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers** section under **Usage Guidelines**.

Command Default

- The default encapsulation type is dot1q.
- The default access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.
- The encapsulation type is dependent on the platform or interface hardware.
- The access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.
- **ethertype** *value* for 802.1Q encapsulation is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6500 series switches.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

Release	Modification
12.1(1)E	Switchport creation on Catalyst 6500 series switches was added.
12.2(2)XT	This command was introduced to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switch port creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX to support the Supervisor Engine 720 on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.2(17a)SX	This command was modified to include the following: • Restriction of ISL trunk-encapsulation. • Addition of the **dot1q** keyword and **ethertype***value* keyword and argument.
12.2(17d)SXB	Support for the Supervisor Engine 2 on the Cisco 7600 series routers and Catalyst 6500 series switches was added.
12.2(18)SXD	This command was modified to allow the **switchport trunk allowed vlan**command to be entered on interfaces where the span destination port is either a trunk or an access port.
12.2(18)SXE	This command added a restriction that Gigabit Ethernet (GE) Optimized Layer 2 WAN ports are not supported on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs from 1 to 4094 for specified platforms.
12.2(33)SXH	This command was changed as follows: • Allowed the tagging of native VLAN traffic on a per-port basis. • Introduced on the Supervisor Engine 720-10GE.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

802.1Q Trunks

- When you connect Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. Cisco recommends that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every

VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.

- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree bridge protocol data units (BPDUs) on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Shared Spanning Tree Protocol (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- The 802.1Q switches that are not Cisco switches maintain only a single instance of spanning-tree (Mono Spanning Tree [MST]) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a switch through an 802.1Q trunk without a Cisco switch, the MST of the switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as the Common Spanning Tree (CST).
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, switches that are not Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the 802.1Q cloud receive these flooded BPDUs. This condition allows Cisco switches to maintain a per-VLAN spanning-tree topology across a cloud of 802.1Q switches that are not Cisco switches. The 802.1Q cloud of switches separating the Cisco switches is treated as a single broadcast segment among all switches connected to the 802.1Q cloud of switches that are not Cisco switches through 802.1Q trunks.
- Make sure that the native VLAN is the same on *all* of the 802.1Q trunks that connect the Cisco switches to the 802.1Q cloud of switches that are not Cisco switches.
- If you are connecting multiple Cisco switches to a 802.1Q cloud of switches that are not Cisco switches, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to an 802.1Q cloud of switches that are not Cisco switches through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning-tree “port inconsistent” state and no traffic will pass through the port.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support 802.1Q formats.

The *vlanlist* format is **all** | **none** | **add** | **remove** | **except***vlanlist*[,*vlanlist*...] where:

- **all** --Specifies all VLANs from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.
- **none** --Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** form of the command.
- **add** --Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** --Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except** --Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan list*-- Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

This command is not supported on GE Layer 2 WAN ports.

You can enter the **switchport trunk** command only on the PO. If you enter the **switchport trunk** command on a port member the following message is displayed:

```
Configuration is not allowed on Port members. Remove the interface from the Port Channel
to modify its config
```

The **switchport trunk encapsulation dot1q**command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats. Only 802.1Q encapsulation is supported by shared port adapters (SPAs).

If you enter the **switchport trunk encapsulation isl** command on a port channel containing an interface that does not support ISL-trunk encapsulation, the command is rejected.

You can enter the **switchport trunk allowed vlan** command on interfaces where the span destination port is either a trunk or an access port.

You can enter the **switchport trunk native vlan tag** command to enable the tagging of native VLAN traffic on a per-port basis. When tagging is enabled, all the packets on the native VLAN are tagged and all incoming untagged data packets are dropped, but untagged control packets are accepted. When tagging is disabled, the native VLAN packets going out on trunk ports are not tagged and the incoming untagged packets are allowed and assigned to the native VLAN. The **no switchport trunknative vlan tag** command overrides the **vlan dot1q tag native** command for global tagging.

Note The **switchport trunk native vlan tag** interface configuration mode command does not enable native VLAN tagging unless you first configure the switch to tag native VLAN traffic globally. To enable native VLAN tagging globally, use the **vlan dot1q tag native** command in global configuration mode.

Note The **switchport trunk pruning vlan** *vlan-list* command does not support extended-range VLANs; valid *vlan-list* values are from 1 to 1005.

The **dot1q ethertype** *value* keyword and argument are not supported on port-channel interfaces. You can enter the command on the individual port interface only. Also, you can configure the ports in a channel group to have different EtherType configurations.

Caution Be careful when configuring the custom EtherType value on a port. If you enter the **negotiate** keyword and DISL and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, then ISL is the selected format and may pose as a security risk. The **no** form of this command resets the trunk-encapsulation format to the default.

- The **no** form of the **switchport trunk native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.
- The **no** form of the **switchport trunk native vlan tag** command configures the Layer 2 port not to tag native VLAN traffic.
- The **no** form of the **switchport trunk allowed vlan** command resets the list to the default list, which allows all VLANs.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

- The **no** form of the **switchport trunk pruning vlan**command resets the list to the default list, which enables all VLANs for VTP pruning.
- The **no** form of the **switchport trunk encapsulation dot1qethertype***value* command resets the list to the default value.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** [*vlan-list*[**,***vlan-list*...]] where:

- **all** --Specifies all the appropriate VLANs. This keyword is not supported in the **switchporttrunkpruningvlan** command.
- **none** --Indicates an empty list. This keyword is not supported in the **switchporttrunkallowedvlan** command.
- **add** *vlan-list* **,** *vlan-list...*]-- Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** *vlan-list* **,** *vlan-list...*]-- Removes the defined list of VLANs from those currently set instead of replacing the list. You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic (for example, Cisco Discovery Protocol, version 3; VTP; Port Aggregation Protocol, version 4 (PAgP4); and DTP) in VLAN 1.

Note You can remove any of the default VLANs (1002 to 1005) from a trunk; this action is not allowed in earlier releases.

- **except** *vlan-list* **,** *vlan-list...*] --Excludes the specified list of VLANs from those currently set instead of replacing the list.
- *vlan-list* **,** *vlan-list...* -- Specifies a single VLAN number from 1 to 4094 or a continuous range of VLANs that are described by two VLAN numbers from 1 to 4094. You can specify multiple VLAN numbers or ranges of numbers using a comma-separated list.

To specify a range of VLANs, enter the smaller VLAN number first, separated by a hyphen and the larger VLAN number at the end of the range.

Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Cisco 7600 series router running the Cisco IOS software on both the supervisor engine and the Multilayer Switch Feature Card (MSFC) to a Cisco 7600 series router running the Catalyst operating system. These VLANs are reserved in Cisco 7600 series routers running the Catalyst operating system. If enabled, Cisco 7600 series routers running the Catalyst operating system may disable the ports if a trunking channel is between these systems.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Note To set trunk characteristics, the interface must be in trunk mode.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** | **WORD**, where:

- **all**—Specifies all VLANs: 1-2349—VLAN IDs in range 1; and 2450-4095—VLAN IDs in range 2.
- **none**—Indicates an empty list.
- **add**—Adds the defined list of VLANs to those currently set instead of replacing the list.

Cisco IOS Software Command Reference—Cisco ISR 4000 Series

- **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- **WORD**—Is either a single VLAN number from 1 to 4095 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Examples

The following example shows how to cause a port interface configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

Router(config-if)# switchport trunk encapsulation dot1q

The following example shows how to configure the Layer 2 port to tag native VLAN traffic:

```
Router(config-if)#
switchport trunk native vlan tag
```

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Note To set trunk characteristics, the interface must be in trunk mode.

The following example shows how to allow trunking on specified VLANs:

```
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 1-2,40,60,1002-1005
```

Related Commands

Command	Description
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

INDEX

F

H

I

K

L

M

N

O

P

Q

R

S

U

V