Cisco 4000 Series ISRs Software Configuration Guide

Last Modified: March 31, 2015

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

Text Part Number: OL-29328-03

© 2015–2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 10

CHAPTER 11

CHAPTER 12

CHAPTER 13

Preface

This section briefly describes the objectives of this document and provides links to additional information on related products and services:

Objectives

This guide provides an overview of the Cisco 4000 Series Integrated Services Routers (ISRs) and explains how to configure the various features on these routers.

The structure of this document is explained in Overview, on page 3.

Important Information on Features and Commands

For more information about Cisco IOS XE software, including features available on the router (described in configuration guides), see the Cisco IOS XE 3S Software Documentation set. In addition to the features described in the Cisco IOS XE 3S Configuration Guides, there also separate configuration guides for features such as *No Service Password Recovery*, *Multilink PPP Support*, and *Network Synchronization*. See the Configuration Guides for the Cisco ISR 4400 Series.

To verify support for specific features, use Cisco Feature Navigator. For more information about this, see Using Cisco Feature Navigator, on page 23.

To find reference information for a specific Cisco IOS XE command, see the Cisco IOS Master Command List, All Releases.

Related Documentation

- Documentation Roadmap for the Cisco 4400 Series Integrated Services Routers
- Release Notes for the Cisco 4400 Series Integrated Services Routers

Commands

Cisco IOS XE commands are identical in look, feel, and usage to Cisco IOS commands on most platforms. To find reference information for a specific Cisco IOS XE command, see the Cisco IOS Master Command List, All Releases document.

Features

The router runs Cisco IOS XE software which is used on multiple platforms. For more information on the available software features, see the configuration guides on the Cisco IOS XE 3S Software Documentation page.

In addition to the features in the Cisco IOS XE 3S Configuration Guides, there are also separate configuration guides for the features listed in the following table.

Feature	URL
No Service Password Recovery	http://www.cisco.com/c/en/us/td/docs/routers/access/4400/feature/guide/isr4451nspr.html
Multilink PPP Support	http://www.cisco.com/c/en/us/td/docs/routers/access/4400/feature/guide/isr4451mlpp.html
Network Synchronization	http://www.cisco.com/c/en/us/td/docs/routers/access/4400/feature/guide/isr4400netclock.html
Integrated AppNav/AppNav-XE and ISR-WAAS	http://www.cisco.com/c/en/us/td/docs/routers/access/4400/appnav/isr/isr_appnav.html

To verify support for specific features, use the Cisco Feature Navigator tool. For more information, see Using Cisco Feature Navigator, on page 23.

Document Conventions

This documentation uses the following conventions:

Convention	Description
^ or **Ctrl**	The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive.

Convention	Description
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.

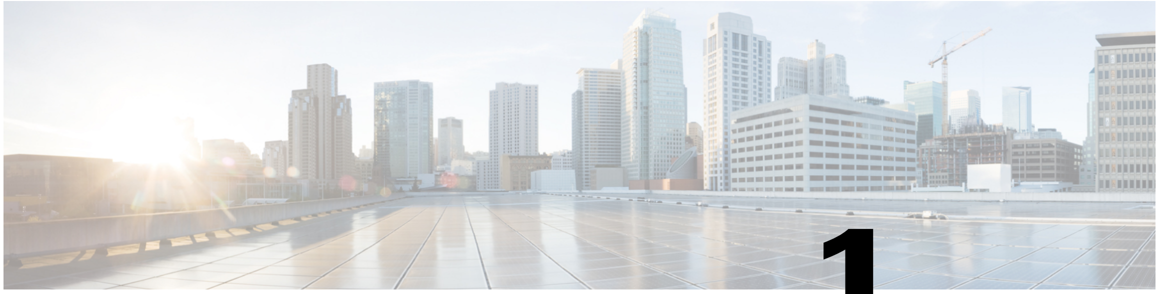
Convention	Description
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS XE software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

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

Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Note The Feature Information table in the technology configuration guide mentions when a feature was introduced. It might or might not mention when other platforms were supported for that feature. To determine if a particular feature is supported on your platform, look at the technology configuration guides posted on your product landing page. When a technology configuration guide is displayed on your product landing page, it indicates that the feature is supported on that platform.

CHAPTER 2

Overview

This document is a summary of software functionality that is specific to the Cisco 4000 Series Integrated Services Routers (ISRs).

The following table lists the router models that belong to the Cisco 4000 Series ISRs.

Table 1: Cisco 4000 Series Router Models

Cisco ISR 4400 Series	Cisco ISR 4300 Series
• Cisco ISR 4431 • Cisco ISR 4451	• Cisco ISR 4321 • Cisco ISR 4331 • Cisco ISR 4351

Note Unless otherwise specified, the information in this document is applicable to both Cisco 4400 series and Cisco 4300 series routers.

The following sections are included in this chapter:

Introduction

The Cisco 4000 series ISRs are modular routers with LAN and WAN connections that can be configured by means of interface modules, including Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs). NIM slots also support removable storage for hosted applications.

The following features are provided for enterprise and service provider applications:

- Enterprise Applications
  - High-end branch gateway
  - Regional site aggregation
  - Key server or PfR master controller
  - Device consolidation or "Rack in a Box"
- Service Provider Applications
  - High-end managed services in Customer-Premises Equipment (CPE)
  - Services consolidation platform
  - Route reflector or shadow router
  - Flexible customer edge router

The router runs Cisco IOS XE software, and uses software components in many separate processes. This modular architecture increases network resiliency, compared to standard Cisco IOS software.

Sections in this Document

Table 2: Sections in this Document

Section	Description
Overview, on page 3	Provides a high-level description of the router and describes the main internal processes of the router.
Using Cisco IOS XE Software, on page 9	Describes the basics of using Cisco IOS XE software with the router.
Using the Management Interfaces, on page 35	Describes the uses of a Gigabit Ethernet management interface and a web user interface.
Console Port, Telnet, and SSH Handling, on page 51	Describes software features that are common across Cisco IOS XE platforms.
Installing the Software, on page 67	Contains important information about filesystems, packages, licensing, and installing software.
Basic Router Configuration, on page 107	Describes the basic tasks required to configure a router.
Slot and Subslot Configuration, on page 121	Provides information about the chassis slot numbers and subslots where the service modules are installed.
Process Health Monitoring, on page 125	Provides information about managing and monitoring the health of various components of the router.

Section	Description
System Messages, on page 133	Provides information about syslog messages.
Trace Management, on page 141	Describes the tracing function where logs of internal events on a router are recorded.
Environmental Monitoring and PoE Management, on page 147	Describes the environmental monitoring features on a router.
Configuring High Availability, on page 173	Provides information about high availability features on a router to ensure network-wide protection.
Configuration Examples, on page 287	Lists examples that include software installation and packaging.
Managing Cisco Enhanced Services and Network Interface Modules, on page 245	Includes information about modules that can be attached to the router and provides related links to further documentation. For further details on configuring the modules (NIMs and SMs), also see the Documentation Roadmap.

Processes

The list of background processes in the following table may be useful for checking router state and troubleshooting. However, you do not need to understand these processes to understand most router operations.

Table 3: Individual Processes

Process	Purpose	Affected FRUs	Sub Package Mapping
Chassis Manager	Controls chassis management functions, including management of the High Availability (HA) state, environmental monitoring, and FRU state control.	RP SIP ESP	RPControl SIPBase ESPBase
Host Manager	Provides an interface between the IOS process and many of the information gathering functions of the underlying platform kernel and operating system.	RP SIP ESP	RPControl SIPBase ESPBase

Process	Purpose	Affected FRUs	Sub Package Mapping
Logger	Provides IOS logging services to processes running on each FRU.	RP SIP ESP	RPControl SIPBase ESPBase
IOS	Implements all forwarding and routing features for the router.	RP	RPIOS
Forwarding Manager	Manages downloading of configuration details to the ESP and the communication of forwarding plane information, such as statistics, to the IOS process.	RP ESP	RPControl ESPBase
Pluggable Services	Provide integration between platform policy applications, such as authentication and the IOS process.	RP	RPControl
Shell Manager	Provides user interface (UI) features relating to non-IOS components of the consolidated package. These features are also available for use in diagnostic mode when the IOS process fails.	RP	RPControl
IO Module process	Exchanges configuration and other control messages with a NIM, or Enhanced Service Module (SM-X).	IO Module	SIPSPA
CPP driver process	Manages CPP hardware forwarding engine on the ESP.	ESP	ESPBase
CPP HA process	Manages HA state for the CPP hardware forwarding engine.	ESP	ESPBase

Process	Purpose	Affected FRUs	Sub Package Mapping
CPP SP process	Performs high-latency tasks for the CPP-facing functionality in the ESP instance of the Forwarding Manager process.	ESP	ESPBase

For further details of router capabilities and models, see the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

CHAPTER 3

Using Cisco IOS XE Software

This chapter describes the basics of using the Cisco IOS XE software and includes the following section:

Accessing the CLI Using a Router Console

Before You Begin

There are two serial ports: a console (CON) port and an auxiliary (AUX) port. Use the CON port to access the command-line interface (CLI) directly or when using Telnet.

The following sections describe the main methods of accessing the router:

- Accessing the CLI Using a Directly-Connected Console, on page 9
- Using SSH to Access Console, on page 11
- Accessing the CLI from a Remote Console Using Telnet, on page 11
- Accessing the CLI from a USB Serial Console Port, on page 13

Accessing the CLI Using a Directly-Connected Console

The CON port is an EIA/TIA-232 asynchronous, serial connection with no-flow control and an RJ-45 connector. The CON port is located on the front panel of the chassis.

The following sections describe the procedure to access the control interface:

- Connecting to the Console Port, on page 10
- Using the Console Interface, on page 10

Connecting to the Console Port

Step 1 Configure your terminal emulation software with the following settings:

- 9600 bits per second (bps)
- 8 data bits
- No parity
- No flow control

Step 2 Connect to the CON port using the RJ-45-to-RJ-45 cable and the RJ-45-to-DB-25 DTE adapter or the RJ-45-to-DB-9 DTE adapter (labeled Terminal).

Using the Console Interface

Step 1 Enter the following command:

```
Router> enable
```

Step 2 (Go to Step 3 if the enable password has not been configured.) At the password prompt, enter your system password:

```
Password: enablepass
```

When your password is accepted, the privileged EXEC mode prompt is displayed.

```
Router#
```

You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 3 If you enter the **setup** command, see “Using Cisco Setup Command Facility” in the “Initial Configuration” section of the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

Step 4 To exit the console session, enter the **quit** command:

```
Router# quit
```

Using SSH to Access Console

Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. To enable SSH support on the device:

Step 1 Configure the hostname:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname xxx_lab
```

Here, *host name* is the router hostname or IP address.

Step 2 Configure the DNS domain of the router:

```
xxx_lab(config)# xxx.cisco.com
```

Step 3 Generate an SSH key to be used with SSH:

```
xxx_lab(config)#  crypto key generate rsa
The name for the keys will be: xxx_lab.xxx.cisco.com Choose the size of the key modulus in the range

of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few
minutes.
How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
xxx_lab(config)#
```

Step 4 By default, the vtys? transport is Telnet. In this case, Telnet is disabled and only SSH is supported:

```
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)#transport input SSH
```

Step 5 Create a username for SSH authentication and enable login authentication:

```
xxx_lab(config)# username jsmith privilege 15 secret 0 p@ss3456
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)# login local
```

Step 6 Verify remote connection to the device using SSH.

Accessing the CLI from a Remote Console Using Telnet

The following topics describe the procedure to access the CLI from a remote console using Telnet:

- Preparing to Connect to the Router Console Using Telnet, on page 11
- Using Telnet to Access a Console Interface, on page 12

Preparing to Connect to the Router Console Using Telnet

To access the router remotely using Telnet from a TCP/IP network, configure the router to support virtual terminal lines using the **line vty** global configuration command. Configure the virtual terminal lines to require users to log in and specify a password.

See the Cisco IOS Terminal Services Command Reference document for more information about the line **vty global** configuration command.

To prevent disabling login on a line, specify a password with the **password** command when you configure the **login** command.

If you are using authentication, authorization, and accounting (AAA), configure the **login authentication** command. To prevent disabling login on a line for AAA authentication when you configure a list with the login authentication command, you must also configure that list using the **aaa authentication login** global configuration command.

For more information about AAA services, see the Cisco IOS XE Security Configuration Guide: Secure Connectivity and the Cisco IOS Security Command Reference documents. For more information about the **login line-configuration** command, see the Cisco IOS Terminal Services Command Reference document.

In addition, before you make a Telnet connection to the router, you must have a valid hostname for the router or have an IP address configured on the router. For more information about the requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, see the Cisco IOS Configuration Fundamentals Configuration Guide.

Using Telnet to Access a Console Interface

Step 1 From your terminal or PC, enter one of the following commands:

- **connect host** [*port*] [*keyword*]
- **telnet host** [*port*] [*keyword*]

Here, *host* is the router hostname or IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information about these commands, see the Cisco IOS Terminal Services Command Reference document.

Note If you are using an access server, specify a valid port number, such as **telnet 172.20.52.40 2004**, in addition to the hostname or IP address.

The following example shows how to use the **telnet** command to connect to a router named **router**:

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

Step 2 Enter your login password:

```
User Access Verification
Password: mypassword
```

Note If no password has been configured, press **Return**.

Step 3 From user EXEC mode, enter the **enable** command:

```
Router> enable
```

Step 4 At the password prompt, enter your system password:

```
Password: enablepass
```

Step 5 When the **enable** password is accepted, the privileged EXEC mode prompt is displayed:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the Telnet session, use the **exit** or **logout** command.

```
Router# logout
```

Accessing the CLI from a USB Serial Console Port

The router provides an additional mechanism for configuring the system: a type B miniport USB serial console that supports remote administration of the router using a type B USB-compliant cable. See the “Connecting to a Console Terminal or Modem” section in the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

Using Keyboard Shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

The following table lists the keyboard shortcuts for entering and editing commands.

Table 4: Keyboard Shortcuts

Key Name	Purpose
Ctrl-B or the **Left Arrow** key[1]	Move the cursor back one character.
Ctrl-F or the **Right Arrow** key[1]	Move the cursor forward one character.
Ctrl-A	Move the cursor to the beginning of the command line.
Ctrl-E	Move the cursor to the end of the command line.
Esc B	Move the cursor back one word.
Esc F	Move the cursor forward one word.

Using the History Buffer to Recall Commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands.

The following table lists the history substitution commands.

Table 5: History Substitution Commands

Command	Purpose
Ctrl-P or the **Up Arrow** key[1]	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the **Down Arrow** key[1]	Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the **Up Arrow** key.
Router# show history	While in EXEC mode, lists the last few commands you entered.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Understanding Command Modes

The command modes available in Cisco IOS XE are the same as those available in traditional Cisco IOS. Use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

The following table describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

Table 6: Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.

Command Mode	Access Method	Prompt	Exit Method
Privileged EXEC	From user EXEC mode, use the **enable** command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
Diagnostic	The router boots up or accesses diagnostic mode in the following scenarios: • In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload. • A user-configured access policy is configured using the **transport-map** command that directs a user into diagnostic mode. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) is entered and the router is configured to go to diagnostic mode when the break signal is received.	`Router(diag)#`	If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the router rebooted to get out of diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or by using a method that is configured to connect to the Cisco IOS CLI.

Command Mode	Access Method	Prompt	Exit Method
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon#>`	To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded.

Understanding Diagnostic Mode

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into the diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In the diagnostic mode, a subset of the commands that are available in user EXEC mode are made available to the users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.
- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire router, a module, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the router when the router is working normally.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help that is specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

Command	Purpose
`help`	Provides a brief description of the help system in any command mode.
`abbreviated-command-entry?`	Provides a list of commands that begin with a particular character string. **Note** There is no space between the command and the question mark.
`abbreviated-command-entry<Tab>`	Completes a partial command name.
`?`	Lists all the commands that are available for a particular command mode.
`command ?`	Lists the keywords or arguments that you must enter next on the command line. **Note** There is a space between the command and the question mark.

Finding Command Options: Example

This section provides information about how to display the syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering a part of a command followed by a space. The Cisco IOS XE software displays a list and brief descriptions of the available keywords and arguments. For example, if you are in global configuration mode and want to see all the keywords and arguments for the **arap** command, you should type **arap ?**.

The <cr> symbol in command help output stands for carriage return. On older keyboards, the carriage return key is the **Return** key. On most modern keyboards, the carriage return key is the **Enter** key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available, and that you must press **Enter** to complete the command.

The following table shows examples of using the question mark (**?**) to assist you in entering commands.

Table 7: Finding Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a “ # ” from the “ > ”, for example, `Router>` to `Router#`

`Router# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router (config)#`

`Router(config)# interface GigabitEthernet ?`
`  <0-0>  GigabitEthernet interface number`
`  <0-2>  GigabitEthernet interface number`
 	
`Router(config)# interface GigabitEthernet 1/?`
`  <0-4>  Port Adapter number`
 	
`Router (config)# interface GigabitEthernet 1/3/?`
`  <0-15>  GigabitEthernet interface number`
 	
`Router (config)# interface GigabitEthernet 1/3/8?`
`.  <0-3>`
`Router (config)# interface GigabitEthernet 1/3/8.0`
 	
`Router(config-if)#`
	Enter interface configuration mode by specifying the interface that you want to configure, using the **interface GigabitEthernet** global configuration command.
	Enter **?** to display what you must enter next on the command line.
	When the <cr> symbol is displayed, you can press **Enter** to complete the command.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`

	Enter **?** to display a list of all the interface configuration commands available for the interface. This example shows only some of the available interface configuration commands.

<table>
<tr><th>Command</th><th>Comment</th></tr>
<tr><td><pre>
Router(config-if)# ?
Interface configuration commands:
  .
  .
  .
  ip   Interface Internet
Protocol
                        config commands
  keepalive   Enable keepalive
  lan-name   LAN Name command
  llc2   LLC2 Interface
Subcommands
  load-interval   Specify interval for load
 calculation
                        for an interface
  locaddr-priority   Assign a priority group
  logging   Configure logging for
interface
  loopback   Configure internal
loopback on an
                        interface
  mac-address   Manually set interface
MAC address
  mls   mls router sub/interface
 commands
  mpoa   MPOA interface
configuration commands
  mtu   Set the interface
                     Maximum Transmission Unit
 (MTU)
  netbios   Use a defined NETBIOS
access list
                        or enable
                        name-caching
  no   Negate a command or set
its defaults
  nrzi-encoding   Enable use of NRZI
encoding
  ntp   Configure NTP
  .
  .
  .
Router(config-if)#
</pre></td><td></td></tr>
<tr><td></td><td>Enter the command that you want to configure for the interface. This example uses the <b>ip</b> command.
Enter <b>?</b> to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</td></tr>
</table>

Command	Comment

Router(config-if)# **ip ?**
Interface IP configuration subcommands:
  access-group   Specify access control for packets
  accounting   Enable IP accounting on this interface
  address   Set the IP address of an interface
  authentication   authentication subcommands
  bandwidth-percent   Set EIGRP bandwidth limit
  broadcast-address   Set the broadcast address of an interface
  cgmp   Enable/disable CGMP
  directed-broadcast Enable forwarding of directed broadcasts
  dvmrp   DVMRP interface commands
  hello-interval   Configures IP-EIGRP hello interval
  helper-address   Specify a destination address for UDP broadcasts
  hold-time   Configures IP-EIGRP hold time
  .
  .
  .
Router(config-if)# **ip**	

Router(config-if)# **ip address ?**
  A.B.C.D   IP address
  negotiated   IP Address negotiated over PPP
Router(config-if)# **ip address**
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.
	A carriage return (<cr>) is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.

Router(config-if)# ip address 172.16.0.1 ? A.B.C.D IP subnet mask Router(config-if)# **ip address 172.16.0.1**	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. <cr> is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.
Router(config-if)# **ip address 172.16.0.1 255.255.255.0 ?** secondary Make this IP address a secondary address <cr> Router(config-if)# **ip address 172.16.0.1 255.255.255.0**	

Command	Comment
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask. Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**. <cr> is displayed. Press **Enter** to complete the command, or enter another keyword.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
`Router(config-if)#`
	Press **Enter** to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Many CLI commands also have a **default** form. By issuing the <*command*> **default** command-name, you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function from a **default** form of the command when the **default** form performs a different function than the plain and **no** forms of the command. To see what default commands are available on your system, enter **default ?** in the appropriate command mode.

Saving Configuration Changes

Use the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It may take a few minutes to save the configuration. After the configuration has been saved, the following output is displayed:

```
[OK]
Router#
```

This task saves the configuration to the NVRAM.

Managing Configuration Files

The startup configuration file is stored in the nvram: file system and the running configuration files are stored in the system: file system. This configuration file storage setup is also used on several other Cisco router platforms.

As a matter of routine maintenance on any Cisco router, users should back up the startup configuration file by copying the startup configuration file from NVRAM to one of the router's other file systems and, additionally, to a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file if the startup configuration file in NVRAM becomes unusable for any reason.

The **copy** command can be used to back up startup configuration files.

Examples of backing up the startup configuration file in NVRAM are shown in Backing Up Configuration Files, on page 298.

For more detailed information on managing configuration files, see the "Managing Configuration Files" section in the Cisco IOS XE Configuration Fundamentals Configuration Guide.

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

show *command* | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee**} *regular-expression*

The output matches certain lines of information in the configuration file.

Example

In this example, a modifier of the **show interface** command (**include protocol**) is used to provide only the output lines in which the expression **protocol** is displayed:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/1 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/2 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/3 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0 is up, line protocol is up
     0 unknown protocol drops
Loopback0 is up, line protocol is up
     0 unknown protocol drops
```

Powering Off a Router

Before You Begin

Before you turn off the power supply, ensure that the chassis is grounded and you perform a soft shutdown.

To perform a soft shutdown and then power off a router, perform the following steps.

Step 1 Ensure that the configuration register is configured to drop to ROMMON. See Configuring the Configuration Register for Autoboot, on page 70.

Step 2 Enter the **reload** command to halt the system:

```
Router# reload

System configuration has been modified. Save? [yes/no]:
Proceed with reload? [confirm]
```

Step 3 After the ROMMON prompt is displayed, move the router's power supply switch to the Off position.

Finding Support Information for Platforms and Cisco Software Images

The Cisco IOS XE software is packaged in feature sets consisting of software images that support specific platforms. The group of feature sets that are available for a specific platform depends on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or see the Release Notes for Cisco IOS XE.

Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator is a tool that enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To use the navigator tool, an account on Cisco.com is not required.

Using Software Advisor

Cisco maintains the Software Advisor tool. See Tools and Resources. Use the Software Advisor tool to see if a feature is supported in a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your router. You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

See the Release Notes document for the Cisco 4000 Series for information about the following:

- Memory recommendations
- Open and resolved severity 1 and 2 caveats

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. For cumulative feature information, refer to the Cisco Feature Navigator at: http://www.cisco.com/go/cfn/.

CLI Session Management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that the other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access a router.

- Changing the CLI Session Timeout, on page 24
- Locking a CLI Session, on page 24

Information About CLI Session Management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that each other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access the router.

Changing the CLI Session Timeout

Step 1 `configure terminal`

Enters global configuration mode

Step 2 `line console 0`

Step 3 `session-timeout` *`minutes`*

The value of *`minutes`* sets the amount of time that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. Specify a value of 0 for *`minutes`* to disable session timeout.

Step 4 `show line console 0`

Verifies the value to which the session timeout has been set, which is shown as the value for " `Idle Session` ".

Locking a CLI Session

Before You Begin

To configure a temporary password on a CLI session, use the **lock** command in EXEC mode. Before you can use the **lock** command, you need to configure the line using the **lockable** command. In this example the line is configured as **lockable**, and then the **lock** command is used and a temporary password is assigned.

Step 1 `Router# configure terminal`

Enters global configuration mode.

Step 2 Enter the line upon which you want to be able to use the **lock** command.

```
Router(config)# line console 0
```

Step 3

```
Router(config)# lockable
```

Enables the line to be locked.

Step 4

```
Router(config)# exit
```

Step 5

```
Router# lock
```

The system prompts you for a password, which you must enter twice.

```
Password: <password>
Again: <password>
Locked
```

CHAPTER 4

Smart Licensing

This chapter provides an overview of the Cisco Smart Licensing Client feature and describes the several tools and processes required to complete the products registration and authorization.

This chapter includes this section:

Smart Licensing Client

Smart Licensing Client feature is a standardized licensing platform that simplifies the Cisco software experience and helps you to understand how Cisco software is used across your network. Smart Licensing is the next eneration licensing platform for all Cisco software products.

Prerequisites for Cisco Smart Licensing Client

- Ensure that Call Home is not disabled before using the Smart Licensing Client feature.

Restrictions for Cisco Smart Licensing Client

- Cisco 4000 Series ISR platforms support Cisco One Suites License, Technology Package License, Throughput License, and HSECK9 license in Cisco Smart Licensing from Cisco IOS Release 15.6(1)S.
- Cisco ISR G2 platforms support only Cisco One Suites in Cisco Smart Licensing from Cisco IOS Release 15.5(1)T.

Information About Cisco Smart Licensing Client

Cisco Smart Licensing - An Overview

A new licensing model, based on a single technology, has been designed for Cisco called Smart Licensing that is intended to provide Enterprise Level Agreement-like capabilities for all of Cisco's products.

Smart Licensing is software based licensing end-to-end platform that consists of several tools and processes to authorize customers the usage and reporting of the Cisco products. The feature has the capability to capture the customers order and communicates with Cisco Cloud License Service through Smart Call Home transport media to complete the products registration and authorization on desired performance and technology level.

The Smart Licensing feature is aimed at giving users an experience of a single, standardized licensing solution for all Cisco products.

To know more about Smart Call Home, please refer to Smart Call Home.

Transitioning from CISL to Smart Licensing

In the Smart Licensing Model, customers can activate licensed objects without the use of a special software key or upgrade license file. The customers simply activate the new functionality using the appropriate product commands and configurations and the functionality is activated. A software reboot may or may not be required depending on the product capabilities and requirements.

Similarly, downgrading or removing an advanced feature, performance, or functionality would require a removal of the configuration or command.

Once either of these actions has been taken, the change in license state is noted by the Smart Software Manager upon next synchronization and an appropriate action is then taken.

Cisco One Suites

Cisco ONE Suites is a new way for customers to purchase infrastructure software. Cisco ONE offers a simplified purchasing model, centered on common customer scenarios in the data center, wide area network, and local access networks. To know more about Cisco One Suites, please refer to Cisco ONE Suites.

How to Activate Cisco Smart Licensing Client

Enable Smart Licensing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license smart enable**
4. **exit**
5. **write memory**
6. **show license all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart enable** **Example:** `Device# license smart enable`	Activates Smart Licensing on the device. **Note** When you enable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent. For the ‘no’ case, if Smart Licensing is already registered, the Smart Agent performs the ”license smart deregister” operation that deactivates Smart Licensing. Reload the device to activate the CSL on the device.
Step 4	**exit** **Example:** `Device# exit`	Exits the global configuration mode.

	Command or Action	Purpose
Step 5	**write memory** **Example:** `Device# write memory`	Saves the running configuration to NVRAM.
Step 6	**show license all** **Example:** `Device# show license all`	(Optional) Displays summary information about all licenses.

Smart License Disable

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no license smart enable**
4. **exit**
5. **write memory**
6. **reload**
7. **show license all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no license smart enable**	Deactivates Smart Licensing on the device.

	Command or Action	Purpose
	Example: `Device(config)# no license smart enable`	**Note** When you enable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent. For the 'no' case, if Smart Licensing is already registered, the Smart Agent performs the "license smart deregister" operation that deactivates Smart Licensing. Reload the device to activate the CSL on the device.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits the global configuration mode.
Step 5	**write memory** **Example:** `Device# write memory`	Saves the running configuration to NVRAM.
Step 6	**reload** **Example:** `Device# reload`	(Optional) Restarts the device to enable the new feature set. **Note** Reload the device if you have not reloaded the device after configuring the Cisco One Suites.
Step 7	**show license all** **Example:** `Device# show license all`	(Optional) Displays summary information about all licenses.

Device Registration

SUMMARY STEPS

1. **enable**
2. **license smart register idtoken** *idtoken* [**force**]
3. **license smart deregister**
4. **license smart renew** [**ID** | **auth**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**license smart register idtoken** *idtoken* [**force**] **Example:** `Device# license smart register idtoken 123`	Registers the device with the back-end server. Token id can be obtained from your virtual a/c in the Smart Licensing server. • **force**: To forcefully register your device irrespective of either the device is registered or not. **Note** The device supplies the token ID to the Cisco server, which sends back a "Device Certificate" that is valid for 365 days.
Step 3	**license smart deregister** **Example:** `Device# license smart deregister`	Deregisters the device from the backend server.
Step 4	**license smart renew** [**ID** | **auth**] **Example:** `Device# license smart renew ID`	(Optional) Manually renews the ID certification or authorization.

Troubleshooting for Cisco Smart Licensing Client

You can troubleshoot Smart Licensing enabling issues using the following commands on the device:

- **show version**
- **show running-config**
- **show license summary**
- **show license all**
- **show license tech support**
- **debug smart_lic error**
- **debug smart_lic trace**

Configuration Examples for Cisco Smart Licensing Client

Example: Displays summary information about all licenses

The following example shows how to use the **show license all** command to display summary information about all licenses.

```
Device#show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: BU Production Test
Virtual Account: ISR4K
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Sep 04 15:40:03 2015 PDT
Last Renewal Attempt: None
Next Renewal Attempt: Mar 02 15:40:02 2016 PDT
Registration Expires: Sep 03 15:34:53 2016 PDT

License Authorization:
Status: AUTHORIZED on Sep 04 15:40:09 2015 PDT
Last Communication Attempt: SUCCEEDED on Sep 04 15:40:09 2015 PDT
Next Communication Attempt: Oct 04 15:40:08 2015 PDT
Communication Deadline: Dec 03 15:35:01 2015 PDT

License Usage
==============

ISR_4400_FoundationSuite (ISR_4400_FoundationSuite):
Description: Cisco ONE Foundation Perpetual License ISR 4400
Count: 1
Version: 1.0
Status: AUTHORIZED

ISR_4400_AdvancedUCSuite (ISR_4400_AdvancedUCSuite):
Description: Cisco ONE Advanced UC Perpetual License ISR 4400
Count: 1
Version: 1.0
Status: AUTHORIZED

ISR_4451_2G_Performance (ISR_4451_2G_Performance):
Description: Performance on Demand License for 4450 Series
Count: 1
Version: 1.0
Status: AUTHORIZED

Product Information
===================
UDI: PID:ISR4451-X/K9,SN:FOC17042FJ9

Agent Version
=============
Smart Agent for Licensing: 1.4.0_rel/16
Component Versions: SA:(1_4_rel)1.0.15, SI:(dev22)1.2.6, CH:(dev5)1.0.32, PK:(dev18)1.0.17


Device#
```

Example: Enabling Smart Licensing

The following example shows how to use the **license smart enable** command to confirm if the Cisco ONE Suite is enabled.

Note The warning message that is displayed in the following example applies only for Cisco ISR G2 platform. For Cisco 4000 Series ISR platform, it does not display warning message when you enable the smart license.

```
Device# license smart enable
Currently only Cisco ONE license suites are supported by Smart Licensing.
Please make sure your Cisco ONE suites are enabled before turning on Smart Licensing.
Any other licenses outside of Cisco ONE suites would be disabled and made unusable in Smart
 Licensing.
If you have any questions, please get in touch with your Cisco representative before using
 this mmode.
Please confirm Cisco ONE suites are enabled? [yes/no]: yes
```

CHAPTER 5

Using the Management Interfaces

The following management interfaces are provided for external users and applications:

Gigabit Ethernet Management Interface

Gigabit Ethernet Management Interface Overview

The router provides an Ethernet management port named GigabitEthernet0.

The Ethernet management port allows you to perform management tasks on the router. It is an interface that should not, and often cannot, forward network traffic, but can be used to access the router via Telnet and Secure Shell (SSH) to perform management tasks on the router. The interface is most useful before a router has begun routing, or in troubleshooting scenarios when other forwarding interfaces are inactive.

The following are some key aspects of the Ethernet management interface:

- The router has one Ethernet management interface named GigabitEthernet0.
- IPv4 and IPv6 are the only routed protocols supported for the interface.
- The management interface provides a way to access the router even if forwarding interfaces are not functional, or the system process is down.

- The Ethernet management interface is a part of its own virtual routing and forwarding (VRF). This is discussed in more detail in Gigabit Ethernet Management Interface VRF, on page 36.

Default Gigabit Ethernet Configuration

By default, a forwarding VRF is configured for the Ethernet management interface with a special group named Mgmt-intf. You cannot change this configuration. Configuring a forwarding VRF for the interface with a special group named Mgmt-intf allows you to isolate the traffic on the Ethernet management interface away from the forwarding plane. Otherwise, the interface can be configured like other Gigabit Ethernet interfaces for most functions.

For example, the default configuration is:

```
Router(config)# interface GigabitEthernet0
Router(config-if)# vrf forwarding Mgmt-intf
```

Gigabit Ethernet Port Numbering

The Gigabit Ethernet management port is always GigabitEthernet0 and the port can be accessed in global configuration mode as shown in the following example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet0
Router(config-if)#
```

Gigabit Ethernet Management Interface VRF

The Gigabit Ethernet management interface is automatically a part of its own VRF. This VRF, which is named Mgmt-intf, is automatically configured on the router and is dedicated to the Ethernet management interface; no other interfaces can join this VRF, and no other interfaces can be placed in the management VRF. The management Ethernet interface VRF does not participate in the MPLS VPN VRF or any other network-wide VRF.

Placing the Gigabit Ethernet management interface in its own VRF has the following effects on the management Ethernet interface:

- Requires configuring multiple features—Because Cisco IOS CLI may be different for certain management Ethernet functions compared to other routers, you should configure or use many of the VRF's features.
- Prevents transit traffic from traversing the router—Because all the module interfaces and the management Ethernet interface are automatically in different VRFs, no transit traffic can enter the management Ethernet interface and leave a module interface, or vice versa.
- Improves security of the interface—Because the Mgmt-intf VRF has its own routing table because of being in its own VRF, routes can be added to the routing table of the management Ethernet interface only if you explicitly enter them.

The management Ethernet interface VRF supports both IPv4 and IPv6 address families.

Note You can configure only the Gigabit Ethernet management interface (and a loopback interface) as a part of the Mgmt-intf VRF. You cannot configure other interfaces in this VRF.

Common Gigabit Ethernet Management Tasks

You can access the Ethernet management interface to perform the following tasks on your router.

Note The following is not a comprehensive list of all the tasks that can be performed using the Ethernet management interface.

- Viewing the VRF Configuration, on page 37
- Viewing Detailed Information for the Gigabit Ethernet Management VRF, on page 38
- Setting a Default Route in the Management Ethernet Interface VRF, on page 38
- Setting the Gigabit Ethernet Management IP Address, on page 38
- Using Telnet over the Gigabit Ethernet Management Interface, on page 38
- Pinging over the Gigabit Ethernet Management Interface, on page 39
- Copying a File Using TFTP or FTP, on page 39
- Setting up the Software Clock Using the NTP Server, on page 39
- Logging, on page 40
- SNMP-Related Services, on page 40
- Assigning a Domain Name, on page 40
- Assigning DNS, on page 40
- Configuring a RADIUS or TACACS+ Server Group, on page 40
- Attaching an ACL to VTY Lines, on page 41

Viewing the VRF Configuration

To view the VRF configuration for the Gigabit Ethernet management interface, use the **show running-config vrf** command. The following example shows the default VRF configuration:

```
Router# show running-config vrf

Building configuration...

Current configuration : 351 bytes
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
```

```
exit-address-family
!
(some output removed for brevity)
```

Viewing Detailed Information for the Gigabit Ethernet Management VRF

To view detailed information about the Gigabit Ethernet management VRF, enter the **show vrf detail Mgmt-intf** command, as shown in the following example:

```
Router# show vrf detail Mgmt-intf

VRF Mgmt-intf (VRF Id = 4085); default RD <not set>; default VPNID <not set>
Interfaces:
Gi0
Address family ipv4 (Table ID = 4085 (0xFF5)):
No Export VPN route-target communities
No Import VPN route-target communities
No import route-map
No export route-map
VRF label distribution protocol: not configured
VRF label allocation mode: per-prefix
Address family ipv6 (Table ID = 503316481 (0x1E000001)):
No Export VPN route-target communities
No Import VPN route-target communities
No import route-map
No export route-map
VRF label distribution protocol: not configured
VRF label allocation mode: per-prefix
```

Setting a Default Route in the Management Ethernet Interface VRF

You can set a default route in the Gigabit Ethernet management interface VRF by entering the following command:

```
Router(config)# ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 next-hop-IP-address
```

To set a default route in the management Ethernet interface VRF with an IPv6 address, enter the following command:

```
Router(config)# ipv6 route vrf Mgmt-intf : : /next-hop-IPv6-address/
```

Setting the Gigabit Ethernet Management IP Address

You can set the IP address of the Gigabit Ethernet management port as you would for the IP address on any other interface.

To configure an IPv4 address on the Ethernet management interface, enter the following commands:

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip address A.B.C.D A.B.C.D
```

To configure an IPv6 address on the Ethernet management interface, enter the following commands:

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ipv6 address X:X:X:X::X
```

Using Telnet over the Gigabit Ethernet Management Interface

You can use Telnet to connect to a router through the Gigabit Ethernet management interface VRF using the **telnet** command and the router's IP address.

To use Telnet to connect to the IPv4 address of a router, enter the following command:

```
Router# telnet 172.17.1.1 /vrf Mgmt-intf
```

To use Telnet to connect to the IPv6 address of a router, enter the following command:

```
Router# telnet 2001:db8::abcd /vrf Mgmt-intf
```

Pinging over the Gigabit Ethernet Management Interface

You can ping other interfaces using the Ethernet management interface through the VRF.

To ping the interface with the IPv4 address, enter the following command:

```
Router# ping vrf Mgmt-intf 172.17.1.1
```

To ping the interface with the IPv6 address, enter the following command:

```
Router# ping vrf Mgmt-intf 2001:db8::abcd
```

Copying a File Using TFTP or FTP

To copy a file using TFTP through the Ethernet management interface, the **ip tftp source-interface GigabitEthernet 0** command must be entered before entering the **copy tftp** command because the **copy tftp** command has no option of specifying a VRF name.

Similarly, to copy a file using FTP through the Ethernet management interface, the **ip ftp source-interface GigabitEthernet 0** command must be entered before entering the **copy ftp** command because the **copy ftp** command has no option of specifying a VRF name.

The following is an example of copying a file using TFTP:

```
Router(config)# ip tftp source-interface gigabitEthernet 0
```

The following is an example of copying a file using FTP:

```
Router(config)# ip ftp source-interface gigabitEthernet 0

Building configuration...
- Omitted lines -
!
!
ip ftp source-interface GigabitEthernet0
ip tftp source-interface GigabitEthernet0
!
```

Setting up the Software Clock Using the NTP Server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server over the Gigabit Ethernet management interface, enter the **ntp server vrf Mgmt-intf** command and specify the IP address of the device providing the update.

To set up the NTP server over the Ethernet management interface with an IPv4 address, enter the following command:

```
Router(config)# ntp server vrf Mgmt-intf 172.17.1.1
```

To set up the NTP server over the Ethernet management interface with an IPv6 address, enter the following command:

```
Router(config)# ntp server vrf Mgmt-intf 2001:db8::abcd
```

Logging

To specify the Gigabit Ethernet management interface as the source IP or IPv6 address for logging, enter the **logging host** *ip-address* **vrf Mgmt-intf** command:

```
Router(config)# logging host 172.17.1.1 vrf Mgmt-intf
```

SNMP-Related Services

To specify the Gigabit Ethernet management interface as the source of all SNMP trap messages, enter the **snmp-server source-interface traps gigabitethernet 0** command:

```
Router(config)# snmp-server source-interface traps gigabitethernet 0
```

Assigning a Domain Name

Assign the IP domain name for the Gigabit Ethernet management interface through the VRF.

To define the default domain name as the Gigabit Ethernet management VRF interface, enter the **ip domain-name vrf Mgmt-intf** *domain* command:

```
Router(config)# ip domain-name vrf Mgmt-intf cisco.com
```

Assigning DNS

To specify the Ethernet management interface VRF as a name server, enter the **ip name-server vrf Mgmt-intf** *IPv4-or-IPv6-address* command:

```
Router(config)# ip name-server vrf Mgmt-intf A.B.C.D
```

or

```
Router(config)# ip name-server vrf Mgmt-intf X:X:X:X::X
```

Configuring a RADIUS or TACACS+ Server Group

To group the Management VRF as part of an AAA server group, enter the **ip vrf forward Mgmt-intf** command when configuring the AAA server group.

The same concept is true for configuring a TACACS+ server group. To group the Management VRF as part of a TACACS+ server group, enter the **ip vrf forwarding Mgmt-intf** command when configuring the TACACS+ server group.

The following is an example of configuring a RADIUS server group:

```
Router(config)# aaa group server radius hello
Router(config-sg-radius)# ip vrf forwarding Mgmt-intf
```

The following is an example of configuring a TACACS+ server group:

```
Router(config)# aaa group server tacacs+ hello
Router(config-sg-tacacs+)# ip vrf forwarding Mgmt-intf
```

Attaching an ACL to VTY Lines

To ensure an access control list (ACL) is attached to vty lines that are and are not using VRF, use the **vrf-also** keyword:

```
Router(config)# line vty 0 4
Router(config-line)# access-class 90 in vrf-also
```

Or

```
Router(config-line)# IPv6 access-class my-vty-acl in vrf-also
```

Configuring IP Addresses in ROMMON and the Ethernet Management Port

IP addresses can be configured in ROMMON using the **IP_ADDRESS=** and **IP_SUBNET_MASK=** commands. You can also configure IP addresses using the **ip address** command in the interface configuration mode.

Before the system is booted and the Cisco IOS process is running on a router, the IP address that is set in ROMMON acts as the IP address of the Ethernet management interface.

After the Cisco IOS process starts and is in control of the Ethernet management interface, the IP address specified when configuring the GigabitEthernet0 interface in the Cisco IOS CLI becomes the IP address of the Ethernet management interface.

The ROMMON-defined IP address is used only until the Cisco IOS process is active. For this reason, the IP addresses specified in ROMMON and in the Cisco IOS XE commands should be identical to ensure that the Gigabit Ethernet management interface functions properly.

Enabling SNMP

For further information about enabling SNMP, see SNMP-Related Services, on page 40 and Configuring SNMP Support.

Web User Interface Management

You can access your router using a web user interface. The web user interface allows you to monitor router performance using an easy-to-read graphical interface. Most aspects of your router can be monitored using the web user interface which enables you to perform the following functions:

- View information in an easy-to-read graphical format.
- Monitor most software processes, including processes related to the Cisco IOS and non-Cisco IOS subpackages within the Cisco IOS XE consolidated package.
- Monitor most hardware components, including all RPs, NIMs, and SM-Xs installed on your router.
- Access legacy web user interface in addition to the enhanced web user interface.
- Gather **show** command output.

This section consists of the following topics:

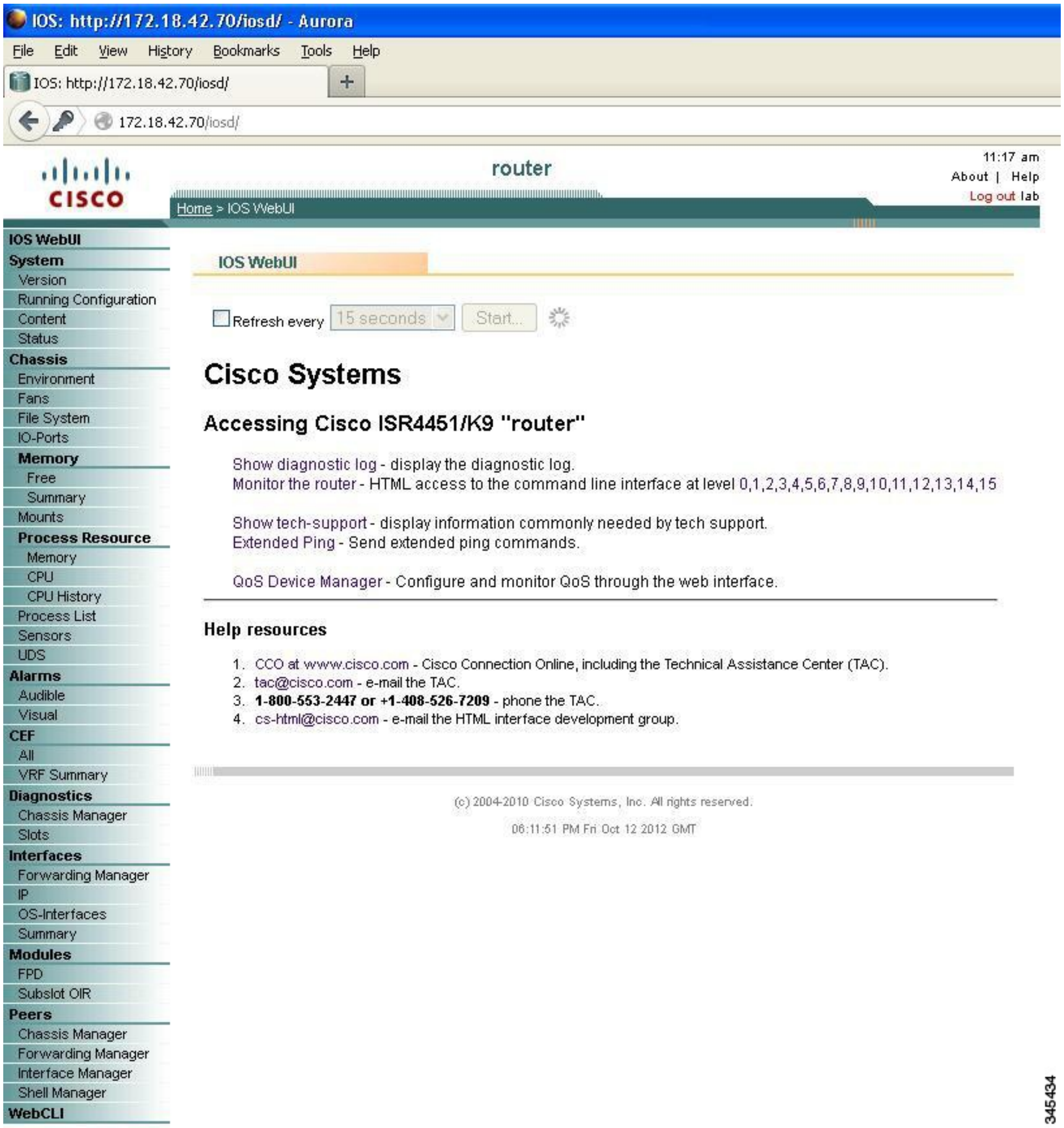
Legacy Web User Interface Overview

Previous Cisco routers have a legacy web user interface that can be used to monitor the router. This legacy web user interface presents information in a straightforward manner without using any graphics. On the router, this interface is part of the larger web user interface and can be accessed by clicking the **IOS Web UI** option in the left-hand menu.

On your router, the legacy web user interface can be used only to configure and monitor the Cisco IOS subpackages. In some scenarios, most notably when an **ip http** command has been successfully entered to enable the HTTP or HTTPS server while a properly configured web user interface transport map has not yet been applied on the router, the legacy web user interface will be accessible while the graphics-based web user interface will be inaccessible.

An example showing the IOS web user interface home page is shown in the following figure.

Figure 1: Legacy Web User Interface Home Page



Cisco Systems

Accessing Cisco ISR4451/K9 "router"

Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

QoS Device Manager - Configure and monitor QoS through the web interface.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447 or +1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

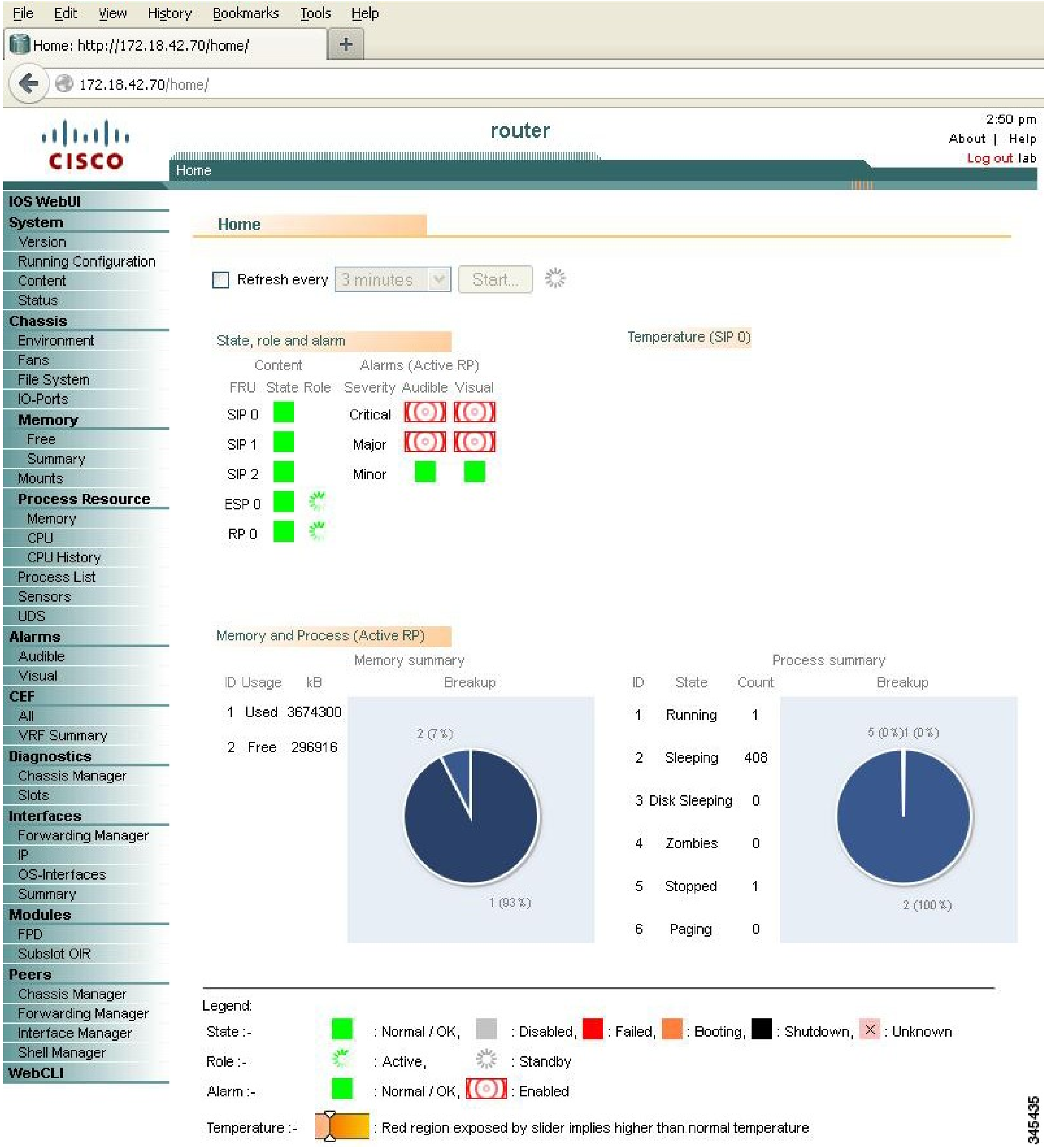
(c) 2004-2010 Cisco Systems, Inc. All rights reserved.

06:11:51 PM Fri Oct 12 2012 GMT

Graphics-Based Web User Interface Overview

The graphics-based web user interface on your router displays router information in the form of graphics-based tables, graphs, or charts, depending on the type of the information. You can access all the monitoring-related information stored in both the Cisco IOS and non-Cisco IOS subpackages, and also a complete view of your router using the web user interface. The following figure is an example of the graphics-based web user interface home page.

Figure 2: Graphics-Based Web User Interface Home Page



☐ Refresh every 3 minutes

State, role and alarm

Content			Alarms (Active RP)		
FRU	State	Role	Severity	Audible	Visual
SIP 0	🟩		Critical	◉	◉
SIP 1	🟩		Major	◉	◉
SIP 2	🟩		Minor	🟩	🟩
ESP 0	🟩	✳			
RP 0	🟩	✳			

Memory and Process (Active RP)

Memory summary

ID	Usage	kB
1	Used	3674300
2	Free	296916

Process summary

ID	State	Count
1	Running	1
2	Sleeping	408
3	Disk Sleeping	0
4	Zombies	0
5	Stopped	1
6	Paging	0

Legend:
State :- 🟩 : Normal / OK, ⬜ : Disabled, 🟥 : Failed, 🟧 : Booting, ⬛ : Shutdown, ☒ : Unknown
Role :- ✳ : Active, ✳ : Standby
Alarm :- 🟩 : Normal / OK, ◉ : Enabled
Temperature :- 🟧 : Red region exposed by slider implies higher than normal temperature

Overview of Persistent Web User Interface Transport Maps

You must configure a persistent web user interface transport map to enable the graphics-based web user interface on your router. When successfully configured and applied to your router, the persistent web user interface transport map defines how the router handles incoming requests from the web user interface. In the persistent web user interface transport map, you can define whether the graphics-based web user interface can be accessed through HTTP, HTTPS, or both protocols. You can apply only one persistent web user interface map to your router.

You must configure the legacy web user interface prior to enabling the graphics-based web user interface on your router. You can use the **ip http** command set to configure the legacy web user interface.

The **ip http** command settings define which ports are used by HTTP or HTTPS for both the legacy and graphics-based web user interface.

For information on configuring the entire graphics-based web user interface, including the configuration of persistent web user interface transport maps on your router, see Configuring Web User Interface Access, on page 45.

Enabling Web User Interface Access

To enable the web user interface for your router, perform these tasks:

- Configuring Web User Interface Access, on page 45
- Accessing the Web User Interface, on page 46
- Web User Interface Authentication, on page 47
- Domain Name System and the Web User Interface, on page 47
- Clocks and the Web User Interface, on page 47
- Using Auto Refresh, on page 48

Configuring Web User Interface Access

Before You Begin

- You must configure the legacy web user interface before you enable the graphics-based web user interface on your router. Access to the web user interface on your router is disabled by default.
- You must specify the default route in the Gigabit Ethernet management VRF interface before configuring the web user interface on your router. The web user interface is disabled when the Gigabit Ethernet management interface is not configured, or is not functioning. For information on configuring a default route in the Gigabit Ethernet management interface on your router, see Setting a Default Route in the Management Ethernet Interface VRF, on page 38.

Step 1 (Optional) Enter the **show clock** command in privileged EXEC mode to ensure that the clock setting on your router is accurate:

```
Router# show clock
*19:40:20.598 UTC Fri Jan 21 2013
```

If the router time is not properly set, use the **clock set** and **clock timezone** commands to set the system clock.

Note For more information about how clock settings on both the router and the web browser can impact the web user interface, see Clocks and the Web User Interface, on page 47.

Step 2 Enter the **configure terminal** command to enter global configuration mode.

Step 3 Enter the following commands to enable the legacy web user interface:

- **ip http server—**Enables HTTP on port 80, which is the default HTTP port.
- **ip http port port-number—**Enables HTTP on the nondefault user-specified port. Default port number is 80.
- **ip http secure-server—**Enables HTTPS on port 443, the default HTTPS port.
- **ip http secure-port port-number—**Enables HTTPS on the nondefault user-specified port.

You can now access the legacy web user interface.

Step 4 Create and name a persistent web user interface transport map by entering the **transport-map type persistent webui** *transport-map - name* command.

Step 5 Enable HTTP, HTTPS, or both by entering the following commands in the transport map configuration mode:

- **server—**Enables HTTP.
- **secure-server—**Enables HTTPS.

Port numbers cannot be set within the transport map. The port numbers that you defined in Step 3 are also used with these settings in the persistent web user interface transport map.

Step 6 (Optional) Enter the **show transport-map name** *transport-map-name* in privileged EXEC command to verify that your transport map is properly configured.

Step 7 Enter the **transport-map type persistent webui** *transport-map - name* command in global configuration mode to enable the transport map.

Accessing the Web User Interface

Step 1 Open your web browser. The web user interface supports the following web browsers:

- Microsoft Internet Explorer 6 or later
- Mozilla Firefox 2.0 or later

Step 2 Enter the address of the router in the Address field of the web browser. The format for the router address is http://<*routername* or *management-ethernet-ip-address*>:[http-port] or https://<*routername* or management-ethernet-ip-address>:[https-port]. The addresses depend upon your web browser user interface configurations and whether your router is participating in DNS.
The following examples are acceptable Address-field entries:

```
HTTP Using Default Port Example
http://172.16.5.1
HTTPS Using Default Port Example
https://172.16.5.1
HTTP Using NonDefault Port Example
http://172.16.5.1:94
```

```
HTTPS Using NonDefault Port Example
https://172.16.5.1:530/
HTTP Using Default Port Participating in DNS Example
http://router1
HTTPS Using Default Port Participating in DNS Example
https://router1
HTTP Using NonDefault Port Participating in DNS Example
http://router1:94
HTTPS Using NonDefault Port Participating in DNS Example
https://router1:530/
```

Step 3 When prompted, enter your username and password.

Note The username and password combination required to enter the web user interface is the same combination required to access the router.

The graphics-based web user interface, similar to the figure in Graphics-Based Web User Interface Overview, on page 43 is displayed.

For additional information on the commands and the options available with each command, see the Cisco IOS Configuration Fundamentals Command Reference.

Web User Interface Authentication

When accessing the web user interface for your router, you must enter the same username and password as the ones configured on your router for authentication purposes. The web browser prompts all users for a username and password combination, and the web browser verifies this information with the router before allowing access to the web user interface.

Only users with a privilege level of 15 can access the web user interface. Authentication of web user interface traffic is governed by the authentication configuration for all other traffic.

To configure authentication on your router, see "Configuring Authentication" in the Cisco IOS Security Configuration Guide.

Domain Name System and the Web User Interface

The Domain Name System (DNS) is a distributed database in which you can map hostnames to IP addresses through the DNS protocol from a DNS server.

If the router is configured to participate in the DNS, users can access the web user interface by entering **http://<dns-hostname>** as the web browser address.

For information on configuring the DNS, see "Configuring DNS" in the IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3S.

Clocks and the Web User Interface

Certain web browsers can reject the request to view the web user interface if the time seen by the web browser differs from the time seen on the router by an hour or more. We recommend checking the router time using the **show clock** command before configuring the router. You can set the router's system time using the **clock set** and **clock timezone** commands.

Similarly, the web browser's clock source, which is usually the personal computer, must display accurate time to properly access the web user interface.

```
Your access is being denied for one of the following reasons:
– Your previous session has timed-out.

– You have been logged out from elsewhere.

– You have not yet logged in.

– The resource requires a higher privilege level login.
```

If web user interface is inaccessible even after fixing one or more of the possible causes of the issue listed above, check your router's clock setting and your PC clock setting to ensure that both the clocks are displaying the correct day and time and retry accessing your web user interface.

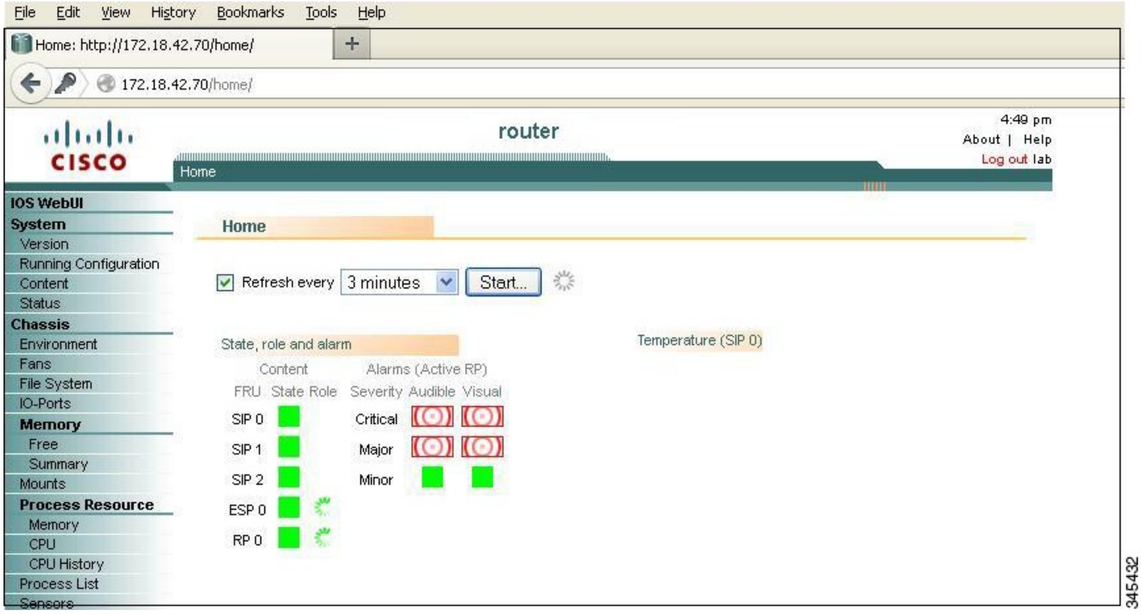
Note Clock-related issues may occur when one clock changes to day light savings time while the other remains unchanged.

Using Auto Refresh

The web user interface does not refresh content automatically by default. To set an auto-refresh interval, follow these steps:

Step 1 Select the **Refresh every** check box on your graphical web user interface home page.
A check mark is displayed in the check box. (See the following figure.)

Figure 3: Auto-Refresh Check Box on the Graphic-Based Web User Interface



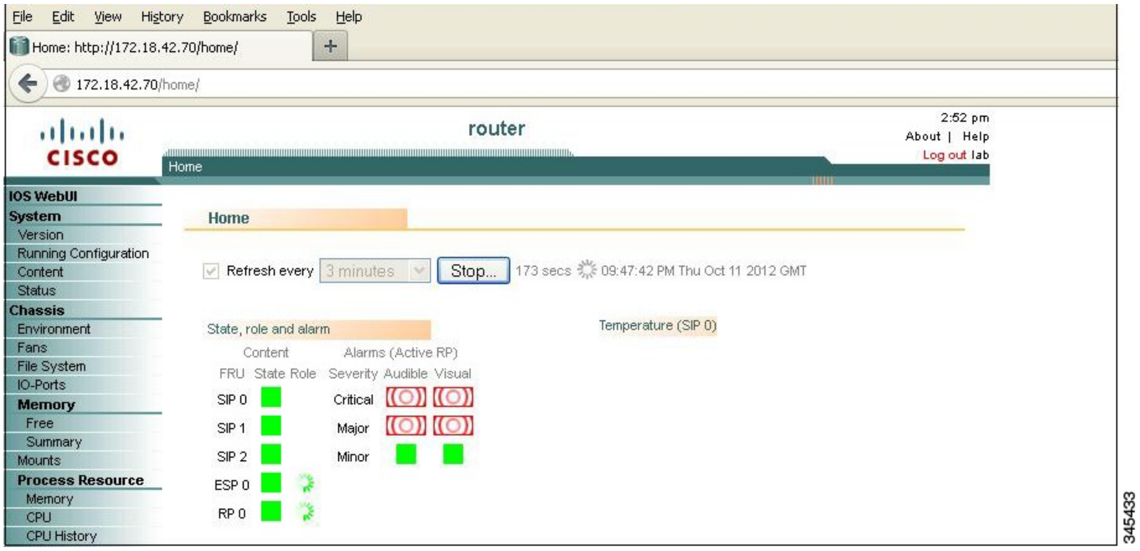
☑ Refresh every 3 minutes

Step 2 Set the frequency of the auto-refresh interval using the drop-down menu.

Step 3 Set the frequency of the auto-refresh interval using the drop-down menu.

Step 4 Click the **Start** button to the right of the drop-down menu.
Immediately after clicking the **Start** button, it becomes the **Stop** button and a countdown timer is displayed on the right of this **Stop** button as shown in the following figure.

Figure 4: Stop Button with Auto Refresh Counter



☑ Refresh every 3 minutes Stop... 173 secs 09:47:42 PM Thu Oct 11 2012 GMT

Configuration Examples

Enabling the web user interface using the default HTTP port: Example

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http server
Router(config)# transport-map type persistent webui http-webui
Router(config-tmap)# server
Router(config-tmap)# exit
Router(config)# exit
Router# show transport-map name http-webui
Transport Map:
  Name: http-webui
  Type: Persistent Webui Transport
Webui:
  Server:        enabled
  Secure Server: disabled
Router# configure terminal
Router(config)# transport type persistent webui input http-webui
*Sep. 21 02:43:55.798: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server wui has been
notified to start
```

Enabling the web user interface using the default HTTPs port: Example

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http secure-server
Router(config)# transport-map type persistent webui https-webui
Router(config-tmap)# secure-server
Router(config-tmap)# exit
Router(config)# transport type persistent webui input https-webui
*Sep. 21 02:38:43.597: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server wui has been
notified to start
```

Enabling the web user interface using the default HTTP and HTTPS ports: Example

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# transport-map type persistent webui http-https-webui
Router(config-tmap)# server
Router(config-tmap)# secure-server
Router(config-tmap)# exit
Router(config)# transport type persistent webui input http-https-webui
*Sep 21 02:47:22.981: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server wui has been
notified to start
```

CHAPTER 6

Console Port, Telnet, and SSH Handling

This chapter includes the following sections:

Notes and Restrictions for Console Port, Telnet, and SSH

- Telnet and Secure Shell (SSH) settings configured in the transport map override any other Telnet or SSH settings when the transport map is applied to the Ethernet management interface.
- Only local usernames and passwords can be used to authenticate users entering a Ethernet management interface. AAA authentication is not available for users accessing the router through a Ethernet management interface using persistent Telnet or persistent SSH.
- Applying a transport map to a Ethernet management interface with active Telnet or SSH sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet or SSH session.
- Configuring the diagnostic and wait banners is optional, but recommended. The banners are especially useful as indicators to users about the status of their Telnet or SSH attempts.

Console Port Overview

The console port on the router is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is used to access the router and is located on the front panel of the Route Processor.

For information on accessing the router using the console port, see Using Cisco IOS XE Software, on page 9.

Console Port Handling Overview

If you are using the console port to access the router, you are automatically directed to the Cisco IOS command-line interface (CLI).

If you are trying to access the router through the console port and send a break signal (by entering **Ctrl-C** or **Ctrl-Shift-6**, or by entering the **send break** command at the Telnet prompt) before connecting to the CLI, you are directed to a diagnostic mode if the non-RPIOS subpackages are accessible. These settings can be changed by configuring a transport map for the console port and applying that transport map to the console interface.

Telnet and SSH Overview

Telnet and SSH on the router can be configured and handled like Telnet and SSH on other Cisco platforms. For information on traditional Telnet, see the line command in the Cisco IOS Terminal Services Command Reference, Release 12.2 document.

For information on configuring traditional SSH, see the “Configuring Secure Shell” chapter in the Cisco IOS Terminal Services Command Reference, Release 12.2 document.

On the router, persistent Telnet and persistent SSH allow network administrators to more clearly define the treatment of incoming traffic when users access the router through the management ethernet port using Telnet or SSH. Notably, persistent Telnet and persistent SSH provide more robust network access by allowing the router to be configured to be accessible through the Ethernet management port using Telnet or SSH even when the Cisco IOS process has failed.

Persistent Telnet and Persistent SSH Overview

In traditional Cisco routers, accessing the router using Telnet or SSH is not possible if the Cisco IOS software fails. When Cisco IOS fails on a traditional Cisco router, the only method of accessing the router is through the console port. Similarly, if all the active Cisco IOS processes have failed on a router that is not using persistent Telnet or persistent SSH, the only method of accessing the router is through the console port.

However, with persistent Telnet and persistent SSH, you can configure a transport map that defines the treatment of incoming Telnet or SSH traffic on the Ethernet management interface. Among the many configuration options, a transport map can be configured to direct all traffic to the Cisco IOS CLI, diagnostic mode, or to wait for a Cisco IOS VTY line to become available and then direct users to diagnostic mode when a user sends a break signal while waiting for the IOS VTY line to become available. If a user uses Telnet or SSH to access diagnostic mode, that Telnet or SSH connection will be usable even in scenarios when no Cisco IOS process is active. Therefore, persistent Telnet and persistent SSH introduce the ability to access the router via diagnostic mode when the Cisco IOS process is not active. For information on diagnostic mode, see Using Cisco IOS XE Software. For information on the options that are can be configured using persistent Telnet or persistent SSH transport maps, see Configuring Persistent Telnet, on page 55 and Configuring Persistent SSH, on page 57.

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **transport-map type console** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. (Optional) **banner** [**diagnostic** | **wait**] *banner-message*
6. **exit**
7. **transport type console** *console-line-number* **input** *transport-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type console** *transport-map-name* **Example:** `Router(config)# transport-map type console consolehandler`	Creates and names a transport map for handling console connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] **Example:** `Router(config-tmap)# connection wait none`	Specifies how a console connection will be handled using this transport map. • **allow interruptible**—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco IOS VTY line to become available. This is the default setting.

	Command or Action	Purpose
		Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The console connection immediately enters diagnostic mode.

Step 5	(Optional) **banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# **banner diagnostic X**`
	`Enter TEXT message. End with the character 'X'.`
	`**--Welcome to Diagnostic Mode--**`
	`**X**`
	`Router(config-tmap)#`
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.
		• **diagnostic**—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.
		Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
		• **wait**—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.
		• *banner-message*—Banner message, which begins and ends with the same delimiting character.

Step 6	**exit** **Example:** `Router(config-tmap)# **exit**`	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	**transport type console** *console-line-number* **input** *transport-map-name* **Example:** `Router(config)# **transport type console 0 input consolehandler**`	Applies the settings defined in the transport map to the console interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** command.

Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

Configuring Persistent Telnet

For a persistent Telnet connection to access an Cisco IOS vty line on the router, local login authentication must be configured for the vty line (the **login** command in line configuration mode). If local login authentication is not configured, users will not be able to access Cisco IOS using a Telnet connection into the management Ethernet interface with an applied transport map. Diagnostic mode will still be accessible in this scenario.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **transport-map type persistent telnet** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] **| none** [**disconnect**]]
5. (Optional) **banner** [**diagnostic | wait**] *banner-message*
6. **transport interface gigabitethernet 0**
7. **exit**
8. **transport type persistent telnetinput** *transport-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type persistent telnet** *transport-map-name* **Example:** `Router(config)# transport-map type persistent telnet telnethandler`	Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] **Example:** `Router(config-tmap)# connection wait none`	Specifies how a persistent Telnet connection will be handled using this transport map: • **allow—**The Telnet connection waits for a Cisco IOS vty line to become available, and exits the router if interrupted. • **allow interruptible—**The Telnet connection waits for the Cisco IOS vty line to become available, and also allows user to enter diagnostic

	Command or Action	Purpose
		mode by interrupting a Telnet connection waiting for the Cisco IOS vty line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none—**The Telnet connection immediately enters diagnostic mode. • **none disconnect—**The Telnet connection does not wait for the Cisco IOS vty line and does not enter diagnostic mode, so all Telnet connections are rejected if no vty line is immediately available in the Cisco IOS software.

Step 5	(Optional) **banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# ` **`banner diagnostic X`**
	`Enter TEXT message. End with the character 'X'.`
	`--Welcome to Diagnostic Mode--`
	`X`
	`Router(config-tmap)#`
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS vty line because of the persistent Telnet configuration.
		• **diagnostic—**Creates a banner message seen by users directed into diagnostic mode because of the persistent Telnet configuration.
		Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
		• **wait—**Creates a banner message seen by users waiting for the vty line to become available.
		• *banner-message***—**The banner message, which begins and ends with the same delimiting character.

Step 6	**transport interface gigabitethernet 0** **Example:** `Router(config-tmap)# ` **`transport interface gigabitethernet 0`**	Applies the transport map settings to the management Ethernet interface (interface gigabitethernet 0). Persistent Telnet can be applied only to the management Ethernet interface on the router. This step must be taken before applying the transport map to the management Ethernet interface.
Step 7	**exit** **Example:** `Router(config-tmap)# ` **`exit`**	Exits transport map configuration mode to re-enter global configuration mode.
Step 8	**transport type persistent telnetinput** *transport-map-name* **Example:** `Router(config)# ` **`transport type persistent telnet input telnethandler`**	Applies the settings defined in the transport map to the management Ethernet interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent telnet** command.

Examples

In the following example, a transport map that will make all Telnet connections wait for a Cisco IOS XE vty line to become available before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the management Ethernet interface (**interface gigabitethernet 0**).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

Configuring Persistent SSH

This task describes how to configure persistent SSH on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **transport-map type persistent ssh** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. **rsa keypair-name** *rsa-keypair-name*
6. (Optional) **authentication-retries** *number-of-retries*
7. (Optional) **banner** [**diagnostic** | **wait**] *banner-message*
8. (Optional) **time-out** *timeout-interval*
9. **transport interface gigabitethernet 0**
10. **exit**
11. **transport type persistent ssh input** *transport-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# `**`configure terminal`**	Enters global configuration mode.
Step 3	**transport-map type persistent ssh** *transport-map-name* **Example:** `Router(config)# `**`transport-map type persistent telnet telnethandler`**	Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] **Example:** `Router(config-tmap)# `**`connection wait interruptible`**	Specifies how a persistent SSH connection will be handled using this transport map: • **allow—**The SSH connection waits for a Cisco IOS VTY line to become available, and exits the router if interrupted. • **allow interruptible—**The SSH connection waits for the VTY line to become available, and also allows a user to enter diagnostic mode by interrupting an SSH connection waiting for the VTY line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none—**The SSH connection immediately enters diagnostic mode. • **none disconnect—**The SSH connection does not wait for the VTY line and does not enter diagnostic mode. Therefore, all SSH connections are rejected if no VTY line is immediately available.
Step 5	**rsa keypair-name** *rsa-keypair-name* **Example:** `Router(config)# `**`rsa keypair-name sshkeys`**	Names the RSA keypair to be used for persistent SSH connections. For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the **ip ssh rsa keypair-name** command, do not apply to persistent SSH connections. No *rsa-keypair-name* is defined by default.
Step 6	(Optional) **authentication-retries** *number-of-retries* **Example:** `Router(config-tmap)# `**`authentication-retries 4`**	(Optional) Specifies the number of authentication retries before dropping the connection. The default *number-of-retries* is 3.

	Command or Action	Purpose

Step 7	(Optional) **banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# ` **`banner diagnostic X`**
	`Enter TEXT message. End with the character 'X'.`
	`--Welcome to Diagnostic Mode--`
	`X`
	`Router(config-tmap)#`
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the VTY line because of the persistent SSH configuration.
		• **diagnostic—**Creates a banner message seen by users directed to diagnostic mode because of the persistent SSH configuration.
		• **wait—**Creates a banner message seen by users waiting for the VTY line to become available.
		• *banner-message*—The banner message, which begins and ends with the same delimiting character.

Step 8	(Optional) **time-out** *timeout-interval* **Example:** `Router(config-tmap)# ` **`time-out 30`**	(Optional) Specifies the SSH time-out interval, in seconds. The default *timeout-interval* is 120 seconds.
Step 9	**transport interface gigabitethernet 0** **Example:** `Router(config-tmap)# ` **`transport interface gigabitethernet 0`**	Applies the transport map settings to the Ethernet management interface (interface gigabitethernet 0). Persistent SSH can be applied only to the Ethernet management interface on the router.
Step 10	**exit** **Example:** `Router(config-tmap)# ` **`exit`**	Exits transport map configuration mode to re-enter global configuration mode.
Step 11	**transport type persistent ssh input** *transport-map-name* **Example:** `Router(config)# ` **`transport type persistent ssh input sshhandler`**	Applies the settings defined in the transport map to the Ethernet management interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent ssh** command.

Examples

The following example shows a transport map that will make all SSH connections wait for the VTY line to become active before connecting to the router being configured and applied to the Ethernet management interface (interface gigabitethernet 0). The RSA keypair is named `sshkeys`.

This example only uses the commands required to configure persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
```

```
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map is configured and will apply the following settings to users attempting to access the Ethernet management port via SSH:

- SSH users will wait for the VTY line to become active, but will enter diagnostic mode if the attempt to access the Cisco IOS software through the VTY line is interrupted.
- The RSA keypair name is sshkeys.
- The connection allows one authentication retry.
- The banner `--Welcome to Diagnostic Mode--` will appear if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner `--Waiting for vty line--` will appear if the connection is waiting for the VTY line to become active.
- The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH:

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for vty line--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

show transport-map [**all** | **name** *transport-map-name* | **type** [**console** | **persistent** [**ssh** | **telnet**]]]

This command can be used either in user EXEC mode or privileged EXEC mode.

Example

The following example shows transport maps that are configured on the router: a console port (`consolehandler`), persistent SSH (`sshhandler`), and persistent Telnet transport (`telnethandler`):

```
Router# show transport-map all
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:
Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: telnethandling1
Type: Persistent Telnet Transport

Connection:
Wait option: Wait Allow


Router# show transport-map type console
Transport Map:
Name: consolehandler
```

```
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map type persistent ssh
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Router# show transport-map type persistent telnet
Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: telnethandling1
Type: Persistent Telnet Transport

Connection:
Wait option: Wait Allow


Router# show transport-map name telnethandler
Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
```

```
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map name consolehandler
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map name sshhandler
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Router#
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait
Shell banner:
```

```
Wait banner :

Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

Example

The following example shows the **show platform software configuration access policy** command being issued both before and after a new transport map for SSH are configured. During the configuration, the connection policy and banners are set for a persistent SSH transport map, and the transport map for SSH is enabled.

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process


Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit

Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS process
```

```
Method : ssh
Rule : wait with interrupt
Shell banner:
Welcome to Diag Mode

Wait banner :
Waiting for IOS


Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

Configuring Auxiliary Port for Modem Connection

Cisco 4000 Series ISR supports connecting a modem to the router auxiliary port for EXEC dial in connectivity. When a modem is connected to the auxiliary port, a remote user can dial in to the router and configure it. To configure a modem on the auxiliary port, perform these steps:

Step 1 Connect the RJ-45 end of the adapter cable to the black AUX port on the router.

Step 2 Use the **show line** command to determine the async interface of the AUX port:

```
Router# show  line

 Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*     0 CTY             -   -   -  - -   0   0   0/0    -
      1 AUX   9600/9600 -   -   -  - -   0   0   0/0    -
      2 VTY             -   -   -  - -   0   0   0/0    -
      3 VTY             -   -   -  - -   0   0   0/0    -
      4 VTY             -   -   -  - -   0   0   0/0    -
      5 VTY             -    -  -  - -   0   0   0/0    -
      6 VTY             -    -  -  - -   0   0   0/0    -
```

Step 3 Use the following commands to configure the router AUX line::

```
Router(config)# line 1

Router(config-line)#modem inOut
Router(config-line)#modem autoconfigure type usr_sportster
Router(config-line)#speed 115200  [Speed to be set according to the modem manual]
Router(config-line)#stopbits 1 [Stopbits to be set according to the modem manual]
Router(config-line)#transport input all
Router(config-line)#flowcontrol hardware [flowcontrol to be set according to the modem manual]
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router(config)#enable password lab
```

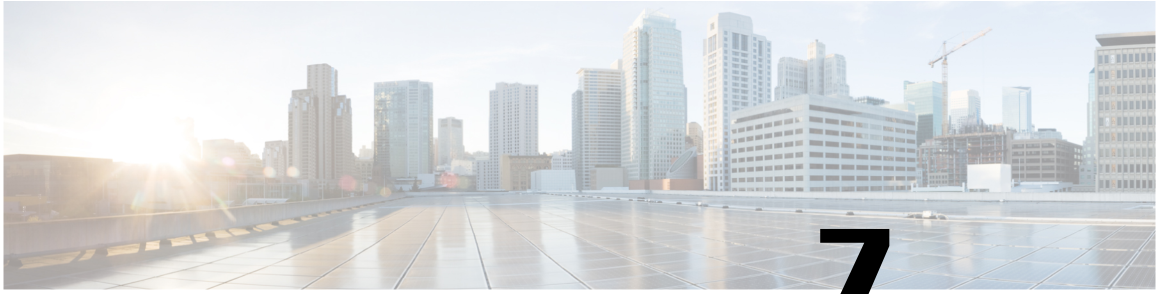
Step 4 Use the reverse telnet method on the modem to verify the modem connectivity and configuration string:

```
Router(config)#int loopback 0
Router(config-if)#ip add 1.1.1.1 255.255.255.0
Router(config-if)#end
Router#telnet 1.1.1.1 2001
Trying 1.1.1.1, 2001 ... Open

User Access Verification

Password: <enter the password given under line configuration>

at    <<<=== Modem command
OK  <<<=== This OK indicates that the modem is connected successully to the AUX port.
```

Step 5 Use an analog phone to verify that the phone line is active and functions properly. Then, connect the analog phone line to the modem.

Step 6 Initialize an EXEC modem call to the router from another device (PC) to test the modem connection.

Step 7 When the connection is established, the dial in client is prompted for a password. Enter the correct password.
Note: This password should match the one that is configured on the auxiliary port line.



CHAPTER 7

Installing the Software

This chapter includes the following sections:

Overview

Installing software on the router involves installing a consolidated package (bootable image). This consists of a bundle of subpackages (modular software units), with each subpackage controlling a different set of functions.

These are the two main methods to install the software:

- Managing and Configuring a Router to Run Using a Consolidated Package, on page 76—This method allows for individual upgrade of subpackages and generally has reduced boot times compared to the method below. Use this method if you want to individually upgrade a module's software.
- Managing and Configuring a Router to Run Using Individual Packages, on page 80—This a simple method that is similar to a typical Cisco router image installation and management that is supported across Cisco routers.

It is better to upgrade software in a planned period of maintenance when an interruption in service is acceptable. The router needs to be rebooted for a software upgrade to take effect.

ROMMON Images

A ROMMON image is a software package used by ROM Monitor (ROMMON) software on a router. The software package is separate from the consolidated package normally used to boot the router. For more information on ROMMON, see the "ROM Monitor Overview and Basic Procedures" section in the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

An independent ROMMON image (software package) may occasionally be released and the router can be upgraded with the new ROMMON software. For detailed instructions, see the documentation that accompanies the ROMMON image.

Note A new version of the ROMMON image is not necessarily released at the same time as a consolidated package for a router.

Provisioning Files

This section provides background information about the files and processes used in Managing and Configuring a Router to Run Using Individual Packages, on page 80.

The consolidated package on a router consists of a collection of subpackages and a provisioning file titled `packages.conf`. To run the software, the usual method used is to boot the consolidated package, which is copied into memory, expanded, mounted, and run within memory. The provisioning file's name can be renamed but subpackage file's names cannot be renamed. The provisioning file and subpackage files must be kept in the same directory. The provisioning file does not work properly if any individual subpackage file is contained within a different directory.

Note An exception to this is that if a new or upgraded module firmware package is subsequently installed, it need not be in the same directory as the provisioning file.

Configuring a router to boot, using the provisioning file packages.conf, is beneficial because no changes have to be made to the boot statement after the Cisco IOS XE software is upgraded.

Alternatively, for an example of booting using subpackages, see Configuring the Router to Boot Using Subpackages, on page 292.

File Systems

The following table provides a list of file systems that can be seen on the Cisco 4000 series routers.

Table 8: Router File Systems

File System	Description
bootflash:	Boot flash memory file system.

File System	Description
flash:	Alias to the boot flash memory file system above.
harddisk:	Hard disk file system (if NIM-SSD, NIM-HDD, or internal mSATA flash device is present in the router). **Note** The internal mSATA flash device is supported only on Cisco ISR4300 Series routers.
cns:	Cisco Networking Services file directory.
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
obfl:	File system for Onboard Failure Logging (OBFL) files.
system:	System memory file system, which includes the running configuration.
tar:	Archive file system.
tmpsys:	Temporary system files file system.
usb0: usb1:	The Universal Serial Bus (USB) flash drive file systems. **Note** The USB flash drive file system is visible only if a USB drive is installed in usb0: or usb1: ports.
usbtoken0: usbtoken1:	usbtoken file system. **Note** A usbtoken file system may not always be visible, because the file system is only visible when a usbtoken is inserted.

Use the **?** help option, or use the **copy** command in command reference guides, if you find a file system that is not listed in the table above.

Autogenerated File Directories and Files

This section discusses the autogenerated files and directories that can be created, and how the files in these directories can be managed.

Table 9: Autogenerated Files

File or Directory	Description
crashinfo files	Crashinfo files may appear in the bootflash: file system. These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, the files are not part of router operations, and can be erased without impacting the functioning of the router.

File or Directory	Description
core directory	The storage area for .core files. If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased.
lost+found directory	This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.
tracelogs directory	The storage area for trace files. Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure. Trace files, however, are not a part of router operations, and can be erased without impacting the router's performance.

Important Notes About Autogenerated Directories

Important information about autogenerated directories include:

- Autogenerated files on the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by Cisco customer support.

  Note Altering autogenerating files on the bootflash: may have unpredictable consequences for system performance.

- Crashinfo, core, and trace files can be deleted.

Flash Storage

Subpackages are installed to local media storage, such as flash. For flash storage, use the **dir bootflash:** command to list the file names.

Note Flash storage is required for successful operation of a router.

Configuring the Configuration Register for Autoboot

The configuration register can be used to change router behavior. This includes controlling how the router boots. Set the configuration register to 0x0 to boot into ROM, by using one of the following commands:

- In Cisco IOS configuration mode, use the **config-reg** 0x0 command.
- From the ROMMON prompt, use the **confreg** 0x0 command.

For more information about the configuration register, see Use of the Configuration Register on All Cisco Routers and Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example, on page 77.

Note Setting the configuration register to 0x2102 will set the router to autoboot the Cisco IOS XE software.

Note The console baud rate is set to 9600 after changing the **confreg** to 0x2102 or 0x0. If you cannot establish a console session after setting **confreg**, or garbage output appears, change the setting on your terminal emulation software to 9600.

Licensing

Cisco Software Licensing

Cisco software licensing consists of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.

You can enable licensed features and store license files in the bootflash of your router. Licenses pertain to consolidated packages, technology packages, or individual features.

An evaluation license is automatically converted to a Right to Use model after 60 days and this license is valid permanently. The conversion to a permanent license applies only to evaluation licenses. For other features supported on your router, you must purchase a permanent license.

See the "Configuring the Cisco IOS Software Activation Feature" chapter of the Software Activation Configuration Guide, Cisco IOS XE Release 3S.

Consolidated Packages

One of the following two consolidated packages (images) is preinstalled on the router:

- **universalk9**—Contains the **ipbasek9** base package and the **securityk9**, **uck9**, and **appxk9** technology packages.

- **universalk9_npe—**Contains the **ipbasek9** base package and the **securityk9_npe**, **uck9**, and **appxk9** technology packages. This image has limited crypto functionality.

  Note The term npe stands for No Payload Encryption.

Note The terms super package and image also refer to a consolidated package.

To obtain software images for the router, go to http://software.cisco.com/download/navigator.html.

An image-based license is used to help bring up all the subsystems that correspond to a license. This license is enforced only at boot time.

Apart from the **universalk9** and **universalk9_npe** images, a Boot ROMMON image is available. For more information, see ROMMON Images, on page 68.

For more information about identifying digitally signed Cisco software and how to show the digital signature information of an image file, see the "Digitally Signed Cisco Software" section in the Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S.

The following examples show how to obtain software authenticity information and internal details of a package:

- Displaying Digitally Signed Cisco Software Signature Information, on page 299
- Obtaining the Description of a Module or Consolidated Package, on page 302

Many features within the consolidated package are contained in the **ipbasek9** base package. The license key for the **ipbasek9** package is activated by default.

Technology Packages

Technology packages contain software features within a consolidated package. To use different sets of features, enable the licenses of selected technology packages. You can enable the licenses for any combination of technology packages.

Each technology package has an evaluation license that converts to a Right to Use (RTU) license after 60 days and is then valid permanently.

The following is a list of technology packages:

- securityk9, on page 72
- uck9, on page 73
- appxk9, on page 73

securityk9

The **securityk9** technology package includes all crypto features, including IPsec, SSL/SSH, Firewall, and Secure VPN.

The **securityk9_npe** package (npe = No Payload Encryption) includes all the features in the **securityk9** technology package without the payload-encryption functionality. This is to fulfill export restriction requirements. The **securityk9_npe** package is available only in the **universalk9_npe** image. The difference in features between the **securityk9** package and the **securityk9_npe** package is therefore the set of payload-encryption-enabling features such as IPsec and Secure VPN.

uck9

The **uck9** technology package includes the following Cisco Unified Communications features:

- CUBE
- CME-SRST
- SBC

appxk9

The **appxk9** technology package contains Application Experience features, which are similar to the features in the DATA package of the Cisco Integrated Services Routers Generation 2 routers. For more information, see: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/software-activation-on-integrated-services-routers-isr/white_paper_c11_556985.html#wp9000791.

There are many features in the **appxk9** package, including MPLS, PfR, L2/L3 VPN, Broadband, and AVC.

Feature Licenses

To use each of the following features, enable a corresponding feature license, as explained in the following sections:

- HSECK9, on page 73
- Performance, on page 74
- CME-SRST, on page 74

HSECK9

The **HSECK9** license is required for a feature to have full crypto functionality. Without the **HSECK9** license, only 225 secure tunnels and 85 Mbps of crypto bandwidth would be available. The **HSECK9** license allows features in the **securityk9** technology package to use the maximum number of secure tunnels and crypto bandwidth. To enable the **HSECK9** license, purchase the **FL-44-HSEC-K9** license from Cisco.com and install it using the **license install** *license-files* command. For further information on obtaining and installing feature licenses, see Configuring the Cisco IOS Software Activation Feature.

Note The **HSECK9** feature does not have an evaluation license that converts to an RTU license after 60 days; a feature license must be obtained.

To enable the license for the **HSECK9** feature, the **securityk9** technology package is also required. For more information about the **securityk9** technology package, see securityk9, on page 72.

Performance

The performance feature, which allows for increased throughput, is enabled by the performance license. This feature is part of the **ipbasek9** technology package. To enable the feature, order the performance license (part number FL-44-PERF-K9). The license is displayed as the throughput license.

To configure the feature, use the **platform hardware throughput level** *throughput* command in the global configuration mode:

```
platform hardware throughput level throughput
```

CME-SRST

The CME-SRST feature requires the **uck9** technology package. To activate the CME-SRST feature license, see Activating the CME-SRST Feature License, on page 74.

Activating the CME-SRST Feature License

Before You Begin

Ensure the following:

- License for **uck9** technology package is available.
- The CME-SRST feature is configured.

SUMMARY STEPS

1. **show license detail cme-srst**
2. **configure terminal**
3. **license accept end user agreement**
4. **exit**
5. **show license detail cme-srst**
6. **write memory**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show license detail cme-srst** **Example:** `Router# show license detail cme-srst`	Displays the available CME-SRST license. **Note** The EULA should be in NOT ACCEPTED state.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**license accept end user agreement** **Example:** `Router# license accept end user agreement`	Configures a one-time acceptance of the EULA for the CME-SRST license. Accept the EULA by typing YES.
Step 4	**exit** **Example:** `Router# exit`	Exits global configuration mode.
Step 5	**show license detail cme-srst** **Example:** `Router# show license detail cme-srst`	Displays the available CME-SRST license. **Note** The EULA should be in ACCEPTED state.
Step 6	**write memory** **Example:** `Router# write memory`	Saves configuration.

Unlicensed Feature: Example

If you try to use a feature that is part of a package that is not enabled, an error message is displayed.

In the following example, the **crypto map** command is called during configuration and an error message is displayed. This is because, the feature associated with **crypto map** is part of the **securityk9** package and the **securityk9** package is not enabled.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto map
^
% Invalid input detected at '^' marker.
```

Use the **show license feature** command to view the license features that are enabled. In the following example, the **securityk9** and the **uck9** packages are not enabled.

Note **ipbasek9** is provided by default.

```
Router# show license feature
Feature name             Enforcement  Evaluation  Subscription   Enabled  RightToUse
appxk9                   yes          yes         no             yes      yes
uck9                     yes          yes         no             no       yes
securityk9               yes          yes         no             no       yes
ipbasek9                 no           no          no             yes      yes
```

LED Indicators

For information on LEDs on the router, see "LED Indicators" in the "Overview" section of the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

For information on LEDs on the SSD Carrier Card NIM, see "Overview of the SSD Carrier Card NIM (NIM-SSD)" in the "Installing and Upgrading Internal Modules and FRUs" section of the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

Related Documentation

For further information on software licenses, see Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2.

For further information on obtaining and installing feature licenses, see Configuring the Cisco IOS Software Activation Feature.

How to Install and Upgrade the Software

To install or upgrade the software, use one of the following methods to use the software from a consolidated package or an individual package. Also see Overview, on page 67.

- Managing and Configuring a Router to Run Using a Consolidated Package, on page 76
- Managing and Configuring a Router to Run Using Individual Packages, on page 80

Managing and Configuring a Router to Run Using a Consolidated Package

Note Do not use these procedures if you also need to install any optional subpackages or plan to upgrade individual subpackages. See Managing and Configuring a Router to Run Using Individual Packages, on page 80.

- Managing and Configuring a Consolidated Package Using copy and boot Commands, on page 76
- Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example, on page 77

Managing and Configuring a Consolidated Package Using copy and boot Commands

To upgrade a consolidated package, copy the consolidated package to the **bootflash:** directory on the router using the **copy** command. After making this copy of the consolidated package, configure the router to boot using the consolidated package file.

The following example shows the consolidated package file being copied to the **bootflash:** file system via TFTP. The config register is then set to boot using **boot system** commands, and the **boot system** commands instruct the router to boot using the consolidated package stored in the **bootflash:** file system. The new configuration is then saved using the **copy running-config startup-config** command, and the system is then reloaded to complete the process.

```
Router# dir bootflash:
Directory of bootflash:/
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer

928862208 bytes total (712273920 bytes free)

Router# copy tftp: bootflash:
Address or name of remote host []? 172.17.16.81
Source filename []? /auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
Destination filename [isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin]?
Accessing
tftp://172.17.16.81//auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
...
Loading /auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin from
172.17.16.81 (via GigabitEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00
isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
928862208 bytes total (503156736 bytes free)
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash bootflash:isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
Router(config)# config-reg 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system flash bootflash:isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
boot-end-marker
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
```

Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router# show run | include boot
boot-start-marker
boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
```

```
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with

reload chassis code


Initializing Hardware ...

System integrity status: c0000600
Failures detected:
Boot FPGA corrupt


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 424317088 (0x194a90a0) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
expected 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5116 msec
Image validated
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (local/local): load_modules took: 2 seconds,
expected max time 2 seconds
```

```
Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
15.4(20140527:095327)
[v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 27-May-14 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Warning: the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.


Press RETURN to get started!


Router>
Router>
Router>enable
Router# show version
Cisco IOS XE Software, Version BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ext
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
15.4(20140527:095327)
v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]

IOS XE Version: BLD_V154_3_S_XE313_THROTTLE_LATEST
```

```
Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: adventerprise
License Type: EvalRightToUse
--More-- Next reload license Level: adventerprise

cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Configuration register is 0x2102
```

Managing and Configuring a Router to Run Using Individual Packages

To choose between running individual packages or a consolidated package, see Overview, on page 67.

The following topics are included in this section:

- Installing Subpackages from a Consolidated Package, on page 80
- Installing a Firmware Subpackage, on page 91

Installing Subpackages from a Consolidated Package

Perform the following procedure to obtain the consolidated package from a TFTP server.

Another variation of this procedure obtains the consolidated package from a USB flash drive. This is described in Installing Subpackages from a Consolidated Package on a Flash Drive, on page 86.

Before You Begin

Copy the consolidated package to the TFTP server.

SUMMARY STEPS

1. **show version**
2. **dir bootflash:**
3. **show platform**
4. **mkdir bootflash:** *URL-to-directory-name*
5. **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*
6. **reload**
7. **boot** *URL-to-directory-name*/**packages.conf**
8. **show version installed**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show version**
	Example:
	`Router# show version`
	`Cisco IOS Software, IOS-XE Software`
	`(X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental`
	`Version 15.3(20120627:221639) [build_151722 111]`
	`Copyright (c) 1986-2012 by Cisco Systems, Inc.`
	`Compiled Thu 28-Jun-12 15:17 by mcpre`
	`.`
	`.`
	`.`
		Shows the version of software running on the router. This can later be compared with the version of software to be installed.

Step 2	**dir bootflash:** **Example:** `Router# dir bootflash:`	Displays the previous version of software and that a package is present.

Step 3	**show platform**
	Example:
	`Router# show platform`
	`Chassis type: ISR4451/K9`
		Displays the inventory.

Step 4	**mkdir bootflash:** *URL-to-directory-name* **Example:** `Router# mkdir bootflash:mydir`	Creates a directory to save the expanded software image. You can use the same name as the image to name the directory.
Step 5	**request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*	Expands the software image from the TFTP server (*URL-to-consolidated-package*) into the directory used to save the image (*URL-to-directory-name*), which was created in Step 4.

	Command or Action	Purpose
	Example: `Router#  request platform software package expand file bootflash:isr4400-universalk9-NIM.bin to bootflash:mydir`	

Step 6	**reload**
	Example:
	`Router# reload`
	`rommon >`
		Enables ROMMON mode, which allows the software in the consolidated file to be activated.

Step 7	**boot** *URL-to-directory-name*/**packages.conf** **Example:** `rommon 1 > boot bootflash:mydir/packages.conf`	Boots the consolidated package, by specifying the path and name of the provisioning file: packages.conf.

Step 8	**show version installed**
	Example:
	`Router# show version installed`
	`Package: Provisioning File, version: n/a, status: active`
		Displays the version of the newly installed software.

Examples

The initial part of the example shows the consolidated package, isr4400-universalk9.164422SSA.bin, being copied to the TFTP server. This is a prerequisite step. The remaining part of the example shows the consolidated file, packages.conf, being booted.

```
Router# copy tftp:isr4400/isr4400-universalk9.164422SSA.bin bootflash:
Address or name of remote host []? 1.1.1.1
Destination filename [isr4400-universalk9.164422SSA.bin]?
Accessing tftp://1.1.1.1/isr4400/isr4400-universalk9.164422SSA.bin...
Loading isr4400/isr4400-universalk9.164422SSA.bin from 1.1.1.1 (via GigabitEthernet0):
!!!!!!!!
[OK - 410506248 bytes]

410506248 bytes copied in 338.556 secs (1212521 bytes/sec)


Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version

15.3(20120627:221639) [build_151722 111]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 28-Jun-12 15:17 by mcpre

IOS XE Version: 2012-06-28_15.31_mcpre

Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
```

```
software.


ROM: IOS-XE ROMMON

Router uptime is 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp:isr4400/isr4400.bin"
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: adventerprise
License Type: EvalRightToUse
Next reload license Level: adventerprise
cisco ISR4451/K9 (2RU) processor with 1136676K/6147K bytes of memory.
Processor board ID FGL161611AB
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.

Configuration register is 0x8000

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 May 3 2012 19:58:37 +00:00 lost+found
178465 drwx 4096 Jun 6 2012 15:20:20 +00:00 core
584065 drwx 4096 Jul 13 2012 19:19:00 +00:00 .prst_sync
405601 drwx 4096 May 3 2012 19:59:30 +00:00 .rollback_timer
113569 drwx 40960 Jul 13 2012 19:19:32 +00:00 tracelogs
64897 drwx 4096 May 3 2012 19:59:42 +00:00 .installer
13 -rw- 1305 May 7 2012 17:43:42 +00:00 startup-config
14 -rw- 1305 May 7 2012 17:43:55 +00:00 running-config
15 -r-- 1541 Jun 4 2012 18:32:41 +00:00 debug.conf
16 -rw- 1252 May 22 2012 19:58:39 +00:00 running-config-20120522
519169 drwx 4096 Jun 4 2012 15:29:01 +00:00 vman_fdb

7451738112 bytes total (7067635712 bytes free)



Router# show platform
Chassis type: ISR4451/K9

Slot         Type                 State                 Insert time (ago)
---------    ------------------- --------------------- -----------------
0            ISR4451/K9           ok                    15:57:33
 0/0         ISR4451-6X1GE        ok                    15:55:24
1            ISR4451/K9           ok                    15:57:33
 1/0         SM-1T3/E3            ok                    15:55:24
2            ISR4451/K9           ok                    15:57:33
 2/0         SM-1T3/E3            ok                    15:55:24
R0           ISR4451/K9           ok, active            15:57:33
F0           ISR4451-FP           ok, active            15:57:33
P0           Unknown              ps, fail              never
P1           XXX-XXXX-XX          ok                    15:56:58
P2           ACS-4450-FANASSY     ok                    15:56:58
```

```
Slot         CPLD Version        Firmware Version
---------    ------------------- ---------------------------------------
0            12090323            15.3(01r)S [ciscouser-ISRRO...
1            12090323            15.3(01r)S [ciscouser-ISRRO...
2            12090323            15.3(01r)S [ciscouser-ISRRO...
R0           12090323            15.3(01r)S [ciscouser-ISRRO...
F0           12090323            15.3(01r)S [ciscouser-ISRRO...

Router# mkdir bootflash:isr4400-universalk9.dir1
Create directory filename [isr4400-universalk9.dir1]?
Created dir bootflash:/isr4400-universalk9.dir1
Router# request platform software package expand file bootflash:isr4400-universalk9.NIM.bin

to bootflash:isr4400-universalk9.dir1
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console.Reload Reason: Reload
Command.

rommon 1 > boot bootflash:isr4400-universalk9.dir1/packages.conf

File size is 0x00002836
Located isr4400-universalk9.dir1/packages.conf
Image size 10294 inode num 324484, bks cnt 3 blk size 8*512
#
File is comprised of 1 fragments (33%)

is_valid_sha1hash: SHA-1 hash:
calculated 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
expected 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
File size is 0x04b3dc00
Located isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg
Image size 78896128 inode num 324491, bks cnt 19262 blk size 8*512
###########################################################################################
File is comprised of 21 fragments (0%)
.....



Router# show version installed
Package: Provisioning File, version: n/a, status: active
File: bootflash:isr4400-universalk9.dir1/packages.conf, on: RP0
Built: n/a, by: n/a
File SHA1 checksum: ad09affd3f8820f4844f27acc1add502e0b8f459

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg, on:
 RP0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e
Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7
```

```
Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: dir1, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb
Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge-BLD-BLD_MCP_DEV_LATEST_20120710
_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpcontrol-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: 2012-07-10_16.23_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpios-universalk9-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb

Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpaccess-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpbase-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes-BLD-BLD_MCP_DEV_LATEST
_20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
```

```
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_sp2700-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
```

Installing Subpackages from a Consolidated Package on a Flash Drive

The steps for installing subpackages from a consolidated package on a USB flash drive are similar to those described in Installing Subpackages from a Consolidated Package, on page 80.

Step 1 **show version**

Step 2 **dir usb***n***:**

Step 3 **show platform**

Step 4 **mkdir bootflash:***URL-to-directory-name*

Step 5 **request platform software package expand fileusb*n*:** ***package-name to URL-to-directory-name***

Step 6 **reload**

Step 7 **boot** *URL-to-directory-name/***packages.conf**

Step 8 **show version installed**

How to Install and Upgrade the Software for Cisco IOS XE Denali Release16.3

To install or upgrade the software, use one of the following methods to use the software from a consolidated package or an individual package. Also see Overview, on page 67.

- Managing and Configuring a Router to Run Using a Consolidated Package, on page 76
- Managing and Configuring a Router to Run Using Individual Packages, on page 80
- Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example, on page 77
- Upgrading to Cisco IOS XE Denali Release 16.3, on page 86

Upgrading to Cisco IOS XE Denali Release 16.3

Upgrading the device to Cisco IOS XE Denali Release 16.3 for the first time uses the same procedures as specified in the earlier section. In addition, Cisco IOS XE Denali Release 16.3 requires a minimum ROMMON version. When the device boots up with Cisco IOS XE Denali image for the first time, the device checks the installed version of the ROMMON, and upgrades if the system is running an older version. During the upgrade, do not power cycle the device. The system automatically power cycles the device after the new ROMMON is installed. After the installation, the system will boot up with the Cisco IOS XE image as normal.

Note When the device boots up for first time and if the device requires an upgrade, the entire boot process may take several minutes. This process will be longer than a normal boot due to the ROMMON upgrade.

The following example illustrates the boot process of a consolidated package:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router# show run | include boot
boot-start-marker
boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with

reload chassis code


Initializing Hardware ...

System integrity status: c0000600


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 504063931 (0x1e0b67bb) bytes
```

```
ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
expected 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5116 msec
Image validated


Detected old ROMMON version 12.2(20150910:184432), upgrade required
Upgrading to newer ROMMON version required by this version of IOS-XE, do not power cycle
the system.  A reboot will automatically occur for the new ROMMON to take effect.
selected : 1
Booted : 1
Reset Reason: 1

Info: Upgrading entire flash from the rommon package
Switching to ROM 0
Upgrade image MD5 signature is b702a0a59a46a20a4924f9b17b8f0887
Upgrade image MD5 signature verification is b702a0a59a46a20a4924f9b17b8f0887
Switching back to ROM 1
ROMMON upgrade complete.

To make the new ROMMON permanent, you must restart the RP.
ROMMON upgrade successful.  Rebooting for upgrade to take effect.


Initializing Hardware ...

System integrity status: 00300610
Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed

Expected hash:
ddaf35a193617abacc417349ae204131
12e6fa4e89a97ea20a9eeee64b55d39a
2192992a274fc1a836ba3c23a3feebbd
454d4423643ce80e2a9ac94fa54ca49f

Obtained hash:
ddaf35a193617abacc417349ae204131
12e6fa4e89a97ea20a9eeee64b55d39a
2192992a274fc1a836ba3c23a3feebbd
454d4423643ce80e2a9ac94fa54ca49f
ROM:Sha512 Self Test Passed
Self Tests Latency: 418 msec
Rom image verified correctly


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

CPLD Version: 33 (MM/DD/YY): 06/23/14 Cisco ISR4351/K9 Slot:0

Current image running: Boot ROM1

Last reset cause: ResetRequest
Reading confreg 0x2102
Reading monitor variables from NVRAM
Enabling interrupts...done

Checking for PCIe device presence...done
Cisco ISR4351/K9 platform with 16777216 Kbytes of main memory

autoboot entry: NVRAM VALUES: bootconf: 0x0, autobootstate: 0
autobootcount: 0, autobootsptr: 0x0
Rommon upgrade requested
Flash upgrade reset 0 in progress
.......
Initializing Hardware ...

Checking for PCIe device presence...done
Reading confreg 2102
System integrity status: 0x300610
Key Sectors:(Primary, GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 288
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Rom image verified correctly


System Bootstrap, Version 16.2(1r), RELEASE SOFTWARE
Copyright (c) 1994-2016  by cisco Systems, Inc.


Current image running: *Upgrade in progress* Boot ROM0

Last reset cause: BootRomUpgrade
ISR4351/K9 platform with 16777216 Kbytes of main memory

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 504063931 (0x1e0b67bb) bytes


Image Base is: 0x56834018
Image Size is: 0x1E089706
Package header rev 1 structure detected
Package type:30000, flags:0x0
IsoSize = 503874534
Parsing package TLV info:
```

```
000: 000000090000001D4B45595F544C565F -         KEY_TLV_
010: 5041434B4147455F434F4D5041544942 - PACKAGE_COMPATIB
020: 494C49545900000000000000090000000B - ILITY
030: 4652555F52505F545950450000000009 - FRU_RP_TYPE
040: 000000184B45595F544C565F5041434B -     KEY_TLV_PACK
050: 4147455F424F4F54415243480000000009 - AGE_BOOTARCH
060: 0000000E415243485F693638365F5459 -     ARCH_i686_TY
070: 5045000000000000900000144B45595F - PE          KEY_
080: 544C565F424F4152445F434F4D504154 - TLV_BOARD_COMPAT
090: 00000009000000012424F4152445F6973 -         BOARD_is
0A0: 72343330305F54595045000000000009 - r4300_TYPE
0B0: 000000184B45595F544C565F43525950 -     KEY_TLV_CRYP
0C0: 544F5F4B4559535452494E4700000009 - TO_KEYSTRING

TLV: T=9, L=29, V=KEY_TLV_PACKAGE_COMPATIBILITY
TLV: T=9, L=11, V=FRU_RP_TYPE
TLV: T=9, L=24, V=KEY_TLV_PACKAGE_BOOTARCH
TLV: T=9, L=14, V=ARCH_i686_TYPE
TLV: T=9, L=20, V=KEY_TLV_BOARD_COMPAT
TLV: T=9, L=18, V=BOARD_isr4300_TYPE
TLV: T=9, L=24, V=KEY_TLV_CRYPTO_KEYSTRING
TLV: T=9, L=10, V=EnCrYpTiOn
TLV: T=9, L=11, V=CW_BEGIN=$$
TLV: T=9, L=19, V=CW_FAMILY=$isr4300$
TLV: T=9, L=59, V=CW_IMAGE=$isr4300-universalk9.2016-06-29_23.31_paj.SSA.bin$
TLV: T=9, L=19, V=CW_VERSION=$16.3.1$
TLV: T=9, L=52, V=CW_DESCRIPTION=$Cisco IOS Software, IOS-XE Software$
TLV: T=9, L=9, V=CW_END=$$
Found DIGISIGN TLV type 12 length = 392
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Found package arch type ARCH_i686_TYPE
Found package FRU type FRU_RP_TYPE
Calculating SHA-1 hash...Validate package: SHA-1 hash:
 calculated 8B082C48:35C23C9E:8A091441:D6FACEE6:B5111533
 expected   8B082C48:35C23C9E:8A091441:D6FACEE6:B5111533

Image validated

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
16.3(20160527:095327)
[v163_throttle]
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 27-May-16 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2016 by cisco Systems, Inc.
```

```
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Warning: the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.


Press RETURN to get started!
```

Installing a Firmware Subpackage

Before You Begin

Obtain a consolidated package that contains your required firmware package and expand the package. (See Managing and Configuring a Router to Run Using Individual Packages, on page 80.) Make a note of the location and name of the firmware package and use this information in the steps below for *URL-to-package-name*.

You can install a firmware subpackage if the router has been configured using, for example, Managing and Configuring a Router to Run Using Individual Packages, on page 80.

Firmware subpackages are not released individually. You can select a firmware package from within a consolidated package after expanding the consolidated package. The firmware package can then be installed as shown in the procedure below.

Note Read the Release Notes document pertaining to the consolidated package to verify that the firmware within the consolidated package is compatible with the version of Cisco IOS XE software that is currently installed on a router.

SUMMARY STEPS

1. **show version**
2. **dir bootflash:**
3. **show platform**
4. **mkdir bootflash:** *URL-to-directory-name*
5. **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*
6. **reload**
7. **boot** *URL-to-directory-name* **/packages.conf**
8. **show version installed**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show version**
	Example:
	`Router# show version`
	`Cisco IOS Software, IOS-XE Software`
	`(X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental`
	`Version 15.3(20120627:221639) [build_151722 111]`
	`Copyright (c) 1986-2012 by Cisco Systems, Inc.`
	`Compiled Thu 28-Jun-12 15:17 by mcpre`
	`.`
	`.`
	`.`
		Shows the version of software running on the router. This can later be compared with the version of software to be installed.

Step 2	**dir bootflash:** **Example:** `Router# dir bootflash:`	Displays the previous version of software and that a package is present.

Step 3	**show platform**
	Example:
	`Router# show platform`
	`Chassis type: ISR4451/K9`
		Checks the inventory.
		Also see the example in Installing Subpackages from a Consolidated Package, on page 80.

Step 4	**mkdir bootflash:** *URL-to-directory-name* **Example:** `Router# mkdir bootflash:mydir`	Creates a directory to save the expanded software image. You can use the same name as the image to name the directory.

Step 5	**request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*
	Example:
	`Router#  request platform software package expand file`
	`bootflash:isr4400-universalk9-NIM.bin to`
	`bootflash:mydir`
		Expands the software image from the TFTP server (*URL-to-consolidated-package*) into the directory used to save the image (*URL-to-directory-name*), which was created in the Step 4.

	Command or Action	Purpose

Step 6	**reload**
	Example:
	`Router# reload`
	`rommon >`
		Enables ROMMON mode, which allows the software in the consolidated file to be activated.

Step 7	**boot** *URL-to-directory-name* **/packages.conf** **Example:** `rommon 1 > boot bootflash:mydir/packages.conf`	Boots the consolidated package by specifying the path and name of the provisioning file: packages.conf.

Step 8	**show version installed**
	Example:
	`Router# show version installed`
	`Package: Provisioning File, version: n/a, status: active`
		Displays the version of the newly installed software.

Examples

The initial part of the following example shows the consolidated package, isr4400-universalk9.164422SSA.bin, being copied to the TFTP server. This is a prerequisite step. The remaining part of the example shows the consolidated file, packages.conf, being booted.

```
Router# tftp:isr4400/isr4400-universalk9.164422SSA.bin bootflash:
Address or name of remote host []? 1.1.1.1
Destination filename [isr4400-universalk9.164422SSA.bin]?
Accessing tftp://1.1.1.1/isr4400/isr4400-universalk9.164422SSA.bin...
Loading isr4400/isr4400-universalk9.164422SSA.bin from 1.1.1.1 (via GigabitEthernet0):
!!!!!!!!
[OK - 410506248 bytes]

410506248 bytes copied in 338.556 secs (1212521 bytes/sec)


Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version

15.3(20120627:221639) [build_151722 111]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 28-Jun-12 15:17 by mcpre

IOS XE Version: 2012-06-28_15.31_mcpre

Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp:isr4400/isr4400.bin"
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: adventerprise
License Type: EvalRightToUse
Next reload license Level: adventerprise
cisco ISR4451/K9 (2RU) processor with 1136676K/6147K bytes of memory.
Processor board ID FGL161611AB
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.

Configuration register is 0x8000

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 May 3 2012 19:58:37 +00:00 lost+found
178465 drwx 4096 Jun 6 2012 15:20:20 +00:00 core
584065 drwx 4096 Jul 13 2012 19:19:00 +00:00 .prst_sync
405601 drwx 4096 May 3 2012 19:59:30 +00:00 .rollback_timer
113569 drwx 40960 Jul 13 2012 19:19:32 +00:00 tracelogs
64897 drwx 4096 May 3 2012 19:59:42 +00:00 .installer
13 -rw- 1305 May 7 2012 17:43:42 +00:00 startup-config
14 -rw- 1305 May 7 2012 17:43:55 +00:00 running-config
15 -r-- 1541 Jun 4 2012 18:32:41 +00:00 debug.conf
16 -rw- 1252 May 22 2012 19:58:39 +00:00 running-config-20120522
519169 drwx 4096 Jun 4 2012 15:29:01 +00:00 vman_fdb

7451738112 bytes total (7067635712 bytes free)



Router# show platform
Chassis type: ISR4451/K9

Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 ISR4451/K9 ok 15:57:33
0/0 ISR4451-6X1GE ok 15:55:24
1 ISR4451/K9 ok 15:57:33
1/0 SM-1T3/E3 ok 15:55:24
2 ISR4451/K9 ok 15:57:33
2/0 SM-1T3/E3 ok 15:55:24
R0 ISR4451/K9 ok, active 15:57:33
F0 ISR4451-FP ok, active 15:57:33
P0 Unknown ps, fail never
P1 XXX-XXXX-XX ok 15:56:58
P2 ACS-4450-FANASSY ok 15:56:58

Slot CPLD Version Firmware Version
--------- ------------------- ---------------------------------------
0 12090323 15.3(01r)S [ciscouser-ISRRO...
1 12090323 15.3(01r)S [ciscouser-ISRRO...
2 12090323 15.3(01r)S [ciscouser-ISRRO...
R0 12090323 15.3(01r)S [ciscouser-ISRRO...
F0 12090323 15.3(01r)S [ciscouser-ISRRO...
```

```
Router# mkdir bootflash:isr4400-universalk9.dir1
Create directory filename [isr4400-universalk9.dir1]?
Created dir bootflash:/isr4400-universalk9.dir1
Router# request platform software package expand file bootflash:isr4400-universalk9.NIM.bin
 to
 bootflash:isr4400-universalk9.dir1
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.

rommon 1 > boot bootflash:isr4400-universalk9.dir1/packages.conf

File size is 0x00002836
Located isr4400-universalk9.dir1/packages.conf
Image size 10294 inode num 324484, bks cnt 3 blk size 8*512
#
File is comprised of 1 fragments (33%)

is_valid_sha1hash: SHA-1 hash:
calculated 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
expected 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
File size is 0x04b3dc00
Located isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg
Image size 78896128 inode num 324491, bks cnt 19262 blk size 8*512
##########################################################################################
File is comprised of 21 fragments (0%)
.....



Router# show version installed
Package: Provisioning File, version: n/a, status: active
File: bootflash:isr4400-universalk9.dir1/packages.conf, on: RP0
Built: n/a, by: n/a
File SHA1 checksum: ad09affd3f8820f4844f27acc1add502e0b8f459

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg, on:
 RP0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e
Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
```

```
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: dir1, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb
Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpcontrol-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: 2012-07-10_16.23_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpios-universalk9-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb

Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpaccess-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpbase-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_sp2700-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
```

Upgrading the Firmware on xDSL NIMs

To upgrade the firmware on a xDSL Network Interface Module (NIM), perform these steps:

Before You Begin

When you boot the router in packages.conf mode with the Cisco IOS XE image (super package) during the installation period, you can upgrade or downgrade the firmware without reloading the router. You need to follow the steps described in Installing a Firmware Subpackage, on page 91 before proceeding with the firmware upgrade.

If you do not boot the router in packages.conf mode with the Cisco IOS XE image, you need to follow the below prerequisites before proceeding with the firmware upgrade:

- Copy the firmware subpackage (NIM firmware) into bootflash:/mydir.
- Send a request to the platform software package expand file *boot flash:/mydir/<IOS-XE image>* to expand the super package.
- Reload the hardware module subslot to boot the module with the new firmware.
- Verify that the module is booted up with the new firmware using the **show platform software subslot x/y module firmware** command.

SUMMARY STEPS

1. copy Cisco IOS XE image into bootflash: **mydir**.
2. **request platform software package expand file** *bootflash:/mydir /<IOS-XE image* to expand super package.
3. **reload**.
4. **boot bootflash:mydir/ /packages.conf**.
5. **copy** NIM firmware subpackage to the folder **bootflash:mydir/**.
6. **request platform software package install** *rp 0 file bootflash:/mydir/<firmware subpackage>*.
7. **hw-module subslot x/y reload** to boot the module with the new firmware.
8. **show platform software subslot 0/2 module firmware** to verify that the module is booted up with the new firmware.

DETAILED STEPS

	Command or Action	Purpose
Step 1	copy Cisco IOS XE image into bootflash: **mydir**. **Example:** `Router# mkdir bootflash:mydir`	Creates a directory to save the expanded software image. You can use the same name as the image to name the directory.

	Command or Action	Purpose
Step 2	**request platform software package expand file** *bootflash:/mydir /<IOS-XE image* to expand super package. **Example:** Router# **request platform software package expand file bootflash:/mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin**	Expands the platform software package to super package.
Step 3	**reload**. **Example:** Router# **reload** rommon >	Enables ROMMON mode, which allows the software in the super package file to be activated.
Step 4	**boot bootflash:mydir/ /packages.conf**. **Example:** rommon 1 > **boot bootflash:mydir/packages.conf**	Boots the super package by specifying the path and name of the provisioning file: packages.conf.
Step 5	**copy** NIM firmware subpackage to the folder **bootflash:mydir**/. **Example:** Router#**copy bootflash:isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg bootflash:mydir/**	Copies the NIM firmware subpackage into bootflash:mydir.
Step 6	**request platform software package install** *rp 0 file bootflash:/mydir/<firmware subpackage>*. **Example:** Router#**equest platform software package install rp 0 file bootflash:mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg**	Installs the software package.
Step 7	**hw-module subslot x/y reload** to boot the module with the new firmware. **Example:** Router#**hw-module subslot 0/2 reload**	Reloads the hardware module subslot and boots the module with the new firmware.
Step 8	**show platform software subslot 0/2 module firmware** to verify that the module is booted up with the new firmware. **Example:** Router# **show platform software subslot 0/2 module firmware** Pe	Displays the version of the newly installed firmware.

Examples

The following example shows how to perform firmware upgrade in a router module:

```
Routermkdir bootflash:mydir
Create directory filename [mydir]?
Created dir bootflash:/mydir
Router#c
Router#copy bootflash:isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin bootflash:mydir/
Destination filename [mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin]?
```

```
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCC
425288648 bytes copied in 44.826 secs (9487544 bytes/sec)
Router#
Router#
Router#dir bootflash:mydir
Directory of bootflash:/mydir/

632738  -rw-        425288648  Dec 12 2014 09:16:42 +00:00
isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin

7451738112 bytes total (474025984 bytes free)
Router#

Router#request platform software package
expand file bootflash:/mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router#reload
Proceed with reload? [confirm]

*Dec 12 09:26:09.874: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.Dec 12 09:26:25.156 R0/0: %PMAN-5-EXITACTION: Process manager is exiting:
process exit with reload chassis code


Initializing Hardware ...

System integrity status: 00000610
 Rom image verified correctly
 System Bootstrap, Version 15.3(3r)S1, RELEASE SOFTWARE
Copyright (c) 1994-2013  by cisco Systems, Inc.

 Current image running: Boot ROM0

Last reset cause: LocalSoft
 Cisco ISR4451-X/K9 platform with 4194304 Kbytes of main memory


rommon 1  boot bootflash:mydir/packages.conf

 File size is 0x000028f1
 Located mydir/packages.conf
 Image size
10481 inode num 632741, bks cnt 3 blk size 8*512

#
 File size is 0x150ae3cc
 Located mydir/isr4400-mono-universalk9.03.14.00.S.155-1.S-std.SPA.pkg
 Image size 353035212 inode num 356929, bks cnt 86191 blk size 8*512
 ###################################################################
######################################################################
 Boot image size = 353035212 (0x150ae3cc) bytes

 Package header rev 1 structure detected
 Calculating SHA-1 hash...done
 validate_package: SHA-1 hash:
  calculated 8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3
  expected   8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3

 RSA Signed RELEASE Image Signature Verification Successful.
 Package Load Test Latency : 3799 msec
 Image validated
 Dec 12 09:28:50.338 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 61864 kB] - Please clean up files on bootflash.

              Restricted Rights Legend
```

```
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(1)S,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Nov-14 18:28 by mcpre



Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco ISR4451-X/K9 (2RU) processor with 1681388K/6147K bytes of memory.
Processor board ID FTX1736AJUT
2 Ethernet interfaces
4 Gigabit Ethernet interfaces
2 ATM interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of flash memory at bootflash:.

Press RETURN to get started!

*Dec 12 09:28:58.922:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = appxk9 and License = appxk9
*Dec 12 09:28:58.943:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = ipbasek9 and License = ipbasek9
*Dec 12 09:28:58.981:
 %ISR_THROUGHPUT-6-LEVEL: Throughput level has been set to 1000000 kbps
*Dec 12 09:29:13.302: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
```

```
*Dec 12 09:28:51.438: %CMRP-3-PFU_MISSING:cmand:  The platform does not detect a power
supply in slot 1
*Dec 12 09:29:01.256: %CMLIB-6-THROUGHPUT_VALUE:cmand:  Throughput license found, throughput
 set to 1000000 kbps
*Dec 12 09:29:03.223: %CPPHA-7-START:cpp_ha:  CPP 0 preparing ucode
*Dec 12 09:29:03.238: %CPPHA-7-START:cpp_ha:  CPP 0 startup init
*Dec 12 09:29:11.335: %CPPHA-7-START:cpp_ha:  CPP 0 running init
*Dec 12 09:29:11.645: %CPPHA-7-READY:cpp_ha:  CPP 0 loading and initialization complete
*Dec 12 09:29:11.711: %IOSXE-6-PLATFORM:cpp_cp:
Process CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
*Dec 12 09:29:16.280:
%IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO:
Management vrf Mgmt-intf created with ID 1, ipv4 table-id 0x1, ipv6 table-id 0x1E000001
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state to up
*Dec 12 09:29:17.521: %SYS-5-LOG_CONFIG_CHANGE: Buffer logging disabled
*Dec 12 09:29:18.867: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Dec 12 09:29:18.871:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/2, interfaces disabled
*Dec 12 09:29:18.873:
%SPA_OIR-6-OFFLINECARD: SPA (ISR4451-X-4x1GE) offline in subslot 0/0
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VA-B) offline in subslot 0/1
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:29:18.876: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0
*Dec 12 09:29:18.876: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
*Dec 12 09:29:18.882: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/2
*Dec 12 09:29:18.935: %SYS-5-RESTART: System restarted --
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(1)S,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Nov-14 18:28 by mcpre
*Dec 12 09:29:18.895: %SPA-3-ENVMON_NOT_MONITORED:iomd:  Environmental monitoring
is not enabled for ISR4451-X-4x1GE[0/0]
*Dec 12 09:29:19.878: %LINK-5-CHANGED: Interface GigabitEthernet0,

changed state to administratively down
*Dec 12 09:29:22.419: %SPA_OIR-6-ONLINECARD: SPA (ISR4451-X-4x1GE) online in subslot 0/0
*Dec 12 09:29:22.610: %SYS-6-BOOTTIME: Time taken to reboot after reload =  194 seconds
*Dec 12 09:29:24.354: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to down
*Dec 12 09:29:24.415: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
changed state to down
*Dec 12 09:29:24.417: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
changed state to down
*Dec 12 09:29:30.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to up
*Dec 12 09:29:30.925: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
 changed state to up
*Dec 12 09:29:30.936: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
 changed state to up
*Dec 12 09:29:31.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
*Dec 12 09:29:31.930: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0/2, changed state to up
*Dec 12 09:29:31.936: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0/3, changed state to up
*Dec 12 09:29:34.147: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 12 09:30:29.152: %SPA_OIR-6-ONLINECARD: SPA (NIM-VA-B) online in subslot 0/1
*Dec 12 09:30:29.470: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface Ethernet0/1/0, changed state to down
```

```
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
*Dec 12 09:31:03.074: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to up
*Dec 12 09:31:05.075: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to up
*Dec 12 09:31:06.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2/0,
changed state to up
*Dec 12 09:31:12.559: %CONTROLLER-5-UPDOWN: Controller VDSL 0/1/0, changed state to up
*Dec 12 09:31:20.188: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to up
*Dec 12 09:31:21.188: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/1/0,
changed state to up
Router>
Router>en
Password:
Router#
Router#show controller vdsl 0/2/0
Controller VDSL 0/2/0 is UP

Daemon Status:  UP

   XTU-R (DS)  XTU-C (US)
Chip Vendor ID:  'BDCM'    'BDCM'
Chip Vendor Specific:   0x0000    0xA41B
Chip Vendor Country:    0xB500    0xB500
Modem Vendor ID: 'CSCO'    '    '
Modem Vendor Specific:  0x4602    0x0000
Modem Vendor Country:   0xB500    0x0000
Serial Number Near:     FOC18426DQ8 4451-X/K15.5(1)S
Serial Number Far:
Modem Version Near:     15.5(1)S
Modem Version Far:      0xa41b

Modem Status(L1): TC Sync (Showtime!)
DSL Config Mode: VDSL2
Trained Mode(L1): G.993.2 (VDSL2) Profile 30a

TC Mode:  PTM
Selftest Result: 0x00
DELT configuration: disabled
DELT state:  not running

Failed full inits: 0
Short inits:  0
Failed short inits: 0

Modem FW  Version: 4.14L.04
Modem PHY Version: A2pv6F039h.d24o_rc1

Line 1:

   XTU-R (DS)  XTU-C (US)
Trellis:   ON    ON
SRA:     disabled   disabled
SRA count:    0    0
Bit swap:    enabled   enabled
Bit swap count:   9    0
Profile 30a:    enabled
Line Attenuation:   3.5 dB    0.0 dB
Signal Attenuation:   0.0 dB    0.0 dB
Noise Margin:   30.9 dB  12.4 dB
Attainable Rate: 200000 kbits/s   121186 kbits/s
Actual Power:  13.3 dBm   7.2 dBm
Per Band Status:        D1  D2  D3  U0  U1  U2  U3
Line Attenuation(dB):   0.9 1.5 5.5 N/A 0.1 0.9 3.8
Signal Attenuation(dB): 0.8 1.5 5.5 N/A 0.0 0.2 3.2
Noise Margin(dB):       31.1 31.0 30.9 N/A 12.3 12.4 12.5
Total FECC:  0    0
Total ES:  0    0
Total SES:  0    0
Total LOSS:  0    0
Total UAS:  51    51
Total LPRS:  0    0
Total LOFS:  0    0
Total LOLS:  0    0


     DS Channel1   DS Channel0 US Channel1   US Channel0
Speed (kbps):    NA       100014  NA       100014
SRA Previous Speed:   NA            0  NA            0
Previous Speed:    NA            0  NA            0
Reed-Solomon EC:   NA            0  NA            0
CRC Errors:    NA            0  NA            0
Header Errors:    NA            0  NA            0
Interleave (ms):   NA         9.00  NA         0.00
Actual INP:    NA         4.00  NA         0.00

Training Log : Stopped
Training Log Filename : flash:vdsllog.bin

Router#
Router#

Router#copy bootflash:isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
 bootflash:mydir/
Destination filename [mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
6640604 bytes copied in 1.365 secs (4864911 bytes/sec)
Router#

Router#request platform software package install rp 0 file
bootflash:mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation

--- Starting impact testing ---
Checking operational impact of change
Finished impact testing

--- Starting list of software package changes ---
Old files list:
  Removed isr4400-firmware_nim_xdsl.03.14.00.S.155-1.S-std.SPA.pkg
New files list:
  Added isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Finished list of software package changes
```

```
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
Skipping soft links for firmware upgrade
Skipping soft links for firmware upgrade
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19
/release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
  Replacing running software
  Replacing CLI software
  Restarting software
  Applying final IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.
Router#
Router#show platform software subslot 0/2 module firmware
Avg Load info
-------------------------------------------
1.83 1.78 1.44 3/45 607

Kernel distribution info
-------------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2
(Buildroot 2011.11) ) #3 SMP PREEMPT Fri Nov 7 09:26:19 IST 2014

Module firmware versions
-------------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039h.d24o_rc1

Boot Loader: Secondry
-------------------------------------------
Version: 1.1

Modem Up time
-------------------------------------------
0D 0H 25M 38S

Router#

Router#hw-module subslot 0/2 reload
```

```
Proceed with reload of module? [confirm]
Router#
*Dec 12 09:55:59.645: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
reloaded on subslot 0/2
*Dec 12 09:55:59.646: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:55:59.647: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to down
*Dec 12 09:57:22.514: new extended attributes received from iomd(slot 0 bay 2 board 0)
*Dec 12 09:57:22.514: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
 reloaded on subslot 0/2
*Dec 12 09:57:22.515: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
Router#
Router#
*Dec 12 09:58:35.471: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
Router#

Router#show platform software subslot 0/2 module firmware
Avg Load info
-------------------------------------------
0.84 0.23 0.08 1/45 598

Kernel distribution info
-------------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2 (Buildroot 2011.11) )
#6 SMP PREEMPT Mon Nov 17 10:51:41 IST 2014

Module firmware versions
-------------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039n.d24o_rc1

Boot Loader: Secondry
-------------------------------------------
Version: 1.1

Modem Up time
-------------------------------------------
0D 0H 0M 42S

Router#
```

CHAPTER 8

Basic Router Configuration

This section includes information about some basic router configuration, and contains the following sections:

Default Configuration

When you boot up the router for the first time, you will notice that some basic configuration has already been performed. Use the **show running-config** command to view the initial configuration, as shown in the following example:

```
Router# show running-config
Building configuration...
Current configuration : 977 bytes
!
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
```

```
exit-address-family
!
address-family ipv6
exit-address-family
!
!
no aaa new-model
!
ipv6 multicast rpf use-bgp
!
!
multilink bundle-name authenticated
!
!
redundancy
mode none
!

interface GigabitEthernet0/0/0
no ip address
negotiation auto
!
interface GigabitEthernet0/0/1
no ip address
negotiation auto
!
interface GigabitEthernet0/0/2
no ip address
negotiation auto
!
interface GigabitEthernet0/0/3
no ip address
negotiation auto
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
negotiation auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

!
control-plane
!
!
line con 0
stopbits 1
line vty 0 4
login
!
!
end
```

Configuring Global Parameters

To configure the global parameters for your router, follow these steps.

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *name*
3. **enable secret** *password*
4. **no ip domain-lookup**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`Router> `**`enable`**
	`Router# `**`configure terminal`**
	`Router(config)#`
		Enters global configuration mode when using the console port.
		Use the following to connect to the router with a remote terminal:
		`telnet router-name or address`
		`Login: login-id`
		`Password: *********`
		`Router> enable`

Step 2	**hostname** *name* **Example:** `Router(config)# `**`hostname Router`**	Specifies the name for the router.
Step 3	**enable secret** *password* **Example:** `Router(config)# `**`enable secret cr1ny5ho`**	Specifies an encrypted password to prevent unauthorized access to the router.
Step 4	**no ip domain-lookup** **Example:** `Router(config)# `**`no ip domain-lookup`**	Disables the router from translating unfamiliar words (typos) into IP addresses. For complete information on global parameter commands, see the Cisco IOS Release Configuration Guide documentation set.

Configuring Gigabit Ethernet Interfaces

To manually define onboard Gigabit Ethernet interfaces, follow these steps, beginning from global configuration mode.

SUMMARY STEPS

1. **interface gigabitethernet** *slot/bay/port*
2. **ip address** *ip-address mask*
3. **ipv6 address** *ipv6-address/prefix*
4. **no shutdown**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface gigabitethernet** *slot/bay/port* **Example:** `Router(config)# interface gigabitethernet 0/0/1`	Enters the configuration mode for a Gigabit Ethernet interface on the router.
Step 2	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 192.168.12.2 255.255.255.0`	Sets the IP address and subnet mask for the specified Gigabit Ethernet interface. Use this Step if you are configuring an IPv4 address.
Step 3	**ipv6 address** *ipv6-address/prefix* **Example:** `Router(config-if)# ipv6 address 2001.db8::ffff:1/128`	Sets the IPv6 address and prefix for the specified Gigabit Ethernet interface. Use this step instead of Step 2, if you are configuring an IPv6 address.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the Gigabit Ethernet interface and changes its state from administratively down to administratively up.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the Gigabit Ethernet interface and returns to privileged EXEC mode.

Configuring a Loopback Interface

Before You Begin

The loopback interface acts as a placeholder for the static IP address and provides default routing information.

To configure a loopback interface, follow these steps.

SUMMARY STEPS

1. **interface** *type number*
2. (Option 1) **ip address** *ip-address mask*
3. (Option 2) **ipv6 address** *ipv6-address/prefix*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface Loopback 0`	Enters configuration mode on the loopback interface.
Step 2	(Option 1) **ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.108.1.1 255.255.255.0`	Sets the IP address and subnet mask on the loopback interface. (If you are configuring an IPv6 address, use the **ipv6 address** *ipv6-address/prefix* command described below.
Step 3	(Option 2) **ipv6 address** *ipv6-address/prefix* **Example:** `Router(config-if)# 2001:db8::ffff:1/128`	Sets the IPv6 address and prefix on the loopback interface.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the loopback interface and returns to global configuration mode.

Example

The loopback interface in this sample configuration is used to support Network Address Translation (NAT) on the virtual-template interface. This configuration example shows the loopback interface configured on the Gigabit Ethernet interface with an IP address of 192.0.2.0/24, which acts as a static IP address. The loopback interface points back to virtual-template1, which has a negotiated IP address.

```
!
interface loopback 0
ip address 192.0.2.0 255.255.255.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
```

Verifying Loopback Interface Configuration

Enter the **show interface loopback** command. You should see an output similar to the following example:

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Alternatively, use the **ping** command to verify the loopback interface, as shown in the following example:

```
Router# ping 192.0.2.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Configuring Module Interfaces

For detailed information about configuring service modules, see "Service Modules" in the "Service Module Management" section of the Cisco SM-1T3/E3 Service Module Configuration Guide.

Enabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is enabled by default on the router.

Note CDP is not enabled by default on Cisco Aggregation Services Routers or on the Cisco CSR 1000v.

For more information on using CDP, see Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S.

Configuring Command-Line Access

To configure parameters to control access to the router, follow these steps.

SUMMARY STEPS

1. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
2. **password** *password*
3. **login**
4. **exec-timeout** *minutes* [*seconds*]
5. **exit**
6. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
7. **password** *password*
8. **login**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number* **Example:** `Router(config)# line console 0`	Enters line configuration mode, and specifies the type of line. The example provided here specifies a console terminal for access.
Step 2	**password** *password* **Example:** `Router(config-line)# password 5dr4Hepw3`	Specifies a unique password for the console terminal line.
Step 3	**login** **Example:** `Router(config-line)# login`	Enables password checking at terminal session login.

Step 4	**exec-timeout** *minutes* [*seconds*]
	Example:
	`Router(config-line)# exec-timeout 5 30`
	`Router(config-line)#`
		Sets the interval during which the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, adds seconds to the interval value.
		The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of **0 0** specifies never to time out.

Step 5	**exit** **Example:** `Router(config-line)# exit`	Exits line configuration mode to re-enter global configuration mode.

	Command or Action	Purpose

Step 6	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	Example:
	`Router(config)# line vty 0 4`
	`Router(config-line)#`
		Specifies a virtual terminal for remote console access.

Step 7	**password** *password* **Example:** `Router(config-line)# password aldf2ad1`	Specifies a unique password for the virtual terminal line.
Step 8	**login** **Example:** `Router(config-line)# login`	Enables password checking at the virtual terminal session login.

Step 9	**end**
	Example:
	`Router(config-line)# end`
		Exits line configuration mode, and returns to privileged EXEC mode.

Example

The following configuration shows the command-line access commands.

You do not have to input the commands marked **default**. These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
line console 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

Configuring Static Routes

Static routes provide fixed routing paths through the network. They are manually configured on the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes unless they are redistributed by a routing protocol.

To configure static routes, follow these steps.

SUMMARY STEPS

1. (Option 1) **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. (Option 2) **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]}
3. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	(Option 1) **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	Example:
	`Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`
		Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the **ipv6 route** command described below.)

Step 2	(Option 2) **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]}
	Example:
	`Router(config)# ipv6 route 2001:db8:2::/64`
		Specifies a static route for the IP packets.

Step 3	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

Example

In the following configuration example, the static route sends out all IP packets with a destination IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 on the Gigabit Ethernet interface to another device with an IP address of 10.10.10.2. Specifically, the packets are sent to the configured PVC.

You do not have to enter the command marked **default**. This command appears automatically in the configuration file generated when you use the **running-config** command.

```
!
ip classless (default)
ip route 192.168.1.0 255.255.255.0
```

Verifying Configuration

To verify that you have configured static routing correctly, enter the **show ip route** command (or **show ipv6 route** command) and look for static routes marked with the letter S.

When you use an IPv4 address, you should see verification output similar to the following:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, FastEthernet0
```

When you use an IPv6 address, you should see verification output similar to the following:

```
Router# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       ls - LISP site, ld - LISP dyn-EID, a - Application

C   2001:DB8:3::/64 [0/0]
       via GigabitEthernet0/0/2, directly connected
S   2001:DB8:2::/64 [1/0]
       via 2001:DB8:3::1
```

Configuring Dynamic Routes

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routes are shared with other routers in the network.

A router can use IP routing protocols, such as Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (EIGRP), to learn about routes dynamically.

- Configuring Routing Information Protocol, on page 116
- Configuring Enhanced Interior Gateway Routing Protocol, on page 119

Configuring Routing Information Protocol

To configure the RIP on a router, follow these steps.

SUMMARY STEPS

1. **router rip**
2. **version** {**1** | **2**}
3. **network** *ip-address*
4. **no auto-summary**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**router rip** **Example:** Router(config)# **router rip**	Enters router configuration mode, and enables RIP on the router.
Step 2	**version** {**1** | **2**} **Example:** Router(config-router)# **version 2**	Specifies use of RIP version 1 or 2.
Step 3	**network** *ip-address* **Example:** Router(config-router)# **network 192.168.1.1** Router(config-router)# **network 10.10.7.1**	Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.
Step 4	**no auto-summary** **Example:** Router(config-router)# **no auto-summary**	Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries.
Step 5	**end** **Example:** Router(config-router)# **end**	Exits router configuration mode, and enters privileged EXEC mode.

Example

The following configuration example shows RIP Version 2 enabled in IP networks 10.0.0.0 and 192.168.1.0. To see this configuration, use the **show running-config** command from privileged EXEC mode.

```
!
Router# show running-config
Building configuration...

Current configuration : 1616 bytes
!
! Last configuration change at 03:17:14 EST Thu Sep 6 2012
!
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
```

```
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable password cisco
!
no aaa new-model
!
transport-map type console consolehandler
 banner wait ^C
Waiting for IOS vty line
^C
 banner diagnostic ^C
Welcome to diag mode
^C
!
clock timezone EST -4 0
!
!


ip domain name cisco.com
ip name-server vrf Mgmt-intf 203.0.113.1
ip name-server vrf Mgmt-intf 203.0.113.129

!
ipv6 multicast rpf use-bgp
!
!
multilink bundle-name authenticated
!
redundancy
 mode none
!
ip ftp source-interface GigabitEthernet0
ip tftp source-interface GigabitEthernet0
!
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 172.18.77.212 255.255.255.240
 negotiation auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 172.18.77.209
!
control-plane
!
!
line con 0
```

```
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
transport type console 0 input consolehandler
!
ntp server vrf Mgmt-intf 10.81.254.131
!
end
```

Verifying Configuration

To verify that you have configured RIP correctly, enter the **show ip route** command and look for RIP routes marked with the letter R. You should see an output similar to the one shown in the following example:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R    3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0/0
```

Configuring Enhanced Interior Gateway Routing Protocol

To configure Enhanced Interior Gateway Routing Protocol (EIGRP), follow these steps.

SUMMARY STEPS

1. **router eigrp** *as-number*
2. **network** *ip-address*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 109`	Enters router configuration mode, and enables EIGRP on the router. The autonomous-system number identifies the route to other EIGRP routers and is used to tag the EIGRP information.

Step 2	**network** *ip-address*
	Example:
	`Router(config)# network 192.168.1.0`
	`Router(config)# network 10.10.12.115`
		Specifies a list of networks on which EIGRP is to be applied, using the IP address of the network of directly connected networks.

	Command or Action	Purpose

Step 3	**end**
	Example:
	`Router(config-router)# end`
		Exits router configuration mode, and enters privileged EXEC mode.

Example

The following configuration example shows the EIGRP routing protocol enabled in IP networks 192.168.1.0 and 10.10.12.115. The EIGRP autonomous system number is 109. To see this configuration, use the **show running-config** command.

```
Router# show running-config
.
.
.
!
router eigrp 109
 network 192.168.1.0
  network 10.10.12.115
!
.
.
.
```

Verifying the Configuration

To verify that you have configured IP EIGRP correctly, enter the **show ip route** command, and look for EIGRP routes marked by the letter D. You should see verification output similar to the following:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D     3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

CHAPTER 9

Slot and Subslot Configuration

This chapter contains information on slots and subslots. Slots specify the chassis slot number in your router and subslots specify the slot where the service modules are installed.

For further information on the slots and subslots, see the “About Slots and Interfaces” section in the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

The following section is included in this chapter:

Configuring the Interfaces

The following sections describe how to configure Gigabit interfaces and also provide examples of configuring the router interfaces:

Configuring Gigabit Ethernet Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *slot/subslot/port*
4. **ip address** *ip-address mask* [**secondary**] **dhcp pool**
5. **negotiation auto**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>` **`enable`**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router#` **`configure terminal`**	Enters global configuration mode.
Step 3	**interface GigabitEthernet** *slot/subslot/port* **Example:** `Router(config)#` **`interface GigabitEthernet 0/0/1`**	Configures a GigabitEthernet interface. • **GigabitEthernet—**Type of interface. • *slot*—Chassis slot number. • */subslot*—Secondary slot number. The slash (/) is required. • /port—Port or interface number. The slash (/) is required.
Step 4	**ip address** *ip-address mask* [**secondary**] **dhcp pool** **Example:** `Router(config-if)#` **`ip address 10.0.0.1 255.255.255.0 dhcp pool`**	Assigns an IP address to the GigabitEthernet • **ip address** *ip-address*—IP address for the interface. • *mask*—Mask for the associated IP subnet. • **secondary** (optional)—Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. • **dhcp—**IP address negotiated via DHCP. • **pool—**IP address autoconfigured from a local DHCP pool.
Step 5	**negotiation auto** **Example:** `Router(config-if)#` **`negotiation auto`**	Selects the negotiation mode. • **auto—**Performs link autonegotiation.

Step 6	**end**
	Example:
	`Router(config-if)#` **`end`**
		Ends the current configuration session and returns to privileged EXEC mode.

Configuring the Interfaces: Example

The following example shows the **interface gigabitEthernet** command being used to add the interface and set the IP address. **0/0/0** is the slot/subslot/port. The ports are numbered 0 to 3.

```
Router# show running-config interface gigabitEthernet 0/0/0
Building configuration...
Current configuration : 71 bytes
!
interface gigabitEthernet0/0/0
no ip address
negotiation auto
end

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 0/0/0
```

Viewing a List of All Interfaces: Example

In this example, the **show platform software interface summary** and **show interfaces summary** commands are used to display all the interfaces:

```
Router# show platform software interface summary
  Interface                 IHQ  IQD  OHQ  OQD  RXBS  RXPS  TXBS  TXPS  TRTL
-----------------------------------------------------------------------------
* GigabitEthernet0/0/0        0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/1        0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/2        0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/3        0    0    0    0     0     0     0     0     0
* GigabitEthernet0            0    0    0    0     0     0     0     0     0


Router# show interfaces summary
   *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

Interface             IHQ  IQD    OHQ    OQD    RXBS    RXPS    TXBS    TXPS    TRTL
------------------------------------------------------------------------------------------

* GigabitEthernet0/0/0 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/1 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/2 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/3 0    0      0      0      0       0       0       0       0
* GigabitEthernet      0    0      0      0      0       0       0       0       0
```

Viewing Information About an Interface: Example

The following example shows how to display a brief summary of an interface's IP information and status, including the virtual interface bundle information, by using the **show ip interface brief** command:

```
Router# show ip interface brief
Interface              IP-Address      OK?  Method  Status                 Protocol
GigabitEthernet0/0/0    10.0.0.1       YES  manual  down                   down
GigabitEthernet0/0/1    unassigned     YES  NVRAM   administratively down  down
GigabitEthernet0/0/2    10.10.10.1     YES  NVRAM   up                     up
GigabitEthernet0/0/3    8.8.8.1        YES  NVRAM   up                     up
GigabitEthernet0        172.18.42.33   YES  NVRAM   up                     up
```

CHAPTER 10

Process Health Monitoring

This chapter describes how to manage and monitor the health of various components of your router. It contains the following sections:

Monitoring Control Plane Resources

The following sections explain the of memory and CPU monitoring from the perspective of the Cisco IOS process and the overall control plane:

Avoiding Problems Through Regular Monitoring

Processes should provide monitoring and notification of their status/health to ensure correct operation. When a process fails, a syslog error message is displayed and either the process is restarted or the router is rebooted. A syslog error message is displayed when a monitor detects that a process is stuck or has crashed. If the process can be restarted, it is restarted; else, the router is restarted.

Monitoring system resources enables you to detect potential problems before they occur, thus avoiding outages. The following are the advantages of regular monitoring:

- Lack of memory on line cards that are in operation for a few years can lead to major outages. Monitoring memory usage helps to identify memory issues in the line cards and enables you to prevent an outage.
- Regular monitoring establishes a baseline for a normal system load. You can use this information as a basis for comparison when you upgrade hardware or software—to see if the upgrade has affected resource usage.

Cisco IOS Process Resources

You can view CPU utilization statistics on active processes and see the amount of memory being used in these processes using the **show memory** command and the **show process cpu** command. These commands provide a representation of memory and CPU utilization from the perspective of only the Cisco IOS process; they do not include information for resources on the entire platform. For example, when the **show memory** command is used in a system with 8 GB RAM running a single Cisco IOS process, the following memory usage is displayed:

```
Router# show memory
           Head           Total(b)     Used(b)     Free(b)      Lowest(b)    Largest(b)
Processor  2ABEA4316010   4489061884   314474916   4174586968   3580216380   3512323496
lsmpi_io   2ABFAFF471A8   6295128      6294212     916          916          916
Critical   2ABEB7C72EB0   1024004      92          1023912      1023912      1023912
```

The **show process cpu** command displays Cisco IOS CPU utilization average:

```
Router# show process cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1         583     48054         12  0.00%  0.00%  0.00%   0 Chunk Manager
   2         991    176805          5  0.00%  0.00%  0.00%   0 Load Meter
   3           0         2          0  0.00%  0.00%  0.00%   0 IFCOM Msg Hdlr
   4           0        11          0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0         3          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6      230385    119697       1924  0.00%  0.01%  0.00%   0 Check heaps
   7          49        28       1750  0.00%  0.00%  0.00%   0 Pool Manager
   8           0         2          0  0.00%  0.00%  0.00%   0 Timers
   9       17268    644656         26  0.00%  0.00%  0.00%   0 ARP Input
  10         197    922201          0  0.00%  0.00%  0.00%   0 ARP Background
  11           0         2          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  12           0         1          0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  13           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  14           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
  15           0         2          0  0.00%  0.00%  0.00%   0 DDR Timers
  16           1        15         66  0.00%  0.00%  0.00%   0 Entity MIB API
  17          13      1195         10  0.00%  0.00%  0.00%   0 EEM ED Syslog
  18          93        46       2021  0.00%  0.00%  0.00%   0 PrstVbl
  19           0         1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
```

Overall Control Plane Resources

Control plane memory and CPU utilization on each control processor allows you to keep a tab on the overall control plane resources. You can use the **show platform software status control-processor brief** command (summary view) or the **show platform software status control-processor** command (detailed view) to view control plane memory and CPU utilization information.

All control processors should show status, Healthy. Other possible status values are Warning and Critical. Warning indicates that the router is operational, but that the operating level should be reviewed. Critical implies that the router is nearing failure.

If you see a Warning or Critical status, take the following actions:

- Reduce the static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, reduce the number of VLANs, and so on.

The following sections describe the fields in the **show platform software status control-processor** command output.

Load Average

Load average represents the process queue or process contention for CPU resources. For example, on a single-core processor, an instantaneous load of 7 would mean that seven processes are ready to run, one of which is currently running. On a dual-core processor, a load of 7 would mean that seven processes are ready to run, two of which are currently running.

Memory Utilization

Memory utilization is represented by the following fields:

- Total—Total line card memory
- Used—Consumed memory
- Free—Available memory
- Committed—Virtual memory committed to processes

CPU Utilization

CPU utilization is an indication of the percentage of time the CPU is busy, and is represented by the following fields:

- CPU—Allocated processor
- User—Non-Linux kernel processes
- System—Linux kernel process
- Nice—Low-priority processes
- Idle—Percentage of time the CPU was inactive
- IRQ—Interrupts
- SIRQ—System Interrupts
- IOwait—Percentage of time CPU was waiting for I/O

Example: show platform software status control-processor Command

The following are some examples of using the **show platform software status control-processor** command:

```
Router# show platform software status control-processor
RP0: online, statistics updated 5 seconds ago
Load Average: healthy
  1-Min: 0.07, status: healthy, under 5.00
  5-Min: 0.11, status: healthy, under 5.00
  15-Min: 0.09, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3971216
  Used: 3415976 (86%)
  Free: 555240 (14%)
  Committed: 2594412 (65%), status: healthy, under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.40, System:  1.20, Nice:  0.00, Idle: 97.39
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
```

```
CPU1: CPU Utilization (percentage of time spent)
  User:  0.89, System:  0.79, Nice:  0.00, Idle: 98.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  0.80, System:  2.50, Nice:  0.00, Idle: 96.70
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  3.09, System:  6.19, Nice:  0.00, Idle: 90.60
  IRQ:  0.00, SIRQ:  0.09, IOwait:  0.00
CPU4: CPU Utilization (percentage of time spent)
  User:  0.10, System:  0.30, Nice:  0.00, Idle: 99.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU5: CPU Utilization (percentage of time spent)
  User:  0.89, System:  1.59, Nice:  0.00, Idle: 97.50
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU6: CPU Utilization (percentage of time spent)
  User:  0.80, System:  1.10, Nice:  0.00, Idle: 98.10
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU7: CPU Utilization (percentage of time spent)
  User:  0.20, System:  3.40, Nice:  0.00, Idle: 96.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

Router# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.09   0.10   0.09

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3971216  3426452 (86%)   544764 (14%)   2595212 (65%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   1.60   0.90   0.00  97.30   0.10   0.10   0.00
         1   0.09   1.29   0.00  98.60   0.00   0.00   0.00
         2   0.10   0.10   0.00  99.79   0.00   0.00   0.00
         3   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         4   0.60   4.90   0.00  94.50   0.00   0.00   0.00
         5   0.70   1.30   0.00  98.00   0.00   0.00   0.00
         6   0.10   0.00   0.00  99.90   0.00   0.00   0.00
         7   1.39   0.49   0.00  98.10   0.00   0.00   0.00
```

Monitoring Hardware Using Alarms

Router Design and Monitoring Hardware

The router sends alarm notifications when problems are detected, allowing you to monitor the network remotely. You do not need to use **show** commands to poll devices on a routine basis; however, you can perform onsite monitoring if you choose.

BootFlash Disk Monitoring

The bootflash disk must have enough free space to store two core dumps. This condition is monitored, and if the bootflash disk is too small to store two core dumps, a syslog alarm is generated, as shown in the following example:

```
Aug 22 13:40:41.038 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 7084440 kB] - Please clean up files on bootflash.
```

The size of the bootflash disk must be at least of the same size as that of the physical memory installed on the router. If this condition is not met, a syslog alarm is generated as shown in the following example:

```
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Flash capacity (8 GB) is insufficient for fault
analysis based on
installed memory of RP (16 GB)
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Please increase the size of installed flash to at
least 16 GB (same as
physical memory size)
```

Approaches for Monitoring Hardware Alarms

- Onsite Network Administrator Responds to Audible or Visual Alarms, on page 129
- Viewing the Console or Syslog for Alarm Messages, on page 130
- Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP, on page 132

Onsite Network Administrator Responds to Audible or Visual Alarms

- About Audible and Visual Alarms, on page 129
- Clearing an Audible Alarm, on page 129
- Clearing a Visual Alarm, on page 130

About Audible and Visual Alarms

An external element can be connected to a power supply using the DB-25 alarm connector on the power supply. The external element is a DC light bulb for a visual alarm and a bell for an audible alarm.

If an alarm illuminates the CRIT, MIN, or MAJ LED on the faceplate of the router, and a visual or audible alarm is wired, the alarm also activates an alarm relay in the power supply DB-25 connector, and either the bell rings or the light bulb flashes.

Clearing an Audible Alarm

To clear an audible alarm, perform one of the following tasks:

- Press the **Audible Cut Off** button on the faceplate.
- Enter the **clear facility-alarm** command.

Clearing a Visual Alarm

To clear a visual alarm, you must resolve the alarm condition. The **clear facility-alarm** command does not clear an alarm LED on the faceplate or turn off the DC light bulb. For example, if a critical alarm LED is illuminated because an active module was removed without a graceful deactivation, the only way to resolve that alarm is to replace the module.

Viewing the Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a system message log (syslog).

- Enabling the logging alarm Command, on page 130
- Examples of Alarm Messages, on page 130
- Reviewing and Analyzing Alarm Messages, on page 132

Enabling the logging alarm Command

The **logging alarm** command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of the alarms to be logged. All the alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

Examples of Alarm Messages

The following are examples of alarm messages that are sent to the console when a module is removed before performing a graceful deactivation. The alarm is cleared when the module is reinserted.

Module Removed

```
*Aug 22 13:27:33.774: %ISR4451-X_OIR-6-REMSPA: Module removed from subslot 1/1, interfaces
 disabled
*Aug 22 13:27:33.775: %SPA_OIR-6-OFFLINECARD: Module (SPA-4XT-SERIAL) offline in subslot
1/1
```

Module Reinserted

```
*Aug 22 13:32:29.447: %ISR4451-X_OIR-6-INSSPA: Module inserted in subslot 1/1
*Aug 22 13:32:34.916: %SPA_OIR-6-ONLINECARD: Module (SPA-4XT-SERIAL) online in subslot 1/1
*Aug 22 13:32:35.523: %LINK-3-UPDOWN: SIP1/1: Interface EOBC1/1, changed state to up
```

Alarms

To view alarms, use the **show facility-alarm status** command. The following example shows a critical alarm for the power supply:

```
Router# show facility-alarm status
System Totals  Critical: 5  Major: 0  Minor: 0
```

```
Source                     Severity      Description [Index]
------                     --------      -------------------
Power Supply Bay 0         CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0       CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/1       CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/2       CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3       CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/0       INFO          Transceiver Missing [0]
xcvr container 0/0/1       INFO          Transceiver Missing [0]
xcvr container 0/0/2       INFO          Transceiver Missing [0]
xcvr container 0/0/3       INFO          Transceiver Missing [0]
```

To view critical alarms, use the **show facility-alarm status critical** command, as shown in the following example:

```
Router# show facility-alarm status critical
System Totals  Critical: 5  Major: 0  Minor: 0

Source                     Severity      Description [Index]
------                     --------      -------------------
Power Supply Bay 0         CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0       CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/1       CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/2       CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3       CRITICAL      Physical Port Link Down [1]
```

To view the operational state of the major hardware components on the router, use the **show platform diag** command. This example shows that power supply P0 has failed:

```
Router# show platform diag
Chassis type: ISR4451/K9

Slot: 0, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:42 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Sub-slot: 0/0, ISR4451-4X1GE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:02:48 (1w0d ago)
  Logical insert detect time  : 00:02:48 (1w0d ago)

Slot: 1, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:43 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: 2, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:44 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: R0, ISR4451/K9
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:09 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: F0, ISR4451-FP
  Running state               : init, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:37 (1w0d ago)
  Hardware ready signal time  : 00:00:00 (never ago)
  Packet ready signal time    : 00:00:00 (never ago)
  CPLD version                :
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: P0, Unknown
  State                       : ps, fail
  Physical insert detect time : 00:00:00 (never ago)

Slot: P1, XXX-XXXX-XX
  State                       : ok
  Physical insert detect time : 00:01:26 (1w0d ago)

Slot: P2, ACS-4450-FANASSY
  State                       : ok
  Physical insert detect time : 00:01:26 (1w0d ago)
```

Reviewing and Analyzing Alarm Messages

To facilitate the review of alarm messages, you can write scripts to analyze alarm messages sent to the console or syslog. Scripts can provide reports on events such as alarms, security alerts, and interface status.

Syslog messages can also be accessed through Simple Network Management Protocol (SNMP) using the history table defined in the CISCO-SYSLOG-MIB.

Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP

The SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network. Of all the approaches to monitor alarms, SNMP is the best approach to monitor more than one router in an enterprise and service provider setup.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access router information through a network management system (NMS) instead of reviewing logs, polling devices, or reviewing log reports.

To use SNMP to get alarm notification, use the following MIBs:

- ENTITY-MIB, RFC 4133 (required for the CISCO-ENTITY-ALARM-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-SENSOR-MIB (for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)

CHAPTER 11

System Messages

System messages are saved in a log file or directed to other devices from the software running on a router. These messages are also known as syslog messages. System messages provide you with logging information for monitoring and troubleshooting purposes.

The following sections are included in this chapter:

Information About Process Management

You can access system messages by logging in to the console through Telnet protocol and monitoring your system components remotely from any workstation that supports the Telnet protocol.

Starting and monitoring software is referred to as process management. The process management infrastructure for a router is platform independent, and error messages are consistent across platforms running on Cisco IOS XE. You do not have to be directly involved in process management, but we recommend that you read the system messages that refer to process failures and other issues.

How to Find Error Message Details

To show further details about a process management or a syslog error message, enter the error message into the Error Message Decoder tool at: https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi.

For example, enter the message `%PMAN-0-PROCESS_NOTIFICATION` into the tool to view an explanation of the error message and the recommended action to be taken.

The following are examples of the description and the recommended action displayed by the Error Message Decoder tool for some of the error messages.

Error Message: `%PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]`

Explanation	Recommended Action

The process lifecycle notification component failed, preventing proper detection of a process start and stop. This problem is likely the result of a software defect in the software subpackage.	Note the time of the message and investigate the kernel error message logs to learn more about the problem and see if it is correctable. If the problem cannot be corrected or the logs are not helpful, copy the error message exactly as it appears on the console along with the output of the **show tech-support** command and provide the gathered information to a Cisco technical support representative.

Error Message: `%PMAN-0-PROCFAILCRIT A critical process [chars] has failed (rc [dec])`

Explanation	Recommended Action
A process important to the functioning of the router has failed.	Note the time of the message and investigate the error message logs to learn more about the problem. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAILOPT An optional process [chars] has failed (rc [dec])`

Explanation	Recommended Action

A process that does not affect the forwarding of traffic has failed.	Note the time of the message and investigate the kernel error message logs to learn more about the problem. Although traffic will still be forwarded after receiving this message, certain functions on the router may be disabled because of this message and the error should be investigated. If the logs are not helpful or indicate a problem you cannot correct, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAIL The process [chars] has failed (rc [dec])`

Explanation	**Recommended Action**

The process has failed as the result of an error.	This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAIL_IGNORE [chars] process exits and failures are being ignored due to debug settings. Normal router functionality will be affected. Critical router functions like RP switchover, router reload, FRU resets, etc. may not function properly.`

Explanation	Recommended Action
A process failure is being ignored due to the user-configured debug settings.	If this behavior is desired and the debug settings are set according to a user's preference, no action is needed. If the appearance of this message is viewed as a problem, change the debug settings. The router is not expected to behave normally with this debug setting. Functionalities such as SSO switchover, router reloads, FRU resets, and so on will be affected. This setting should only be used in a debug scenario. It is not normal to run the router with this setting.

Error Message: `%PMAN-3-PROCHOLDDOWN The process [chars] has been helddown (rc [dec])`

Explanation	Recommended Action

The process was restarted too many times with repeated failures and has been placed in the hold-down state.	This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-RELOAD_RP_SB_NOT_READY : Reloading: [chars]`

Explanation	**Recommended Action**
The route processor is being reloaded because there is no ready standby instance.	Ensure that the reload is not due to an error condition.

Error Message: `%PMAN-3-RELOAD_RP : Reloading: [chars]`

Explanation	**Recommended Action**
The RP is being reloaded.	Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-3-RELOAD_SYSTEM : Reloading: [chars]`

Explanation	**Recommended Action**
The system is being reloaded.	Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-3-PROC_BAD_EXECUTABLE : Bad executable or permission problem with process [chars]`

Explanation	Recommended Action
The executable file used for the process is bad or has permission problem.	Ensure that the named executable is replaced with the correct executable.

Error Message: `%PMAN-3-PROC_BAD_COMMAND:Non-existent executable or bad library used for process <process name>`

Explanation	Recommended Action
The executable file used for the process is missing, or a dependent library is bad.	Ensure that the named executable is present and the dependent libraries are good.

Error Message: `%PMAN-3-PROC_EMPTY_EXEC_FILE : Empty executable used for process [chars]`

Explanation	Recommended Action
The executable file used for the process is empty.	Ensure that the named executable is non-zero in size.

Error Message: `%PMAN-5-EXITACTION : Process manager is exiting: [chars]`

Explanation	Recommended Action
The process manager is exiting.	Ensure that the process manager is not exiting due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-6-PROCSHUT : The process [chars] has shutdown`

Explanation	Recommended Action
The process has gracefully shut down.	No user action is necessary. This message is provided for informational purposes only.

Error Message: `%PMAN-6-PROCSTART : The process [chars] has started`

Explanation	Recommended Action
The process has launched and is operating properly.	No user action is necessary. This message is provided for informational purposes only.

Error Message: `%PMAN-6-PROCSTATELESS : The process [chars] is restarting stateless`

Explanation	Recommended Action
The process has requested a stateless restart.	No user action is necessary. This message is provided for informational purposes only.

CHAPTER 12

Trace Management

The following sections are included in this chapter:

Tracing Overview

Tracing is a function that logs internal events. Trace files containing trace messages are automatically created and saved to the tracelogs directory on the hard disk: file system on the router, which stores tracing files in bootflash.

The contents of trace files are useful for the following purposes:

- Troubleshooting—Helps to locate and solve an issue with a router. The trace files can be accessed in diagnostic mode even if other system issues are occurring simultaneously.
- Debugging—Helps to obtain a detailed view of system actions and operations.

How Tracing Works

Tracing logs the contents of internal events on a router. Trace files containing all the trace output pertaining to a module are periodically created and updated and stored in the tracelog directory. Trace files can be erased from this directory to recover space on the file system without impacting system performance. The files can be copied to other destinations using file transfer functions (such as FTP and TFTP) and opened using a plain text editor.

Note Tracing cannot be disabled on a router.

Use the following commands to view trace information and set tracing levels:

- **show platform software trace message**—Shows the most recent trace information for a specific module. This command can be used in privileged EXEC and diagnostic modes. When used in diagnostic mode, this command can gather trace log information during a Cisco IOS XE failure.
- **set platform software trace**—Sets a tracing level that determines the types of messages that are stored in the output. For more information on tracing levels, see Tracing Levels, on page 142.

Tracing Levels

Tracing levels determine how much information should be stored about a module in the trace buffer or file.

The following table shows all the tracing levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

Table 10: Tracing Levels and Descriptions

Tracing Level	Level Number	Description
Emergency	0	The message is regarding an issue that makes the system unusable.
Alert	1	The message is regarding an action that must be taken immediately.
Critical	2	The message is regarding a critical condition. This is the default setting for every module on the router.
Error	3	The message is regarding a system error.
Warning	4	The message is regarding a system warning.
Notice	5	The message is regarding a significant issue, but the router is still working normally.
Informational	6	The message is useful for informational purposes only.
Debug	7	The message provides debug-level output.

Tracing Level	Level Number	Description
Verbose	8	All possible tracing messages are sent.
Noise	—	All possible trace messages pertaining to a module are logged. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level than verbose level, the noise level will become equal to the level of the newly introduced tracing level.

If a tracing level is set, messages are collected from both lower tracing levels and from its own level.

For example, setting the tracing level to 3 (error) means that the trace file will contain output messages for levels: 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error).

If you set the trace level to 4 (warning), it results in output messages for levels: 0 (emergencies), 1 (alerts), 2 (critical), 3 (error), and 4 (warning).

The default tracing level for every module on the router is 5 (notice).

A tracing level is not set in a configuration mode, which results in tracing-level settings being returned to default values after the router reloads.

Caution Setting the tracing level of a module to debug level or higher can have a negative impact on the performance.

Caution Setting high tracing levels on a large number of modules can severely degrade performance. If a high tracing level is required in a specific context, it is almost always preferable to set the tracing level of a single module to a higher level rather than setting multiple modules to high levels.

Viewing a Tracing Level

By default, all the modules on a router are set to 5 (notice). This setting is maintained unless changed by a user.

To see the tracing level for a module on a router, enter the **show platform software trace level** command in privileged EXEC mode or diagnostic mode.

The following example shows how the **show platform software trace level** command is used to view the tracing levels of the forwarding manager processes on an active RP:

```
Router# show platform software trace level forwarding-manager rp active
Module Name                     Trace Level
-----------------------------------------------
acl                             Notice
```

```
binos                           Notice
binos/brand                     Notice
bipc                            Notice
bsignal                         Notice
btrace                          Notice
cce                             Notice
cdllib                          Notice
cef                             Notice
chasfs                          Notice
chasutil                        Notice
erspan                          Notice
ess                             Notice
ether-channel                   Notice
evlib                           Notice
evutil                          Notice
file_alloc                      Notice
fman_rp                         Notice
fpm                             Notice
fw                              Notice
icmp                            Notice
interfaces                      Notice
iosd                            Notice
ipc                             Notice
ipclog                          Notice
iphc                            Notice
IPsec                           Notice
mgmte-acl                       Notice
mlp                             Notice
mqipc                           Notice
nat                             Notice
nbar                            Notice
netflow                         Notice
om                              Notice
peer                            Notice
qos                             Notice
route-map                       Notice
sbc                             Notice
services                        Notice
sw_wdog                         Notice
tdl_acl_config_type             Notice
tdl_acl_db_type                 Notice
tdl_cdlcore_message             Notice
tdl_cef_config_common_type      Notice
tdl_cef_config_type             Notice
tdl_dpidb_config_type           Notice
tdl_fman_rp_comm_type           Notice
tdl_fman_rp_message             Notice
tdl_fw_config_type              Notice
tdl_hapi_tdl_type               Notice
tdl_icmp_type                   Notice
tdl_ip_options_type             Notice
tdl_ipc_ack_type                Notice
tdl_IPsec_db_type               Notice
tdl_mcp_comm_type               Notice
tdl_mlp_config_type             Notice
tdl_mlp_db_type                 Notice
tdl_om_type                     Notice
tdl_ui_message                  Notice
tdl_ui_type                     Notice
tdl_urpf_config_type            Notice
tdllib                          Notice
trans_avl                       Notice
uihandler                       Notice
uipeer                          Notice
uistatus                        Notice
urpf                            Notice
vista                           Notice
wccp                            Notice
```

Setting a Tracing Level

To set a tracing level for a module on a router, or for all the modules within a process on a router, enter the **set platform software trace** command in the privileged EXEC mode or diagnostic mode.

The following example shows the tracing level for the ACL module in the Forwarding Manager of the ESP processor in slot 0 set to `info`:

```
set platform software trace forwarding-manager F0 acl info
```

Viewing the Content of the Trace Buffer

To view the trace messages in the trace buffer or file, enter the **show platform software trace message** command in privileged EXEC or diagnostic mode. In the following example, the trace messages for the Host Manager process in Route Processor slot 0 are viewed using the **show platform software trace message command**:

```
Router# show platform software trace message host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
```

CHAPTER 13

Environmental Monitoring and PoE Management

The Cisco 4000 series Integrated Services routers have hardware and software features that periodically monitor the router's environment. For more information, see the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

This chapter provides information on the environmental monitoring features on your router that allow you to monitor critical events and generate statistical reports on the status of various router components and, includes the following sections:

Environmental Monitoring

The router provides a robust environment-monitoring system with several sensors that monitor the system temperatures. Microprocessors generate interrupts to the HOST CPU for critical events and generate a periodic status and statistics report. The following are some of the key functions of the environmental monitoring system:

- Monitoring temperature of CPUs, motherboard, and midplane
- Monitoring fan speed
- Recording abnormal events and generating notifications
- Monitoring Simple Network Management Protocol (SNMP) traps
- Generating and collecting Onboard Failure Logging (OBFL) data
- Sending call home event notifications
- Logging system error messages
- Displaying present settings and status

Environmental Monitoring and Reporting Functions

Monitoring and reporting functions allow you to maintain normal system operation by identifying and resolving adverse conditions prior to loss of operation.

Environmental Monitoring Functions

Environmental monitoring functions use sensors to monitor the temperature of the cooling air as it moves through the chassis.

The local power supplies provide the ability to monitor:

- Input and output current
- Output voltage
- Input and output power
- Temperature
- Fan speed

The router is expected to meet the following environmental operating conditions:

- Operating Temperature Nominal—32°F to 104°F (0°C to 40°C)
- Operating Humidity Nominal—10% to 85% RH noncondensing
- Operating Humidity Short Term—10% to 85% RH noncondensing
- Operating Altitude—Sea level 0 ft to 10,000 ft (0 to 3000 m)
- AC Input Range—85 to 264 VAC

In addition, each power supply monitors its internal temperature and voltage. A power supply is either within tolerance (normal) or out of tolerance (critical). If an internal power supply's temperature or voltage reaches a critical level, the power supply shuts down without any interaction with the system processor.

The following table displays the levels of status conditions used by the environmental monitoring system.

Table 11: Levels of Status Conditions Used by the Environmental Monitoring System

Status Level	Description
Normal	All monitored parameters are within normal tolerance.
Warning	The system has exceeded a specified threshold. The system continues to operate, but operator action is recommended to bring the system back to a normal state.

Status Level	Description
Critical	An out-of-tolerance temperature or voltage condition exists. Although the system continues to operate, it is approaching shutdown. Immediate operator action is required.

The environmental monitoring system sends system messages to the console, for example, when the conditions described here are met:

Fan Failure

When the system power is on, all the fans should be operational. Although the system continues to operate if a fan fails, the system displays the following message:

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

Sensors Out of Range

When sensors are out of range, the system displays the following message:

```
%ENVIRONMENTAL-1-ALERT: V: 1.0v PCH, Location: R0, State: Warning, Reading: 1102 mV

%ENVIRONMENTAL-1-ALERT: V: PEM Out, Location: P1, State: Warning, Reading: 0 mV

%ENVIRONMENTAL-1-ALERT: Temp: Temp 3, Location R0, State : Warning, Reading : 90C
```

Fan Tray (Slot P2) Removed

When the fan tray for slot P2 is removed, the system displays the following message:

```
%IOSXE_PEM-6-REMPEM_FM: PEM/FM slot P2 removed
```

Fan Tray (Slot P2) Reinserted

When the fan tray for slot P2 is reinserted, the system displays the following message:

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P2 inserted
```

Fan Tray (Slot 2) is Working Properly

When the fan tray for slot 2 is functioning properly, the system displays the following message:

```
%IOSXE_PEM-6-PEMOK: The PEM in slot P2 is functioning properly
```

Fan 0 in Slot 2 (Fan Tray) is Not Working

When Fan 0 in the fan tray of slot 2 is not functioning properly, the system displays the following message:

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

Fan 0 in Slot 2 (Fan Tray) is Working Properly

When Fan 0 in the fan tray of slot 2 is functioning properly, the system displays the following message:

```
%IOSXE_PEM-6-FANOK: The fan in slot 2/0 is functioning properly
```

Main Power Supply in Slot 1 is Powered Off

When the main power supply in slot 1 is powered off, the system displays the following message:

```
%IOSXE_PEM-3-PEMFAIL: The PEM in slot 1 is switched off or encountering a
failure condition.
```

Main Power Supply is Inserted in Slot 1

When the main power supply is inserted in slot 1, the system displays the following messages:

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P1 inserted
%IOSXE_PEM-6-PEMOK: The PEM in slot 1 is functioning properly
```

Temperature and Voltage Exceed Max/Min Thresholds

The following example shows the warning messages indicating the maximum and minimum thresholds of the temperature or voltage:

```
Warnings :
--------
For all the temperature sensors (name starting with “Temp:”) above,
the critical warning threshold is 100C (100C and higher)
the warning threshold is 80C (range from 80C to 99C)
the low warning threshold is 1C (range from -inf to 1C).

For all voltage sensors (names starting with "V:"),
the high warning threshold starts at that voltage +10%. (voltage + 10% is warning)
the low warning threshold starts at the voltage -10%. (voltage - 10% is warning)
```

Environmental Reporting Functions

You can retrieve and display environmental status reports using the following commands:

- **debug environment**
- **debug platform software cman env monitor polling**
- **debug ilpower**
- **debug power** [**inline** | **main**]
- **show diag all eeprom**
- **show diag slot R0 eeprom detail**
- **show environment**
- **show environment all**
- **show inventory**
- **show platform all**
- **show platform diag**
- **show platform software status control-processor**
- **show version**
- **show power**
- **show power inline**

These commands show the current values of parameters such as temperature and voltage.

The environmental monitoring system updates the values of these parameters every 60 seconds. Brief examples of these commands are shown below:

debug environment: Example

```
Router# debug environment location P0
Environmental sensor Temp: Temp 1 P0 debugging is on
Environmental sensor Temp: Temp 2 P0 debugging is on
Environmental sensor Temp: Temp 3 P0 debugging is on
Environmental sensor V: PEM Out P0 debugging is on
Environmental sensor I: PEM In P0 debugging is on
Environmental sensor I: PEM Out P0 debugging is on
Environmental sensor W: In pwr P0 debugging is on
Environmental sensor W: Out pwr P0 debugging is on
Environmental sensor RPM: fan0 P0 debugging is on

*Sep 12 00:45:13.956: Sensor: Temp: Temp 1 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=29
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: Temp: Temp 1 P0 State=Normal Reading=29
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: Temp: Temp 2 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=33
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: Temp: Temp 2 P0 State=Normal Reading=34
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: Temp: Temp 3 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=34
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: Temp: Temp 3 P0 State=Normal Reading=35
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: V: PEM Out P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=12709
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: V: PEM Out P0 State=Normal Reading=12724
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: I: PEM In P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=1
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: I: PEM In P0 State=Normal Reading=1
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: I: PEM Out P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=4
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: I: PEM Out P0 State=Normal Reading=4
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: W: In pwr P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=92
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: W: In pwr P0 State=Normal Reading=92
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: W: Out pwr P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=46
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: W: Out pwr P0 State=Normal Reading=46
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: RPM: fan0 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=3192
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: RPM: fan0 P0 State=Normal Reading=3180
```

```
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
```

debug platform software cman env monitor polling: Example

```
Router# debug platform software cman env monitor polling
platform software cman env monitor polling debugging is on
Router#
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 1, P0, 29
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 2, P0, 34
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 3, P0, 35
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback V: PEM Out, P0, 12709
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM In, P0, 1
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM Out, P0, 4
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback W: In pwr, P0, 93
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback W: Out pwr, P0, 48
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P0, 3192
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 1, P1, 33
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 2, P1, 32
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 3, P1, 36
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback V: PEM Out, P1, 12666
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM In, P1, 1
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM Out, P1, 4
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: In pwr, P1, 55
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: Out pwr, P1, 46
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P1, 2892
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P2, 4894
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan1, P2, 4790
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan2, P2, 5025
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan3, P2, 5001
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: fan pwr, P2, 8
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 1, R0, 25
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 2, R0, 28
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 1, R0, 30
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 2, R0, 35
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 12v, R0, 12735
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 5v, R0, 5125
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 3.3v, R0, 3352
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.05v, R0, 1052
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 2.5v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.8v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.2v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.15v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.1v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.0v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.8v PCH, R0, 1787
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v PCH, R0, 1516
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v CPUC, R0, 1526
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v CPUI, R0, 1529
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.0v PCH, R0, 1009
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v QLM, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: VCore, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: VTT, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 0.75v CPUI, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 0.75v CPUC, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback I: 12v, R0, 7
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: pwr, R0, 81
```

debug ilpower: Example

```
Router# debug ilpower ?
cdp ILPOWER CDP messages
controller ILPOWER controller
event ILPOWER event
ha ILPOWER High-Availability
port ILPOWER port management
powerman ILPOWER powerman
registries ILPOWER registries
scp ILPOWER SCP messages
```

debug power [inline|main]: Example

In this example, there is one 1000W power supply and one 450W power supply. Inline and main power output is shown.

```
Router# debug power ?
inline ILPM inline power related
main Main power related
<cr>
Router# debug power
POWER all debug debugging is on

Router# show debugging | include POWER
POWER:
POWER main debugging is on
POWER inline debugging is on
Router#
..
*Jan 21 01:29:40.786: %ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P1, State: Warning,
Reading: 0 mV
*Jan 21 01:29:43.968: %IOSXE_PEM-6-PEMOK: The PEM in slot P1 is functioning properly
*Jan 21 01:29:43.968: %PLATFORM_POWER-6-MODEMATCH: Main power is in Boost mode
*Jan 21 01:29:43.968: Power M: Received Msg for 12V/Main, total power 1450, Run same as cfg
 Yes
*Jan 21 01:29:43.968: Power M: Received Msg for POE/ILPM, total power 500, Run same as cfg
 No
*Jan 21 01:29:43.968: Power I: Updating pool power is 500 watts
*Jan 21 01:29:43.968: Power I: Intimating modules of total power 500 watts
*Jan 21 01:29:46.488: Power M: Received Msg for 12V/Main, total power 1450, Run same as cfg
 Yes
*Jan 21 01:29:46.488: Power M: Received Msg for POE/ILPM, total power 500, Run same as cfg
 No
*Jan 21 01:29:46.488: Power I: Updating pool power is 500 watts
*Jan 21 01:29:46.488: Power I: Intimating modules of total power 500 watts
Router#
```

show diag all eeprom: Example

```
Router# show diag all eeprom
MIDPLANE EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
Asset ID : P1B-R2C-CP1.0
CLEI Code : TDBTDBTDBT
Power/Fan Module P0 EEPROM data:

Product Identifier (PID) : XXX-XXXX-XX
Version Identifier (VID) : XXX
PCB Serial Number : DCA1547X047
CLEI Code : 0000000000
Power/Fan Module P1 EEPROM data:

Product Identifier (PID) : XXX-XXXX-XX
Version Identifier (VID) : XXX
PCB Serial Number : DCA1533X022
CLEI Code : 0000000000
Power/Fan Module P2 EEPROM data is not initialized

Internal PoE is not present
Slot R0 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
CLEI Code : TDBTDBTDBT
Slot F0 EEPROM data:
```

```
Product Identifier (PID) : ISR4451-FP
Version Identifier (VID) : V00
PCB Serial Number : FP123456789
Hardware Revision : 4.1
Slot 0 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
CLEI Code : TDBTDBTDBT
Slot 1 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
CLEI Code : TDBTDBTDBT
Slot 2 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
CLEI Code : TDBTDBTDBT
SPA EEPROM data for subslot 0/0:

Product Identifier (PID) : ISR441-4X1GE
Version Identifier (VID) : V01
PCB Serial Number : JAB092709EL
Top Assy. Part Number : 68-2236-01
Top Assy. Revision : A0
Hardware Revision : 2.2
CLEI Code : CNUIAHSAAA
SPA EEPROM data for subslot 0/1 is not available

SPA EEPROM data for subslot 0/2 is not available

SPA EEPROM data for subslot 0/3 is not available

SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 1/0 is not available

SPA EEPROM data for subslot 1/1 is not available

SPA EEPROM data for subslot 1/2 is not available

SPA EEPROM data for subslot 1/3 is not available

SPA EEPROM data for subslot 1/4 is not available

SPA EEPROM data for subslot 2/0 is not available

SPA EEPROM data for subslot 2/1 is not available

SPA EEPROM data for subslot 2/2 is not available

SPA EEPROM data for subslot 2/3 is not available
SPA EEPROM data for subslot 2/4 is not available
```

show environment: Example

In this example, note the output for the slots POE0 and POE1. Cisco IOS XE 3.10 and higher supports an external PoE module.

```
Router# show environment

Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0
```

```
Slot Sensor Current State Reading
---- ------ ------------- -------
P0 Temp: Temp 1 Normal 28 Celsius
P0 Temp: Temp 2 Normal 43 Celsius
P0 Temp: Temp 3 Normal 44 Celsius
P0 V: PEM Out Normal 12404 mV
P0 I: PEM In Normal 1 A
P0 I: PEM Out Normal 7 A
P0 P: In pwr Normal 106 Watts
P0 P: Out pwr Normal 87 Watts
P0 RPM: fan0 Normal 2952 RPM
P2 RPM: fan0 Normal 4421 RPM
P2 RPM: fan1 Normal 4394 RPM
P2 RPM: fan2 Normal 4433 RPM
P2 RPM: fan3 Normal 4410 RPM
P2 P: pwr Normal 6 Watts
POE0 Temp: Temp 1 Normal 44 Celsius
POE0 I: 12v In Normal 2 A
POE0 V: 12v In Normal 12473 mV
POE0 P: In pwr Normal 25 Watts
POE1 Temp: Temp 1 Normal 40 Celsius
POE1 I: 12v In Normal 2 mA
POE1 V: 12v In Normal 12473 mV
POE1 P: In pwr Normal 20 Watts
R0 Temp: Inlet 1 Normal 24 Celsius
R0 Temp: Inlet 2 Normal 26 Celsius
R0 Temp: Outlet 1 Normal 33 Celsius
R0 Temp: Outlet 2 Normal 32 Celsius
R0 Temp: core-B Normal 43 Celsius
R0 Temp: core-C Normal 38 Celsius
R0 V: 12v Normal 12355 mV
R0 V: 5v Normal 5090 mV
R0 V: 3.3v Normal 3331 mV
R0 V: 3.0v Normal 2998 mV
R0 V: 2.5v Normal 2436 mV
R0 V: 1.05v Normal 1049 mV
R0 V: 1.8v Normal 1798 mV
R0 V: 1.2v Normal 1234 mV
R0 V: Vcore-C Normal 1155 mV
R0 V: 1.1v Normal 1104 mV
R0 V: 1.0v Normal 1012 mV
R0 V: 1.8v-A Normal 1782 mV
R0 V: 1.5v-A Normal 1505 mV
R0 V: 1.5v-C1 Normal 1516 mV
R0 V: 1.5v-B Normal 1511 mV
R0 V: Vcore-A Normal 1099 mV
R0 V: 1.5v-C2 Normal 1492 mV
R0 V: Vcore-B1 Normal 891 mV
R0 V: Vcore-B2 Normal 904 mV
R0 V: 0.75v-B Normal 754 mV
R0 V: 0.75v-C Normal 759 mV
R0 I: 12v Normal 8 A
R0 P: pwr Normal 86 Watts
0/1 P: pwr Normal 5 Watts
P1 Temp: Temp 1 Normal 30 Celsius
P1 Temp: Temp 2 Normal 38 Celsius
P1 Temp: Temp 3 Normal 39 Celsius
P1 V: PEM Out Normal 12404 mV
P1 I: PEM In Normal 1 A
P1 I: PEM Out Normal 6 A
P1 P: In pwr Normal 86 Watts
P1 P: Out pwr Normal 68 Watts
P1 RPM: fan0 Normal 2940 RPM
```

show environment all: Example

```
Router# show environment all
Sensor List: Environmental Monitoring
Sensor Location State Reading
Temp: Temp 1 P0 Normal 29 Celsius
```

```
Temp: Temp 2 P0 Normal 43 Celsius
Temp: Temp 3 P0 Normal 44 Celsius
V: PEM Out P0 Normal 12404 mV
I: PEM In P0 Normal 1 A
I: PEM Out P0 Normal 8 A
P: In pwr P0 Normal 111 Watts
P: Out pwr P0 Normal 91 Watts
RPM: fan0 P0 Normal 2940 RPM
RPM: fan0 P2 Normal 4419 RPM
RPM: fan1 P2 Normal 4395 RPM
RPM: fan2 P2 Normal 4426 RPM
RPM: fan3 P2 Normal 4412 RPM
P: pwr P2 Normal 6 Watts
Temp: Temp 1 POE0 Normal 44 Celsius
I: 12v In POE0 Normal 2 A
V: 12v In POE0 Normal 12473 mV
P: In pwr POE0 Normal 25 Watts
Temp: Temp 1 POE1 Normal 40 Celsius
I: 12v In POE1 Normal 2 mA
V: 12v In POE1 Normal 12473 mV
P: In pwr POE1 Normal 20 Watts
Temp: Inlet 1 R0 Normal 24 Celsius
Temp: Inlet 2 R0 Normal 27 Celsius
Temp: Outlet 1 R0 Normal 33 Celsius
Temp: Outlet 2 R0 Normal 32 Celsius
Temp: core-B R0 Normal 49 Celsius
Temp: core-C R0 Normal 37 Celsius
V: 12v R0 Normal 12355 mV
V: 5v R0 Normal 5084 mV
V: 3.3v R0 Normal 3331 mV
V: 3.0v R0 Normal 2998 mV
V: 2.5v R0 Normal 2433 mV
V: 1.05v R0 Normal 1052 mV
V: 1.8v R0 Normal 1798 mV
V: 1.2v R0 Normal 1226 mV
V: Vcore-C R0 Normal 1155 mV
V: 1.1v R0 Normal 1104 mV
V: 1.0v R0 Normal 1015 mV
V: 1.8v-A R0 Normal 1782 mV
V: 1.5v-A R0 Normal 1508 mV
V: 1.5v-C1 R0 Normal 1513 mV
V: 1.5v-B R0 Normal 1516 mV
V: Vcore-A R0 Normal 1099 mV
V: 1.5v-C2 R0 Normal 1492 mV
V: Vcore-B1 R0 Normal 1031 mV
V: Vcore-B2 R0 Normal 901 mV
V: 0.75v-B R0 Normal 754 mV
V: 0.75v-C R0 Normal 754 mV
I: 12v R0 Normal 8 A
P: pwr R0 Normal 97 Watts
P: pwr 0/1 Normal 5 Watts
Temp: Temp 1 P1 Normal 30 Celsius
Temp: Temp 2 P1 Normal 39 Celsius
Temp: Temp 3 P1 Normal 39 Celsius
V: PEM Out P1 Normal 12404 mV
I: PEM In P1 Normal 1 A
I: PEM Out P1 Normal 6 A
P: In pwr P1 Normal 87 Watts
P: Out pwr P1 Normal 66 Watts
RPM: fan0 P1 Normal 2940 RPM
```

show inventory: Example

```
Router# show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
PID: ISR4451/K9 , VID: V01, SN: FGL160110QZ

NAME: "Power Supply Module 0", DESCR: "450W AC Power Supply for Cisco ISR4450"
PID: XXX-XXXX-XX , VID: XXX, SN: DCA1547X047

NAME: "Power Supply Module 1", DESCR: "450W AC Power Supply for Cisco ISR4450"
```

```
PID: XXX-XXXX-XX , VID: XXX, SN: DCA1614Y022

NAME: "Fan Tray", DESCR: "Cisco ISR4450 Fan Assembly"
PID: ACS-4450-FANASSY , VID: , SN:

NAME: "POE Module 0", DESCR: "Single POE for Cisco ISR4451"
PID: PWR-POE-4400 , VID: , SN: FHH1638P00E

NAME: "POE Module 1", DESCR: "Single POE for Cisco ISR4451"
PID: PWR-POE-4400 , VID: , SN: FHH1638P00G

NAME: "GE-POE Module", DESCR: "POE Module for On Board GE for Cisco ISR4400"
PID: 800G2-POE-2 , VID: V01, SN: FOC151849W9

NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451/K9 , VID: , SN:
NAME: "NIM subslot 0/2", DESCR: " NIM-4MFT-T1/E1 - T1/E1 Serial Module"
PID: NIM-4MFT-T1/E1 , VID: V01, SN: FOC16254E6W

NAME: "NIM subslot 0/3", DESCR: "NIM SSD Module"
PID: NIM-SSD , VID: V01, SN: FHH16510032

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9 , VID: , SN:

NAME: "SM subslot 1/0", DESCR: "SM-X-1T3/E3 - Clear T3/E3 Serial Module"
PID: SM-X-1T3/E3 , VID: V01, SN: FOC164750RG

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9 , VID: , SN:

NAME: "SM subslot 2/0", DESCR: "SM-ES3X-24-P: EtherSwitch SM L3 + PoEPlus + MACSec + 24
10/100/1000"
PID: SM-ES3X-24-P , VID: V01, SN: FHH1629007C

NAME: "module R0", DESCR: "Cisco ISR4451 Route Processor"
PID: ISR4451/K9 , VID: V01, SN: FOC15507S95

NAME: "module F0", DESCR: "Cisco ISR4451 Forwarding Processor"
PID: ISR4451/K9 , VID: , SN:
```

show platform: Example

```
Router# show platform
Chassis type: ISR4451/K9

Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 ISR4451/K9 ok 3d11h
0/0 ISR4451-X-4x1GE ok 3d11h
0/2 NIM-4MFT-T1/E1 ok 3d11h
0/3 NIM-SSD ok 3d11h
1 ISR4451/K9 ok 3d11h
1/0 SM-X-1T3/E3 ok 3d11h
2 ISR4451/K9 ok 3d11h
2/0 SM-ES3X-24-P ok 3d11h
R0 ISR4451/K9 ok, active 3d11h
F0 ISR4451/K9 ok, active 3d11h
P0 XXX-XXXX-XX ok 3d11h
P1 XXX-XXXX-XX ok 3d11h
P2 ACS-4450-FANASSY ok 3d11h
POE0 PWR-POE-4400 ok 3d11h
POE1 PWR-POE-4400 ok 3d11h
GE-POE 800G2-POE-2 ok 3d11h
```

show platform diag: Example

```
Router# show platform diag
Chassis type: ISR4451/K9

Slot: 0, ISR4451/K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:43 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Sub-slot: 0/0, ISR4451-X-4x1GE
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Sub-slot: 0/2, NIM-4MFT-T1/E1
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Sub-slot: 0/3, NIM-SSD
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Slot: 1, ISR4451/K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:44 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Sub-slot: 1/0, SM-X-1T3/E3
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Slot: 2, ISR4451/K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:45 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Sub-slot: 2/0, SM-ES3X-24-P
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Slot: R0, ISR4451/K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:04 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Slot: F0, ISR4451/K9
Running state : ok, active
```

```
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:02:39 (3d10h ago)
Hardware ready signal time : 00:00:00 (never ago)
Packet ready signal time : 00:02:48 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Slot: P0, XXX-XXXX-XX
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: P1, XXX-XXXX-XX
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: P2, ACS-4450-FANASSY
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: POE0, PWR-POE-4451
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: POE1, PWR-POE-4451
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: GE-POE, 800G2-POE-2
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)
```

show platform software status control-processor: Example

```
Router# show platform software status control-processor
RP0: online, statistics updated 2 seconds ago
Load Average: health unknown
1-Min: 0.13, status: health unknown, under
5-Min: 0.07, status: health unknown, under
15-Min: 0.06, status: health unknown, under
Memory (kb): healthy
Total: 3971244
Used: 2965856 (75%)
Free: 1005388 (25%)
Committed: 2460492 (62%), status: health unknown, under 0%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 1.00, System: 2.90, Nice: 0.00, Idle: 96.00
IRQ: 0.10, SIRQ: 0.00, IOwait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 10.71, System: 29.22, Nice: 0.00, Idle: 60.06
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.80, System: 1.30, Nice: 0.00, Idle: 97.90
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 10.61, System: 34.03, Nice: 0.00, Idle: 55.25
IRQ: 0.00, SIRQ: 0.10, IOwait: 0.00
CPU4: CPU Utilization (percentage of time spent)
User: 0.60, System: 1.20, Nice: 0.00, Idle: 98.20
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU5: CPU Utilization (percentage of time spent)
User: 13.18, System: 35.46, Nice: 0.00, Idle: 51.24
IRQ: 0.00, SIRQ: 0.09, IOwait: 0.00
CPU6: CPU Utilization (percentage of time spent)
User: 0.80, System: 2.40, Nice: 0.00, Idle: 96.80
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU7: CPU Utilization (percentage of time spent)
User: 10.41, System: 33.63, Nice: 0.00, Idle: 55.85
```

```
IRQ: 0.00, SIRQ: 0.10, IOwait: 0.00
```

show diag slot RO eeprom detail: Example

```
Router# show diag slot R0 eeprom detail
Slot R0 EEPROM data:

EEPROM version : 4
Compatible Type : 0xFF
PCB Serial Number : FHH153900AU
Controller Type : 1902
Hardware Revision : 0.0
PCB Part Number : 73-13854-01
Top Assy. Part Number : 800-36894-01
Board Revision : 01
Deviation Number : 122081
Fab Version : 01
Product Identifier (PID) : CISCO------<0A>
Version Identifier (VID) : V01<0A>
Chassis Serial Number : FHH1539P00Q
Chassis MAC Address : 0000.0000.0000
MAC Address block size : 96
Asset ID : REV1B<0A>
Asset ID :
```

show version: Example

```
Router# show version
Cisco IOS XE Software, Version 03.13.00.S - Standard Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.4(3)S, RELEASE
 SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 27-May-14 05:36 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 2 hours, 19 minutes
Uptime for this control processor is 2 hours, 22 minutes
System returned to ROM by reload
System image file is "tftp: isr4400-universalk9.03.13.00.S.154-3.S-std.SPA.bin"
Last reload reason: Reload Command


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

```
Technology Package License Information:

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
                   Current       Type                Next reboot
------------------------------------------------------------------
appx               None            None                None
uc                 None            None                None
security           None            None                None
ipbase             ipbasek9       Permanent            ipbasek9

cisco 4451 ISR processor with 1213154K/6147K bytes of memory.
Processor board ID FHH1539P00Q
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3391455K bytes of Compact flash at bootflash:.

Configuration register is 0x0”
```

Configuring Power Supply Mode

You can configure the power supplies of both the router and a connected Power over Ethernet (PoE) module.

- Configuring the Router Power Supply Mode, on page 161
- Configuring the External PoE Service Module Power Supply Mode, on page 161
- Examples for Configuring Power Supply Mode, on page 162
- Available PoE Power, on page 163

Configuring the Router Power Supply Mode

Configure the main power supply on the router using the **power main redundant** command:

- **power main redundant—**Sets the main power supply in redundant mode.
- **no power main redundant—**Sets the main power supply in boost mode.

Note The default mode for the router power supply is redundant mode.

Configuring the External PoE Service Module Power Supply Mode

Configure the power supply of an external PoE service module using the **power inline redundant** command:

- **power inline redundant—**Sets the external PoE service module power supply in redundant mode.
- **no power inline redundant—**Sets the external PoE service module power supply in boost mode.

Note The default mode for the external PoE service module power supply is redundant mode.

The **show power** command shows whether boost or redundant mode is configured and whether this mode is currently running on the system.

Examples for Configuring Power Supply Mode

Example—Configured Mode of Boost for Main PSU and PoE Module

In this example, the **show power** command shows the configured mode as `Boost`, which is also the current runtime state. The `Main PSU` shows information about the main power supply. The `POE Module` shows information about the inline/PoE power. In this example, the current run-time state for the main power supply is the same as the configured state (`Boost` mode).

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 2000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1000 Watts
Router#
```

Example—Configured Mode of Boost for Main PSU and PoE Module

In this example, the **show power** command shows the power supplies that are present in the device. The Main PSU and POE Module are configured to the `Boost` mode, which differs from the current runtime state. The current runtime state is the `Redundant` mode. A likely explanation for this is that there is only one main power supply present in the router. See mode example 4 in the table titled "Modes of Operation" in Available PoE Power, on page 163.

You can enter the **show platform** command to show the power supplies that are present in the device.

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : No
Total power available : 1000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
Router#
```

Example—Configured Mode of Redundant for Main PSU and PoE Module

In this example, the **show power** command shows the configured mode is `Redundant` for both the main and inline power. The system has one 450 W and one 100 W power supply.

```
Router# show power
Main PSU :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : No
```

```
Total power available : 0 Watts
Router#
```

Example—Configured Mode of Boost for Main Power

In this example, the main power is configured to be in `boost` mode by using the **no** form of the **power main redundant** command. This sets the main power to `boost` mode with 1450 W and inline power to `redundant` mode with 500 W.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power main redundant
Router(config)#
*Jan 31 03:35:22.284: %PLATFORM_POWER-6-MODEMATCH: Inline power is in Redundant mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 500 Watts
Router#
```

Example—Configured Mode of Boost for PoE Power

In this example, an attempt is made to configure the inline power in boost mode by using the **no** form of the **power inline redundant** command. The inline power mode is **not** changed to boost mode because that would require a total power available in redundant mode of 1000 W. The inline power mode is redundant and is shown by the following values for the PoE Module:

- `Configured Mode : Boost`
- `Current runtime state same : No`

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
Router(config)#
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
Router#
```

Available PoE Power

For the PoE feature to be available on the external PoE module, the total power from the power supplies must be 500 W or higher.

Note To ensure the PoE feature is functional on the external PoE module, verify the availability of PoE power on your router using the **show platform** and **show power** commands.

To determine there is enough PoE power for use by an external PoE service module, use the **show platform** and **show power** commands to calculate the available PoE power based on the wattage values of the main power supplies and PoE inverters.

Take the values of your main P0 and P1 power supplies to give the Total Power (for main power supplies.) Then take the values of your PoE1 and PoE2 power inverters to calculate the Total PoE Power.

The following table shows example modes of operation, which may be similar to your configuration.

The Total PoE Power value, in the final column of the table needs to be 500 W or higher for the PoE feature to be functional on a connected PoE service module.

Note Add power inverters to the router before inserting an external PoE module. Otherwise, even if the Total PoE Power is sufficient, the PoE power will not be used by the external PoE module and the module will need to be re-booted for the PoE feature to be functional.

Configuring a power mode of boost or redundant on the main power supplies, or PoE inverters, may affect the value for Total PoE Power.

The following table shows all power values in Watts. The wattage ratings of the main power supplies are shown in columns Main P0 and Main P1. The wattage ratings of the PoE inverters are shown in columns PoE0 and PoE1.

Table 12: Modes of Operation

Mode Example	Main P0	Main P1	Config Mode	Total Power (Main)	PoE0	PoE1	Config Mode	Total PoE Power
1	450	None	Redundant or Boost	450	None	500	Redundant or Boost	0 (None)
2	450	450	Boost	900	None	500	Redundant or Boost	0 (None)
3	450	450	Redundant	450	500	None	Redundant or Boost	0 (None)
4	1000	None	Redundant or Boost	1000	500	None	Redundant or Boost	500
5	1000	450	Redundant	450	500	500	Redundant or Boost	0 (None)
6	1000	450	Boost	1450	500	500	Boost	500
7	1000	1000	Redundant	1000	500	500	Boost	500

Mode Example	Main P0	Main P1	Config Mode	Total Power (Main)	PoE0	PoE1	Config Mode	Total PoE Power
8	1000	1000	Boost	2000	500	500	Boost	1000

Note In the table above, for 500 W or higher Total PoE Power to be available, the "Total Power" (of the main power supplies) must be 1000 W or higher.

For 1000 W Total PoE Power (see Mode Example 8 above), there must be two 1000 W main power supplies (in `Boost` mode) and two PoE inverters (also in `Boost` mode).

Caution Care should be taken while removing the power supplies and power inverters (especially in `Boost` mode of operation). If the total power consumption is higher than can be supported by one power supply alone and in this condition a power supply is removed, the hardware can be damaged. This may then result in the system being unstable or unusable.

Similarly, in the case where there is only one PoE inverter providing PoE power to a service module, and in this condition the PoE inverter is removed, the hardware may be damaged, and may result in the system being unstable or unusable.

Managing PoE

The Power over Ethernet (PoE) feature allows you to manage power on the FPGE ports. By using PoE, you do not need to supply connected PoE-enabled devices with wall power. This eliminates the cost for additional electrical cabling that would otherwise be necessary for connected devices. The router supports PoE (802.3af) and PoE+ (802.3at). PoE provides up to 15.4 W of power, and PoE+ provides up to 30 W of power.

- PoE Support for FPGE Ports, on page 165
- Monitoring Your Power Supply, on page 166
- Enabling Cisco Discovery Protocol, on page 112
- Configuring PoE for FPGE Ports, on page 168

PoE Support for FPGE Ports

A PoE module supports PoE on the front panel gigabit ethernet ports (FPGE) such as gig0/0/0 and gig0/0/1. You can configure the PoE service module for the FPGE using the **power inline** command, which allows you to turn on or turn off the power to a connected device such as an IEEE phone or device. For more information, see Configuring PoE for FPGE Ports, on page 168.

Monitoring Your Power Supply

You can monitor the total available power budget on your router using the **show power inline [GigabitEthernet detail]** command in privileged EXEC mode.

This command allows you to check the availability of sufficient power for the powered device type before it is connected to the router.

Example—Inline power where there is no PoE module

In this example, there is no module present that supports PoE. Power is being supplied to an IP phone and a switch.

```
Router# show power inline
Available:31.0(w)  Used:30.3(w)  Remaining:0.7(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         14.9    IP Phone 7971       3     30.0
Gi0/0/1   auto   on         15.4    WS-C2960CPD-8PT-L   4     30.0
Router#
```

In this example, the command includes the following information:

Available:31.0(w)—Available PoE power

Used:30.3(w)—PoE power used by all the router's ports

Oper—PoE power state of each connected powered device (on/off)

Power—PoE power used by each connected powered device

Class—PoE power classification

Example—Inline power for one PoE module

In this example, one module that supports PoE is present. Cisco IOS XE 3.10 and higher supports an external PoE module.

```
Router# show power inline
Available:31.0(w)  Used:30.3(w)  Remaining:0.7(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         14.9    IP Phone 7971       3     30.0
Gi0/0/1   auto   on         15.4    WS-C2960CPD-8PT-L   4     30.0

Available:500.0(w)  Used:11.7(w)  Remaining:488.3(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Et2/0/0   auto   off        11.7    n/a                 n/a   750.0
Router#
```

Example—Inline power to connected IP phones

```
Router# show power inline
Available:31.0(w)  Used:30.8(w)  Remaining:0.2(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
```

```
Gi0/0/0   auto   on         15.4    Ieee PD            4     30.0
Gi0/0/1   auto   on         15.4    Ieee PD            4     30.0
```

Example—Inline power to one Gigabit Ethernet port

```
Router# show power inline gigabitEthernet 0/0/0
Interface Admin  Oper       Power   Device             Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         15.4    Ieee PD            4     30.0
```

Example—Inline power to one Gigabit Ethernet port-detail

```
Router# show power inline gigabitEthernet 0/0/0 detail
Interface: Gi0/0/0
 Inline Power Mode: auto
 Operational status: on
 Device Detected: yes
 Device Type: Ieee PD
 IEEE Class: 4
 Discovery mechanism used/configured: Ieee
 Police: off

 Power Allocated
 Admin Value: 30.0
 Power drawn from the source: 15.4
 Power available to the device: 15.4

 Absent Counter: 0
 Over Current Counter: 0
 Short Current Counter: 0
 Invalid Signature Counter: 0
 Power Denied Counter: 0
```

Example—Inline power to an external PoE service module

In this example, after the output lines for Gi0/0/0, and Gi0/0/1, there are output lines for the external PoE service module. Cisco IOS XE 3.10 and higher supports an external PoE module. Et1/0/0 indicates the internal port (slot 1/0) for the first PoE service module. Et2/0/0 indicates the internal port (slot 2/0) in a second PoE service module.

Although both slots are capable of drawing 750 W of PoE power, in this device only 500 W of PoE power is available. Slot 2/0 (Et2/0/0) has been allocated 369.6 W of PoE power.

```
Router# show power inline
Available:31.0(w)  Used:15.4(w)  Remaining:15.6(w)
Interface Admin  Oper       Power   Device             Class Max
                            (Watts)
--------  ----   --------   -----   -----------------   ---   ---
Gi0/0/0   auto   on         15.4    Ieee PD            4     30.0
Gi0/0/1   auto   off        0.0     n/a                n/a   30.0

Available:500.0(w)  Used:369.6(w)  Remaining:500.0(w)
Interface Admin  Oper       Power   Device             Class Max
                            (Watts)
--------  ----   --------   -----   -----------------   ---   ---
Et1/0/0   auto   off        0.0     n/a                n/a   750.
Et2/0/0   auto   off        369.6   n/a                n/a   750.
```

Enabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is enabled by default on the router.

Note CDP is not enabled by default on Cisco Aggregation Services Routers or on the Cisco CSR 1000v.

For more information on using CDP, see Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S.

Configuring PoE for FPGE Ports

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp run**
4. **interface gigabitethernet** *slot/subslot/port*
5. **cdp enable**
6. **power inline** {**auto** { **auto** [**max** *milli-watts*] | **never**}
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cdp run** **Example:** `Router(config)# cdp run`	Enables Cisco Discovery Protocol (CDP) on your router.
Step 4	**interface gigabitethernet** *slot/subslot/port* **Example:** `Router(config)# interface gigabitEthernet 0/0/0`	Allows to configure PoE on ports 0 and 1. • PoE can be configured on ports 0 and 1.

	Command or Action	Purpose
Step 5	**cdp enable** **Example:** `Router(config-if)#  cdp enable`	Enables CDP in the interface configuration mode.

Step 6	**power inline** {**auto** { **auto** [**max** *milli-watts*] | **never**}
	Example:
	`Router(config-if)# power inline auto`
		Allows you to set the power inline options for FPGE ports.
		• **auto—**The **auto** keyword automatically detects the power inline devices and supplies power to such devices.
		• **max** *milli-watts***—**The **max** keyword sets the maximum power allowed on the interface.
		• **never—**The **never** keyword disables the detection and ceases the application of inline power.

Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.

Verifying if PoE Is Enabled on FPGE Port

You can verify whether the PoE is enabled on the FPGE port by looking at the external LED for this port. The external LED for the FPGE port is labelled as GE POE. The GE POE emits a green light when the internal PoE module is plugged in and functioning properly. The GE POE LED is yellow when the internal PoE is plugged in but not functioning properly. The GE POE LED is off when there are no PoE modules plugged in. For more information on LEDs, see the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

You can also detect PoE using the **show platform** and **show diag** commands.

For more information, see the following examples.

show platform: Example

```
Router# show platform
Chassis type: ISR4451/K9

Chassis type: ISR4451/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451/K9          ok                    3d11h
 0/0      ISR4451-X-4x1GE     ok                    3d11h
 0/2       NIM-4MFT-T1/E1    ok                   3d11h
 0/3      NIM-SSD             ok                    3d11h
1         ISR4451/K9          ok                    3d11h
 1/0      SM-X-1T3/E3         ok                    3d11h
2         ISR4451/K9          ok                    3d11h
 2/0      SM-ES3X-24-P        ok                    3d11h
R0        ISR4451/K9          ok, active            3d11h
F0        ISR4451/K9          ok, active            3d11h
```

```
P0        XXX-XXXX-XX         ok                    3d11h
P1        XXX-XXXX-XX         ok                    3d11h
P2        ACS-4451-FANTRAY    ok                    3d11h
POE0      PWR-POE-4451-X      ok                    3d11h
POE1      PWR-POE-4451-X      ok                    3d11h
GE-POE    800G2-POE-2         ok                    3d11h

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         12090323            15.3(01r)S            [ciscouser-ISRRO...
1         12090323            15.3(01r)S            [ciscouser-ISRRO...
2         12090323            15.3(01r)S            [ciscouser-ISRRO...
R0        12090323            15.3(01r)S            [ciscouser-ISRRO...
F0        12090323            15.3(01r)S            [ciscouser-ISRRO...
```

show diag chassis eeprom: Example

```
Router# show diag chassis eeprom
MIDPLANE EEPROM data:

        Product Identifier (PID) : ISR-4451/K9
        Version Identifier (VID) : V01
        PCB Serial Number        : FOC16145VL8
        Hardware Revision        : 1.0
        Asset ID                 : P1C-R03-CP1.0-UMT-RVC
        CLEI Code                : TBD
Power/Fan Module P0 EEPROM data:

        Product Identifier (PID) : PWR-4450-AC
        Version Identifier (VID) : V01
        PCB Serial Number        : DCA1547X02U
        CLEI Code                : 0000000000
Power/Fan Module P1 EEPROM data is not initialized

Power/Fan Module P2 EEPROM data is not initialized

Internal PoE EEPROM data:

        Product Identifier (PID) : PWR-GE-POE-4400
        Version Identifier (VID) : V01
        PCB Serial Number        : FOC151849VD
        Hardware Revision        : 1.0
        CLEI Code                : 0000000000
```

Additional References

The following sections provide references related to the power efficiency management feature.

MIBs

MIBs	MIBs Link
CISCO-ENTITY-FRU-CONTROL-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator at: http://www.cisco.com/go/mibs. Also see MIB Specifications Guide for the Cisco 4451-X Integrated Services Router.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

CHAPTER 14

Configuring High Availability

The Cisco High Availability (HA) technology enable network-wide protection by providing quick recovery from disruptions that may occur in any part of a network. A network's hardware and software work together with Cisco High Availability technology, which besides enabling quick recovery from disruptions, ensures fault transparency to users and network applications.

The following sections describe how to configure Cisco High Availability features on your router:

About Cisco High Availability

The unique hardware and software architecture of your router is designed to maximize router uptime during any network event, and thereby provide maximum uptime and resilience within any network scenario.

This section covers some aspects of Cisco High Availability that may be used on the Cisco 4000 series routers:

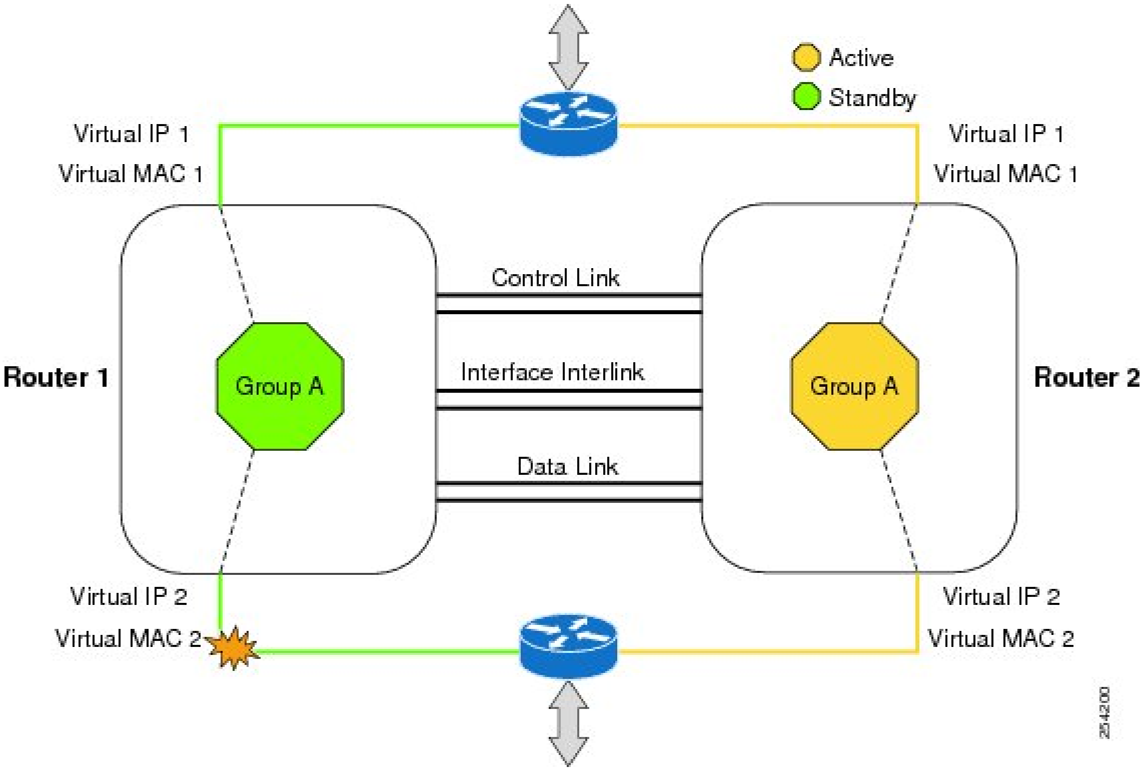
- Interchassis High Availability, on page 173
- Bidirectional Forwarding Detection, on page 175

Interchassis High Availability

The Interchassis High Availability feature is also known as the box-to-box redundancy feature. Interchassis High Availability enables the configuration of pairs of routers to act as backup for each other. This feature can be configured to determine the active router based on several failover conditions. When a failover occurs, the standby router seamlessly takes over and starts processing call signaling and performing media forwarding tasks.

Groups of redundant interfaces are known as redundancy groups. The following figure depicts the active-standby device scenario. It shows how the redundancy group is configured for a pair of routers that have a single outgoing interface.

Figure 5: Redundancy Group Configuration



The routers are joined by a configurable control link and data synchronization link. The control link is used to communicate the status of the routers. The data synchronization link is used to transfer stateful information to synchronize the stateful database for the calls and media flows. Each pair of redundant interfaces are configured with the same unique ID number, also known as the RII. For information on configuring Interchassis HA on your router, see Configuring Interchassis High Availability, on page 175.

IPsec Failover

The IPsec Failover feature increases the total uptime (or availability) of your IPsec network. Traditionally, the increased availability of your IPsec network is accomplished by employing a redundant (standby) router in addition to the original (active) router. When the active router becomes unavailable for a reason, the standby router takes over the processing of IKE and IPsec. IPsec failover falls into two categories: stateless failover and stateful failover.

On the router, only the stateless form of IPsec failover is supported. This stateless failover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary to secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast-forwarding path-failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast-forwarding path-failure detection, BFD provides a consistent failure detection method for network administrators. Because a network administrator can use BFD to detect forwarding path failures at a uniform rate rather than variable rates for different routing protocol hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable.

For more information on BFD, see the “Bidirectional Forwarding Detection” section in the IP Routing BFD Configuration Guide, Cisco IOS XE Release 3S.

Bidirectional Forwarding Detection Offload

The Bidirectional Forwarding Detection Offload feature allows the offload of BFD session management to the forwarding engine for improved failure detection times. BFD offload reduces the overall network convergence time by sending rapid failure detection packets (messages) to the routing protocols for recalculating the routing table. See Configuring BFD Offload, on page 176.

Configuring Cisco High Availability

- Configuring Interchassis High Availability, on page 175
- Configuring Bidirectional Forwarding, on page 176
- Verifying Interchassis High Availability, on page 177
- Verifying BFD Offload, on page 183

Configuring Interchassis High Availability

Prerequisites

- The active device and the standby device must run on the identical version of the Cisco IOS XE software.
- The active device and the standby device must be connected through an L2 connection for the control path.
- The Embedded Service Processor (ESP) must be the same on both the active and standby devices. Route processors must also match and have a similar physical configuration.
- Either the Network Time Protocol (NTP) must be configured or the clock must be set identical on both devices to allow timestamps and call timers to match.
- Virtual router forwarding (VRF) must be defined in the same order on both active and standby routers for an accurate synchronization of data.
- The latency times must be minimal on all control and data links to prevent timeouts.
- Physically redundant links, such as Gigabit EtherChannel, must be used for the control and data paths.

Restrictions

- The failover time for a box-to-box application is higher for a non-box-to-box application.
- LAN and MESH scenarios are not supported.
- The maximum number of virtual MACs supported by the Front Panel Gigabit Ethernet (FPGE) interfaces depends on the platform. For information about the FPGE interfaces, see the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.
- When the configuration is replicated to the standby router, it is not committed to the startup configuration; it is in the running configuration. A user must run the **write memory** command to commit the changes that have been synchronized from the active router, on the standby router.

How to Configure Interchassis High Availability

For more information on configuring Interchassis High Availability on the router, see the IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S.

Configuring Bidirectional Forwarding

For information on configuring BFD on your router, see the IP Routing BFD Configuration Guide.

For BFD commands, see the Cisco IOS IP Routing: Protocol-Independent Command Reference document.

Configuring BFD Offload

Restrictions

- Only BFD version 1 is supported.
- When configured, only offloaded BFD sessions are supported;, BFD session on RP are not supported.
- Only Asynchronous mode or no echo mode of BFD is supported.
- 511 asynchronous BFD sessions are supported.
- BFD hardware offload is supported for IPv4 sessions with non-echo mode only.
- BFD offload is supported only on port-channel interfaces.
- BFD offload is supported only for the Ethernet interface.
- BFD offload is not supported for IPv6 BFD sessions.
- BFD offload is not supported for BFD with TE/FRR.

How to Configure BFD Offload

BFD offload functionality is enabled by default. You can configure BFD hardware offload on the route processor. For more information, see Configuring BFD and the IP Routing BFD Configuration Guide.

Verifying Interchassis High Availability

Use the following **show** commands to verify the Interchassis High Availability.

Note Prerequisites and links to additional documentation configuring Interchassis High Availability are listed in Configuring Interchassis High Availability, on page 175.

- **show redundancy application group [group-id | all]**
- **show redundancy application transport {client | group [group-id]}**
- **show redundancy application control-interface group [group-id]**
- **show redundancy application faults group [group-id]**
- **show redundancy application protocol {protocol-id | group [group-id]}**
- **show redundancy application if-mgr group [group-id]**
- **show redundancy application data-interface group [group-id]**

The following example shows the redundancy application groups configured on the router:

```
Router# show redundancy application group
Group ID    Group Name                      State
--------    ----------                      -----
1           Generic-Redundancy-1            STANDBY
2           Generic-Redundancy2             ACTIVE
```

The following example shows the details of redundancy application group 1:

```
Router# show redundancy application group 1
Group ID:1
Group Name:Generic-Redundancy-1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE
```

The following example shows the details of redundancy application group 2:

```
Router# show redundancy application group 2
Group ID:2
Group Name:Generic-Redundancy2

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

The following example shows details of the redundancy application transport client:

```
Router# show redundancy application transport client
Client         Conn#  Priority   Interface   L3        L4
( 0)RF           0      1         CTRL       IPV4      SCTP

( 1)MCP_HA       1      1         DATA       IPV4      UDP_REL

( 4)AR           0      1         ASYM       IPV4      UDP

( 5)CF           0      1         DATA       IPV4      SCTP
```

The following example shows configuration details for the redundancy application transport group:

```
Router# show redundancy application transport group
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       1.1.1.1         59000    1.1.1.2         59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
1    1       9.9.9.2         53000    9.9.9.1         53000    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       0.0.0.0         0        0.0.0.0         0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       9.9.9.2         59001    9.9.9.1         59001    DATA    IPV4    SCTP
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       1.1.1.1         59004    1.1.1.2         59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       9.9.9.2         53002    9.9.9.1         53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       0.0.0.0         0        0.0.0.0         0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       9.9.9.2         59005    9.9.9.1         59005    DATA    IPV4    SCTP
```

The following example shows the configuration details of redundancy application transport group 1:

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       1.1.1.1         59000    1.1.1.2         59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
1    1       9.9.9.2         53000    9.9.9.1         53000    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       0.0.0.0         0        0.0.0.0         0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       9.9.9.2         59001    9.9.9.1         59001    DATA    IPV4    SCTP
```

The following example shows configuration details of redundancy application transport group 2:

```
Router# show redundancy application transport group 2
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       1.1.1.1         59004    1.1.1.2         59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       9.9.9.2         53002    9.9.9.1         53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       0.0.0.0         0        0.0.0.0         0        NONE_IN NONE_L3 NONE_L4
Client = CF
```

```
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       9.9.9.2         59005    9.9.9.1         59005    DATA    IPV4    SCTP
```

The following example shows configuration details of the redundancy application control-interface group:

```
Router# show redundancy application control-interface group
The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0

The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

The following example shows configuration details of the redundancy application control-interface group 1:

```
Router# show redundancy application control-interface group 1
The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

The following example shows configuration details of the redundancy application control-interface group 2:

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

The following example shows configuration details of the redundancy application faults group:

```
Router# show redundancy application faults group
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The following example shows configuration details specific to redundancy application faults group 1:

```
Router# show redundancy application faults group 1
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The following example shows configuration details specific to redundancy application faults group 2:

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The following example shows configuration details for the redundancy application protocol group:

```
Router# show redundancy application protocol group
RG Protocol RG 1
------------------
Role: Standby
```

```
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 1.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 117, Bytes 7254, HA Seq 0, Seq Number 117, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 115, Bytes 3910, HA Seq 0, Seq Number 1453975, Pkt Loss 0



RG Protocol RG 2
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 1.1.1.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 118, Bytes 7316, HA Seq 0, Seq Number 118, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 102, Bytes 3468, HA Seq 0, Seq Number 1453977, Pkt Loss 0
```

The following example shows configuration details for the redundancy application protocol group 1:

```
Router# show redundancy application protocol group 1
RG Protocol RG 1
------------------
Role: Standby
```

```
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 1.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 120, Bytes 7440, HA Seq 0, Seq Number 120, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 118, Bytes 4012, HA Seq 0, Seq Number 1453978, Pkt Loss 0
```

The following example shows configuration details for the redundancy application protocol group 2:

```
Router# show redundancy application protocol group 2
RG Protocol RG 2
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 1.1.1.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 123, Bytes 7626, HA Seq 0, Seq Number 123, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 107, Bytes 3638, HA Seq 0, Seq Number 1453982, Pkt Loss 0
```

The following example shows configuration details for the redundancy application protocol 1:

```
Router# show redundancy application protocol 1
Protocol id: 1, name: rg-protocol-1
BFD: ENABLE
Hello timer in msecs: 3000
```

```
Hold timer in msecs: 10000
OVLD-1#show redundancy application protocol 2
Protocol id: 2, name: rg-protocol-2
BFD: ENABLE
Hello timer in msecs: 3000
Hold timer in msecs: 10000
```

The following example shows configuration details for redundancy application interface manager group:

```
Router# show redundancy application if-mgr group
 RG ID: 1
 ==========

 interface      GigabitEthernet0/0/3.152
 ----------------------------------------
 VMAC           0007.b421.4e21
 VIP            55.1.1.255
 Shut           shut
 Decrement      10

 interface      GigabitEthernet0/0/2.152
 ----------------------------------------
 VMAC           0007.b421.5209
 VIP            45.1.1.255
 Shut           shut
 Decrement      10


 RG ID: 2
 ==========

 interface      GigabitEthernet0/0/3.166
 ----------------------------------------
 VMAC           0007.b422.14d6
 VIP            4.1.255.254
 Shut           no shut
 Decrement      10

 interface      GigabitEthernet0/0/2.166
 ----------------------------------------
 VMAC           0007.b422.0d06
 VIP            3.1.255.254
 Shut           no shut
 Decrement      10
```

The following examples shows configuration details for redundancy application interface manager group 1 and group 2:

```
Router# show redundancy application if-mgr group 1

 RG ID: 1
 ==========

 interface      GigabitEthernet0/0/3.152
 ----------------------------------------
 VMAC           0007.b421.4e21
 VIP            55.1.1.255
 Shut           shut
 Decrement      10

 interface      GigabitEthernet0/0/2.152
 ----------------------------------------
 VMAC           0007.b421.5209
 VIP            45.1.1.255
 Shut           shut
 Decrement      10

Router# show redundancy application if-mgr group 2
 RG ID: 2
 ==========

 interface      GigabitEthernet0/0/3.166
 ----------------------------------------
 VMAC           0007.b422.14d6
 VIP            4.1.255.254
 Shut           no shut
 Decrement      10

 interface      GigabitEthernet0/0/2.166
 ---------------------------------------
 VMAC           0007.b422.0d06
 VIP            3.1.255.254
 Shut           no shut
 Decrement      10
```

The following example shows configuration details for redundancy application data-interface group:

```
Router# show redundancy application data-interface group
The data interface for rg[1] is GigabitEthernet0/0/1
The data interface for rg[2] is GigabitEthernet0/0/1
```

The following examples show configuration details specific to redundancy application data-interface group 1 and group 2:

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/0/1

Router # show redundancy application data-interface group 2
The data interface for rg[2] is GigabitEthernet0/0/1
```

Verifying BFD Offload

Use the following commands to verify and monitor BFD offload feature on your router.

Note Configuration of BFD Offload is described in Configuring Bidirectional Forwarding, on page 176.

- **show bfd neighbors [details]**
- **debug bfd [packet | event]**
- **debug bfd event**

The **show bfd neighbors** command displays the BFD adjacency database:

```
Router# show bfd neighbor

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.10.1.1                             362/1277      Up        Up        Gi0/0/1.2
192.10.2.1                             445/1278      Up        Up        Gi0/0/1.3
192.10.3.1                            1093/961       Up        Up        Gi0/0/1.4
192.10.4.1                            1244/946       Up        Up        Gi0/0/1.5
192.10.5.1                            1094/937       Up        Up        Gi0/0/1.6
192.10.6.1                            1097/1260      Up        Up        Gi0/0/1.7
192.10.7.1                            1098/929       Up        Up        Gi0/0/1.8
192.10.8.1                            1111/928       Up        Up        Gi0/0/1.9
192.10.9.1                            1100/1254      Up        Up        Gi0/0/1.10
```

The **debug bfd neighbor detail** command displays the debugging information related to BFD packets:

```
Router# show bfd neighbor detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.10.1.1                             362/1277      Up        Up        Gi0/0/1.2
Session state is UP and not using echo function.
Session Host: Hardware
OurAddr: 192.10.1.2
Handle: 33
```

```
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 50(0)
Rx Count: 3465, Rx Interval (ms) min/max/avg: 42/51/46
Tx Count: 3466, Tx Interval (ms) min/max/avg: 39/52/46
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF EIGRP
Uptime: 00:02:50
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 1
             Multiplier: 3               - Length: 24
             My Discr.: 1277             - Your Discr.: 362
             Min tx interval: 50000      - Min rx interval: 50000
             Min Echo interval: 0
```

The **show bfd summary** command displays the BFD summary:

```
Router# show bfd summary

                    Session          Up           Down

Total                   400         400             0
```

The **show bfd drops** command displays the number of packets dropped in BFD:

```
Router# show bfd drops
BFD Drop Statistics
                      IPV4     IPV6    IPV4-M    IPV6-M    MPLS_PW   MPLS_TP_LSP
Invalid TTL             0         0       0         0           0       0
BFD Not Configured      0         0       0         0           0       0
No BFD Adjacency        33        0       0         0           0       0
Invalid Header Bits     0         0       0         0           0       0
Invalid Discriminator   1         0       0         0           0       0
Session AdminDown       94        0       0         0           0       0
Authen invalid BFD ver  0         0       0         0           0       0
Authen invalid len      0         0       0         0           0       0
Authen invalid seq      0         0       0         0           0       0
Authen failed           0         0       0         0           0       0
```

The **debug bfd packet** command displays debugging information about BFD control packets.

```
Router# debug bfd packet
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Rx IP:192.11.22.1 ld/rd:1941/0 diag:0(No Diagnostic)
 Down C cnt:4 ttl:254 (0)
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Tx IP:192.11.22.1 ld/rd:983/1941 diag:3(Neighbor
Signaled Session Down) Init  C cnt:44 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Rx IP:192.11.22.1 ld/rd:1941/983 diag:0(No Diagnostic)
 Up PC cnt:4 ttl:254 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Tx IP:192.11.22.1 ld/rd:983/1941 diag:0(No Diagnostic)
 Up F C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.11.22.1 ld/rd:1941/983 diag:0(No Diagnostic)
 Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.11.22.1 ld/rd:983/1941 diag:0(No Diagnostic)
 Up  C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.11.90.1 ld/rd:1907/0 diag:0(No Diagnostic)
 Down C cnt:3 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.11.90.1 ld/rd:993/1907 diag:3(Neighbor
Signaled Session Down) Init  C cnt:43 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.11.22.1 ld/rd:1941/983 diag:0(No Diagnostic)
 Up C cnt:0 ttl:254 (0)
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Rx IP:192.11.90.1 ld/rd:1907/993 diag:0(No Diagnostic)
 Up PC cnt:3 ttl:254 (0)
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Tx IP:192.11.90.1 ld/rd:993/1907 diag:0(No Diagnostic)
 Up F C cnt:0 (0)
*Nov 12 23:08:28.645: BFD-DEBUG Packet: Rx IP:192.11.90.1 ld/rd:1907/993 diag:0(No Diagnostic)
 Up C cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Rx IP:192.11.90.1 ld/rd:1907/993 diag:0(No Diagnostic)
 Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Tx IP:192.11.90.1 ld/rd:993/1907 diag:0(No Diagnostic)
 Up  C cnt:0 (0)
*Nov 12 23:08:28.993: BFD-DEBUG Packet: Rx IP:192.11.90.1 ld/rd:1907/993 diag:0(No Diagnostic)
 Up C cnt:0 ttl:254 (0)
```

The **debug bfd event** displays debugging information about BFD state transitions:

```
Router# deb bfd event

*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.10.16.1, ld:1401,
handle:77, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.10.16.1, ld:1401, handle:77,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.10.153.1, ld:1400,
handle:39, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.10.153.1, ld:1400, handle:39,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.168.0.1, ld:1399,
handle:25, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.168.0.1, ld:1399, handle:25,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.10.30.1, ld:1403,
handle:173, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.10.30.1, ld:1403, handle:173,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.10.36.1, ld:1402,
handle:95, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.10.36.1, ld:1402, handle:95,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Flags: Poll 0 Final 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Buffer: 0x23480318 0x0000057C 0x00000000
0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Flags: Poll 0 Final 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Buffer: 0x23480318 0x0000057D 0x00000000
0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.649: BFD-DEBUG Packet: Rx IP:192.10.33.1 ld/rd:1601/1404
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1404 handle:207 event:RX ADMINDOWN state:UP
 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1404 handle:207 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.10.33.1, ld:1404, handle:207,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.10.33.1 ld/rd:1404/0 diag:3(Neighbor
Signaled Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Rx IP:192.10.85.1 ld/rd:1620/1405
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1405 handle:209 event:RX ADMINDOWN state:UP
 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1405 handle:209 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.10.85.1, ld:1405, handle:209,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.10.85.1 ld/rd:1405/0 diag:3(Neighbor
Signaled Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.10.33.1, ld:1404,
handle:207, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.10.33.1, ld:1404, handle:207,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.10.85.1, ld:1405,
handle:209, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.10.85.1, ld:1405, handle:209,
 event:DOWN adminDown, (0)
*Nov 12 23:11:31.035: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 192.10.191.1
```

Additional References

The following documents provide information related to the BFD feature.

Related Topic	Document Title
Configuring Stateful Interchassis Configuration.	*Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS XE Release 3S* at: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book.html.
IP Routing Protocol-Independent Commands.	*Cisco IOS IP Routing: Protocol-Independent Command Reference* at: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/command/iri-cr-book.html.

CHAPTER 15

Configuring Call Home

The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and use of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

This chapter describes how to configure the Call Home feature in Cisco IOS Release 15.4(3)S and later releases for the Cisco ISR 4400 Series and Cisco ISR 4300 Series Routers.

This chapter includes the following sections:

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use the Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, see http://tools.cisco.com/ITDIT/CFN/. A Cisco account is not required to access the Cisco Feature Navigator.

Prerequisites for Call Home

The following are the prerequisites before you configure Call Home:

- Contact e-mail address (required for full registration with Smart Call Home, optional if Call Home is enabled in anonymous mode), phone number (optional), and street address information (optional) should be configured so that the receiver can determine the origin of messages received.
- At least one destination profile (predefined or user-defined) must be configured. The destination profile you use depends on whether the receiving entity is a pager, an e-mail address, or an automated service such as Cisco Smart Call Home.

  If the destination profile uses e-mail message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server.
- The router must have IP connectivity to an e-mail server or the destination HTTP server.
- If Cisco Smart Call Home is used, an active service contract covering the device is required to provide full Cisco Smart Call Home service.

Information About Call Home

The Call Home feature can deliver alert messages containing information on configuration, environmental conditions, inventory, syslog, snapshot, and crash events. It provides these alert messages as either e-mail-based or web-based messages. Multiple message formats are available, allowing for compatibility with pager services, standard e-mail, or XML-based automated parsing applications. This feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles, each with configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC (callhome@cisco.com). You can also define your own destination profiles.

Flexible message delivery and format options make it easy to integrate specific support requirements.

This section contains the following subsections:

- Benefits of Using Call Home
- Obtaining Smart Call Home Services

Benefits of Using Call Home

The Call Home feature offers the following benefits:

- Multiple message-format options, which include:
  - Short Text—Suitable for pagers or printed reports.
  - Plain Text—Full formatted message information suitable for human reading.
  - XML—Machine-readable format using XML and Adaptive Markup Language (AML) document type definitions (DTDs). The XML format enables communication with the Cisco TAC.
- Multiple concurrent message destinations.

- Multiple message categories including configuration, environmental conditions, inventory, syslog, snapshot, and crash events.
- Filtering of messages by severity and pattern matching.
- Scheduling of periodic message sending.

Obtaining Smart Call Home Services

If you have a service contract directly with Cisco, you can register for the Smart Call Home service. Smart Call Home analyzes Smart Call Home messages and provides background information and recommendations. For known issues, particularly online diagnostics failures, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time diagnostic alerts.
- Analysis of Smart Call Home messages and, if needed, Automatic Service Request generation routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through an HTTP proxy server or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices provides access to associated field notices, security advisories, and end-of-life information.

You need the following items to register for Smart Call Home:

- SMARTnet contract number for your router
- Your e-mail address
- Your Cisco.com username

For more information about Smart Call Home, see https://supportforums.cisco.com/community/4816/smart-call-home.

Anonymous Reporting

Smart Call Home is a service capability included with many Cisco service contracts and is designed to assist customers resolve problems more quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your customer identity will remain anonymous, and no identifying information will be sent.

Note When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on behalf of Cisco (including countries outside the United States). Cisco maintains the privacy of all customers. For information about how Cisco treats personal information, see the Cisco Privacy Statement at http://www.cisco.com/web/siteassets/legal/privacy.html.

When Call Home is configured in an anonymous way, only crash, inventory, and test messages are sent to Cisco. No customer identifying information is sent.

For more information about what is sent in these messages, see Alert Group Trigger Events and Commands, on page 227.

How to Configure Call Home

The following sections show how to configure Call Home using a single command:

- Configuring Smart Call Home (Single Command), on page 190
- Configuring and Enabling Smart Call Home, on page 191

The following sections show detailed or optional configurations:

- Enabling and Disabling Call Home, on page 192
- Configuring Contact Information, on page 192
- Configuring Destination Profiles, on page 194
- Subscribing to Alert Groups, on page 198
- Configuring General E-Mail Options, on page 203
- Specifying Rate Limit for Sending Call Home Messages, on page 205
- Specifying HTTP Proxy Server, on page 206
- Enabling AAA Authorization to Run IOS Commands for Call Home Messages, on page 206
- Configuring Syslog Throttling, on page 207
- Configuring Call Home Data Privacy, on page 208
- Sending Call Home Communications Manually, on page 209

Configuring Smart Call Home (Single Command)

To enable all Call Home basic configurations using a single command, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*] **Example:** `Router(config)# call-home reporting contact-email-addr email@company.com`	Enables the basic configurations for Call Home using a single command. • **anonymous**—Enables Call-Home TAC profile to send only crash, inventory, and test messages and send the messages anonymously. • **contact-email-addr**—Enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process. • **http-proxy** {*ipv4-address* | *ipv6-address* | *name*}—Configures an ipv4 or ipv6 address or server name. Maximum length is 64 characters. • **port** *port-number*—Port number. Range is 1 to 65535. **Note** The HTTP proxy option allows you to make use of your own proxy server to buffer and secure Internet connections from your devices. **Note** After successfully enabling Call Home either in anonymous or full registration mode using the **call-home reporting** command, an inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. For more information about what is sent in these messages, see Alert Group Trigger Events and Commands, on page 227.

Configuring and Enabling Smart Call Home

For application and configuration information about the Cisco Smart Call Home service, see the “Getting Started” section of the Smart Call Home User Guide at https://supportforums.cisco.com/community/4816/smart-call-home. This document includes configuration examples for sending Smart Call Home messages directly from your device or through a transport gateway (TG) aggregation point.

Note For security reasons, we recommend that you use the HTTPS transport options, due to the additional payload encryption that HTTPS offers. The Transport Gateway software is downloadable from Cisco.com and is available if you require an aggregation point or a proxy for connection to the Internet.

Enabling and Disabling Call Home

To enable or disable the Call Home feature, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **service call-home**
3. **no service call-home**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**service call-home** **Example:** `Router(config)# service call-home`	Enables the Call Home feature.
Step 3	**no service call-home** **Example:** `Router(config)# no service call-home`	Disables the Call Home feature.

Configuring Contact Information

Each router must include a contact e-mail address (except if Call Home is enabled in anonymous mode). You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **contact-email-addr** *email-address*
4. **phone-number** +*phone-number*
5. **street-address** *street-address*
6. **customer-id** *text*
7. **site-id** *text*
8. **contract-id** *text*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**contact-email-addr** *email-address* **Example:** `Router(cfg-call-home)# contact-email-addr username@example.com`	Designates your e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 4	**phone-number** +*phone-number* **Example:** `Router(cfg-call-home)# phone-number +1-800-555-4567`	(Optional) Assigns your phone number. **Note** The number must begin with a plus (+) prefix and may contain only dashes (-) and numbers. Enter up to 17 characters. If you include spaces, you must enclose your entry in quotes ("").
Step 5	**street-address** *street-address* **Example:** `Router(cfg-call-home)# street-address "1234 Picaboo Street, Any city, Any state, 12345"`	(Optional) Assigns your street address where RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes ("").
Step 6	**customer-id** *text* **Example:** `Router(cfg-call-home)# customer-id Customer1234`	(Optional) Identifies customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes ("").
Step 7	**site-id** *text* **Example:** `Router(cfg-call-home)# site-id Site1ManhattanNY`	(Optional) Identifies customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes ("").
Step 8	**contract-id** *text* **Example:** `Router(cfg-call-home)# contract-id Company1234`	(Optional) Identifies your contract ID for the router. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes ("").

Example

The following example shows how to configure contact information:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# phone-number +1-800-555-4567
Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345”
Router(cfg-call-home)# customer-id Customer1234
Router(cfg-call-home)# site-id Site1ManhattanNY
Router(cfg-call-home)# contract-id Company1234
Router(cfg-call-home)# exit
```

Configuring Destination Profiles

A destination profile contains the required delivery information for an alert notification. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

You can create and define a new destination profile or copy and use the predefined destination profile. If you define a new destination profile, you must assign a profile name.

Note If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.

You can configure the following attributes for a destination profile:

- Profile name—String that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive.

  Note You cannot use **all** as a profile name.

- Transport method—Transport mechanism, either e-mail or HTTP (including HTTPS), for delivery of alerts.
  - For user-defined destination profiles, e-mail is the default, and you can enable either or both transport mechanisms. If you disable both methods, e-mail is enabled.
  - For the predefined Cisco TAC profile, you can enable either transport mechanism, but not both.

- Destination address—The actual address related to the transport method to which the alert should be sent.

- Message formatting—The message format used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined Cisco TAC profile, only XML is allowed.

- Message size—The maximum destination message size. The valid range is 50 to 3,145,728 Bytes. The default is 3,145,728 Bytes.
  Anonymous reporting—You can choose for your customer identity to remain anonymous, and no identifying information is sent.

- Subscribing to interesting alert-groups—You can choose to subscribe to alert-groups highlighting your interests.

This section contains the following subsections:

- Creating a New Destination Profile, on page 195
- Copying a Destination Profile, on page 196
- Setting Profiles to Anonymous Mode, on page 197

Creating a New Destination Profile

To create and configure a new destination profile, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. [**no**] **destination transport-method** {**email** | **http**}
5. **destination address** {**email** *email-address* | **http** *url*}
6. **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}
7. **destination message-size-limit** *bytes*
8. **active**
9. **end**
10. **show call-home profile** {*name* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**profile** *name* **Example:** `Router(config-call-home)# profile profile1`	Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.

Step 4	[**no**] **destination transport-method** {**email** | **http**}
	Example:
	`Router(cfg-call-home-profile)# destination transport-method email`
		(Optional) Enables the message transport method. The **no** option disables the method.

	Command or Action	Purpose

Step 5	**destination address** {**email** *email-address* | **http** *url*}
	Example:
	`Router(cfg-call-home-profile)# destination address email myaddress@example.com`
		Configures the destination e-mail address or URL to which Call Home messages are sent.
		Note When entering a destination URL, include either **http://** or **https://**, depending on whether the server is a secure server.

Step 6	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**}
	Example:
	`Router(cfg-call-home-profile)# destination preferred-msg-format xml`
		(Optional) Configures a preferred message format. The default is XML.

Step 7	**destination message-size-limit** *bytes* **Example:** `Router(cfg-call-home-profile)# destination message-size-limit 3145728`	(Optional) Configures a maximum destination message size for the destination profile.
Step 8	**active** **Example:** `Router(cfg-call-home-profile)# active`	Enables the destination profile. By default, the profile is enabled when it is created.

Step 9	**end**
	Example:
	`Router(cfg-call-home-profile)# end`
		Returns to privileged EXEC mode.

Step 10	**show call-home profile** {*name* | **all**}
	Example:
	`Router# show call-home profile profile1`
		Displays the destination profile configuration for the specified profile or all configured profiles.

Copying a Destination Profile

To create a new destination profile by copying an existing profile, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **copy profile** *source-profile target-profile*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**copy profile** *source-profile target-profile* **Example:** `Router(cfg-call-home)# copy profile profile1 profile2`	Creates a new destination profile with the same configuration settings as the existing destination profile.

Setting Profiles to Anonymous Mode

To set an anonymous profile, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. **anonymous-reporting-only**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**profile** *name* **Example:** `Router(cfg-call-home) profile Profile-1`	Enables the profile configuration mode.

	Command or Action	Purpose
Step 4	**anonymous-reporting-only** **Example:** `Router(cfg-call-home-profile)# anonymous-reporting-only`	Sets the profile to anonymous mode. **Note** By default, Call Home sends a full report of all types of events subscribed in the profile. When **anonymous-reporting-only** is set, only crash, inventory, and test messages will be sent.

Subscribing to Alert Groups

An alert group is a predefined subset of Call Home alerts supported in all routers. Different types of Call Home alerts are grouped into different alert groups depending on their type. The following alert groups are available:

- Crash
- Configuration
- Environment
- Inventory
- Snapshot
- Syslog

This section contains the following subsections:

- Periodic Notification, on page 201
- Message Severity Threshold, on page 201
- Configuring a Snapshot Command List, on page 202

The triggering events for each alert group are listed in Alert Group Trigger Events and Commands, on page 227, and the contents of the alert group messages are listed in Message Contents, on page 234.

You can select one or more alert groups to be received by a destination profile.

Note A Call Home alert is only sent to destination profiles that have subscribed to the alert group containing that Call Home alert. In addition, the alert group must be enabled.

To subscribe a destination profile to one or more alert groups, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**}
4. **profile** *name*
5. **subscribe-to-alert-group all**
6. **subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]
7. **subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]
8. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]
9. **subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]
10. **subscribe-to-alert-group crash**
11. **subscribe-to-alert-group snapshot periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.

Step 3	**alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**}
	Example:
	`Router(cfg-call-home)# alert-group all`
		Enables the specified alert group. Use the keyword **all** to enable all alert groups. By default, all alert groups are enabled.

Step 4	**profile** *name* **Example:** `Router(cfg-call-home)# profile profile1`	Enters the Call Home destination profile configuration submode for the specified destination profile.
Step 5	**subscribe-to-alert-group all** **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group all`	Subscribes to all available alert groups using the lowest severity. You can subscribe to alert groups individually by specific type, as described in Step 6 through Step 11.

	Command or Action	Purpose
		Note This command subscribes to the syslog debug default severity. This causes a large number of syslog messages to generate. You should subscribe to alert groups individually, using appropriate severity levels and patterns when possible.
Step 6	**subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic daily 12:00`	Subscribes this destination profile to the Configuration alert group. The Configuration alert group can be configured for periodic notification, as described in Periodic Notification, on page 201.
Step 7	**subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major`	Subscribes this destination profile to the Environment alert group. The Environment alert group can be configured to filter messages based on severity, as described in Message Severity Threshold, on page 201.
Step 8	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic monthly 1 12:00`	Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification, as described in Periodic Notification, on page 201.
Step 9	**subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major`	Subscribes this destination profile to the Syslog alert group. The Syslog alert group can be configured to filter messages based on severity, as described in Message Severity Threshold, on page 201. You can specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message is sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes (“”). You can specify up to five patterns for each destination profile.
Step 10	**subscribe-to-alert-group crash** **Example:** `Router(cfg-call-home-profile)# [no | default] subscribe-to-alert-group crash`	Subscribes to the Crash alert group in user profile. By default, TAC profile subscribes to the Crash alert group and cannot be unsubscribed.
Step 11	**subscribe-to-alert-group snapshot periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}	Subscribes this destination profile to the Snapshot alert group. The Snapshot alert group can be configured for periodic notification, as described in Periodic Notification, on page 201.

	Command or Action	Purpose
	Example: `Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00`	By default, the Snapshot alert group has no command to run. You can add commands into the alert group, as described in Configuring a Snapshot Command List, on page 202. In doing so, the output of the commands added in the Snapshot alert group will be included in the snapshot message.
Step 12	**exit** **Example:** `Router(cfg-call-home-profile)# exit`	Exits the Call Home destination profile configuration submode.

Periodic Notification

When you subscribe a destination profile to the Configuration, Inventory, or Snapshot alert group, you can choose to receive the alert group messages asynchronously or periodically at a specified time. The sending period can be one of the following:

- Daily—Specifies the time of day to send, using an hour:minute format *hh:mm*, with a 24-hour clock (for example, 14:30).
- Weekly—Specifies the day of the week and time of day in the format *day hh:mm*, where the day of the week is spelled out (for example, Monday).
- Monthly—Specifies the numeric date, from 1 to 31, and the time of day, in the format *date hh:mm*.
- Interval—Specifies the interval at which the periodic message is sent, from 1 to 60 minutes.
- Hourly—Specifies the minute of the hour at which the periodic message is sent, from 0 to 59 minutes.

Note Hourly and by interval periodic notifications are available for the Snapshot alert group only.

Message Severity Threshold

When you subscribe a destination profile to the Environment or Syslog alert group, you can set a threshold for the sending of alert group messages based on the level of severity of the message. Any message with a value lower than the destination profile specified threshold is not sent to the destination.

The severity threshold is configured using the keywords listed in the following table. The severity threshold ranges from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). If no severity threshold is configured for the Syslog or Environment alert groups, the default is debugging (level 0). The Configuration and Inventory alert groups do not allow severity configuration; severity is always set as normal.

Note Call Home severity levels are not the same as system message logging severity levels.

Table 13: Severity and Syslog Level Mapping

Level	Keyword	Syslog Level	Description
9	catastrophic	—	Network-wide catastrophic failure.
8	disaster	—	Significant network impact.
7	fatal	Emergency (0)	System is unusable.
6	critical	Alert (1)	Critical conditions, immediate attention needed.
5	major	Critical (2)	Major conditions.
4	minor	Error (3)	Minor conditions.
3	warning	Warning (4)	Warning conditions.
2	notification	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	normal	Information (6)	Normal event signifying return to normal state.
0	debugging	Debug (7)	Debugging messages.

Configuring a Snapshot Command List

To configure a snapshot command list, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. [**no** | **default**] **alert-group-config snapshot**
4. [**no** | **default**] **add-command** *command string*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.

	Command or Action	Purpose
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.
Step 3	[**no** | **default**] **alert-group-config snapshot** **Example:** `Router(cfg-call-home)# alert-group-config snapshot`	Enters snapshot configuration mode. The **no** or **default** command will remove all snapshot command.
Step 4	[**no** | **default**] **add-command** *command string* **Example:** `Router(cfg-call-home-snapshot)# add-command “show version”`	Adds the command to the Snapshot alert group. The **no** or **default** command removes the corresponding command. • *command string*—IOS command. Maximum length is 128.
Step 5	**exit** **Example:** `Router(cfg-call-home-snapshot)# exit`	Exits and saves the configuration.

Configuring General E-Mail Options

To use the e-mail message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) e-mail server address. You can configure the from and reply-to e-mail addresses, and you can specify up to four backup e-mail servers.

Note the following guidelines when configuring general e-mail options:

- Backup e-mail servers can be defined by repeating the **mail-server** command using different priority numbers.
- The **mail-server priority** number parameter can be configured from 1 to 100. The server with the highest priority (lowest priority number) is tried first.

To configure general e-mail options, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **mail-server** [{*ipv4-address* | *ipv6-address*} | *name*] **priority** *number*
4. **sender from** *email-address*
5. **sender reply-to** *email-address*
6. **source-interface** *interface-name*
7. **vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.
Step 3	**mail-server** [{*ipv4-address* | *ipv6-address*} | *name*] **priority** *number* **Example:** `Router(cfg-call-home)# mail-server stmp.example.com priority 1`	Assigns an e-mail server address and its relative priority among configured e-mail servers. Provide either of these: • The e-mail server's IP address. • The e-mail server's fully qualified domain name (FQDN) of 64 characters or less. Assign a priority number between 1 (highest priority) and 100 (lowest priority).
Step 4	**sender from** *email-address* **Example:** `Router(cfg-call-home)# sender from username@example.com`	(Optional) Assigns the e-mail address that appears in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used.
Step 5	**sender reply-to** *email-address* **Example:** `Router(cfg-call-home)# sender reply-to username@example.com`	(Optional) Assigns the e-mail address that appears in the reply-to field in Call Home e-mail messages.
Step 6	**source-interface** *interface-name* **Example:** `Router(cfg-call-home)# source-interface loopback1`	Assigns the source interface name to send call-home messages. • *interface-name*—Source interface name. Maximum length is 64. **Note** For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface.
Step 7	**vrf** *vrf-name* **Example:** `Router(cfg-call-home)# vrf vpn1`	(Optional) Specifies the VRF instance to send call-home e-mail messages. If no vrf is specified, the global routing table is used. **Note** For HTTP messages, if the source interface is associated with a VRF, use the **ip http client source-interface** *interface-name* command in global configuration mode to specify the VRF instance that will be used for all HTTP clients on the device.

	Command or Action	Purpose

Example

The following example shows the configuration of general e-mail parameters, including a primary and secondary e-mail server:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.168.0.1 priority 2
Router(cfg-call-home)# sender from username@example.com
Router(cfg-call-home)# sender reply-to username@example.com
Router(cfg-call-home)# source-interface loopback1
Router(cfg-call-home)# vrf vpn1
Router(cfg-call-home)# exit
Router(config)#
```

Specifying Rate Limit for Sending Call Home Messages

To specify the rate limit for sending Call Home messages, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **rate-limit** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.
Step 3	**rate-limit** *number* **Example:** `Router(cfg-call-home)# rate-limit 40`	Specifies a limit on the number of messages sent per minute. • *number*—Range is 1 to 60. The default is 20.

Specifying HTTP Proxy Server

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.
Step 3	**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number* **Example:** `Router(cfg-call-home)# http-proxy 1.1.1.1 port 1`	Specifies the proxy server for the HTTP request.

Enabling AAA Authorization to Run IOS Commands for Call Home Messages

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **aaa-authorization**
4. **aaa-authorization** [**username** *username*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.
Step 3	**aaa-authorization** **Example:** `Router(cfg-call-home)# aaa-authorization`	Enables AAA authorization. **Note** By default, AAA authorization is disabled for Call Home.
Step 4	**aaa-authorization** [**username** *username*] **Example:** `Router(cfg-call-home)# aaa-authorization username user`	Specifies the username for authorization. • **username** *username*—Default username is callhome. Maximum length is 64.

Configuring Syslog Throttling

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. [**no**] **syslog-throttling**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.

	Command or Action	Purpose
Step 3	[**no**] **syslog-throttling** **Example:** `Router(cfg-call-home)# syslog-throttling`	Enables or disables call-home syslog message throttling and avoids sending repetitive call-home syslog messages. **Note** By default, syslog message throttling is enabled.

Configuring Call Home Data Privacy

The data-privacy command scrubs data, such as IP addresses, from running configuration files to protect the privacy of customers. Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data. Currently, the **show** command output is not being scrubbed except for configuration messages in the outputs for the **show running-config all** and the**show startup-config data** commands.

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **data-privacy** {**level** {**normal** | **high**} | **hostname**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration submode.

Step 3	**data-privacy** {**level** {**normal** | **high**} | **hostname**}
	Example:
	`Router(cfg-call-home)# data-privacy level high`
		Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal.
		Note Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.
		• **normal—**Scrubs all normal-level commands.
		• **high—**Scrubs all normal-level commands plus the IP domain name and IP address commands.
		• **hostname—**Scrubs all high-level commands plus the hostname command.

	Command or Action	Purpose
		Note Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

Sending Call Home Communications Manually

You can manually send several types of Call Home communications. To send Call Home communications, perform the tasks in this section. This section contains the following subsections:

- Sending a Call Home Test Message Manually, on page 209
- Sending Call Home Alert Group Messages Manually, on page 209
- Submitting Call Home Analysis and Report Requests, on page 210
- Manually Sending Command Output Message for One Command or a Command List, on page 212

Sending a Call Home Test Message Manually

You can use the **call-home test** command to send a user-defined Call Home test message.

To manually send a Call Home test message, perform the following step:

SUMMARY STEPS

1. **call-home test** [“*test-message*”] **profile** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home test** [“*test-message*”] **profile** *name* **Example:** `Router# call-home test profile profile1`	Sends a test message to the specified destination profile. The user-defined test message text is optional but must be enclosed in quotes (“”) if it contains spaces. If no user-defined message is configured, a default message is sent.

Sending Call Home Alert Group Messages Manually

You can use the **call-home send** command to manually send a specific alert group message.

Note the following guidelines when manually sending a Call Home alert group message:

- Only the crash, snapshot, configuration, and inventory alert groups can be sent manually.

- When you manually trigger a crash, snapshot, configuration, or inventory alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the profile's active status, subscription status, or severity setting.
- When you manually trigger a crash, snapshot, configuration, or inventory alert group message and do not specify a destination profile name, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.

To manually trigger Call Home alert group messages, perform the following steps:

SUMMARY STEPS

1. **call-home send alert-group snapshot** [**profile** *name*]
2. **call-home send alert-group crash** [**profile** *name*]
3. **call-home send alert-group configuration** [**profile** *name*]
4. **call-home send alert-group inventory** [**profile** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home send alert-group snapshot** [**profile** *name*] **Example:** `Router# call-home send alert-group snapshot profile profile1`	Sends a snapshot alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 2	**call-home send alert-group crash** [**profile** *name*] **Example:** `Router# call-home send alert-group crash profile profile1`	Sends a crash alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 3	**call-home send alert-group configuration** [**profile** *name*] **Example:** `Router# call-home send alert-group configuration profile profile1`	Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 4	**call-home send alert-group inventory** [**profile** *name*] **Example:** `Router# call-home send alert-group inventory profile profile1`	Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles.

Submitting Call Home Analysis and Report Requests

You can use the **call-home request** command to submit information about your system to Cisco to receive helpful analysis and report information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references.

Note the following guidelines when manually sending Call Home analysis and report requests:

- If a **profile** *name* is specified, the request is sent to the profile. If no profile is specified, the request is sent to the Cisco TAC profile. The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.
- The **ccoid** *user-id* is the registered identifier of the Smart Call Home user. If the *user-id* is specified, the response is sent to the e-mail address of the registered user. If no *user-id* is specified, the response is sent to the contact e-mail address of the device.
- Based on the keyword specifying the type of report requested, the following information is returned:
    - **config-sanity—**Information on best practices as related to the current running configuration.
    - **bugs-list—**Known bugs in the running version and in the currently applied features.
    - **command-reference—**Reference links to all commands in the running configuration.
    - **product-advisory—**Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect the devices in your network.

To submit a request for analysis and report information from the Cisco Output Interpreter tool, perform the following steps:

SUMMARY STEPS

1. **call-home request output-analysis** "*show-command*" [**profile** *name*] [**ccoid** *user-id*]
2. **call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home request output-analysis** "*show-command*" [**profile** *name*] [**ccoid** *user-id*] **Example:** `Router# call-home request output-analysis "show diag" profile TG`	Sends the output of the specified show command for analysis. The show command must be contained in quotes ("").
Step 2	**call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*] **Example:** `Router# call-home request config-sanity profile TG`	Sends the output of a predetermined set of commands such as the **show running-config all**, **show version** or **show module** commands, for analysis. In addition, the **call home request product-advisory** sub-command includes all inventory alert group commands. The keyword specified after **request** specifies the type of report requested.

Example

The following example shows a request for analysis of a user-specified **show** command:

```
Router# call-home request output-analysis "show diag" profile TG
```

Manually Sending Command Output Message for One Command or a Command List

You can use the **call-home send** command to execute an IOS command or a list of IOS commands and send the command output through HTTP or e-mail protocol.

Note the following guidelines when sending the output of a command:

- The specified IOS command or list of IOS commands can be any run command, including commands for all modules. The command must be contained in quotes (“”).
- If the e-mail option is selected using the “email” keyword and an e-mail address is specified, the command output is sent to that address. If neither the e-mail nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).
- If neither the “email” nor the “http” keyword is specified, the service request number is required for both long-text and XML message formats and is provided in the subject line of the e-mail.
- If the HTTP option is specified, the CiscoTac-1 profile destination HTTP or HTTPS URL is used as the destination. The destination e-mail address can be specified so that Smart Call Home can forward the message to the e-mail address. The user must specify either the destination e-mail address or an SR number but they can also specify both.

To execute a command and send the command output, perform the following step:

SUMMARY STEPS

1. **call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*] **Example:** `Router# call-home send “show version;show running-config;show inventory” email support@example.com msg-format xml`	Executes the CLI or CLI list and sends output via e-mail or HTTP. • {*cli command* | *cli list*}—Specifies the IOS command or list of IOS commands (separated by ‘;’). It can be any run command, including commands for all modules. The commands must be contained in quotes (“”). • **email** *email* **msg-format {long-text | xml}—**If the **email** option is selected, the command output will be sent to the specified e-mail address in long-text or XML format with the service request number in the subject. The e-mail address, the service request number, or both must be specified. The service request number is required if the e-mail address is not specified (default is attach@cisco.com for long-text format and callhome@cisco.com for XML format).

	Command or Action	Purpose
		• **http** {**destination-email-address** *email*}—If the **http** option is selected, the command output will be sent to Smart Call Home backend server (URL specified in TAC profile) in XML format. **destination-email-address** *email* can be specified so that the backend server can forward the message to the e-mail address. The e-mail address, the service request number, or both must be specified. • **tac-service-request** *SR#*—Specifies the service request number. The service request number is required if the e-mail address is not specified.

Example

The following example shows how to send the output of a command to a user-specified e-mail address:

```
Router# call-home send “show diag” email support@example.com
```

The following example shows the command output sent in long-text format to attach@cisco.com, with the SR number specified:

```
Router# call-home send “show version; show run” tac-service-request 123456
```

The following example shows the command output sent in XML message format to callhome@cisco.com:

```
Router# call-home send “show version; show run” email callhome@cisco.com msg-format xml
```

The following example shows the command output sent in XML message format to the Cisco TAC backend server, with the SR number specified:

```
Router# call-home send “show version; show run” http tac-service-request 123456
```

The following example shows the command output sent to the Cisco TAC backend server through the HTTP protocol and forwarded to a user-specified email address:

```
Router# call-home send “show version; show run” http destination-email-address user@company.com
```

Configuring Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customers networks.

Information About Diagnostic Signatures

Diagnostic Signatures Overview

Diagnostic signatures (DS) for the Call Home system provides a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

DSs provide the ability to define more types of events and trigger types than the standard Call Home feature supports. The DS subsystem downloads and processes files on a device as well as handles callbacks for diagnostic signature events.

The Diagnostic Signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include CLI commands or scripts to perform required actions. These files are digitally signed by Cisco or a third party to certify their integrity, reliability, and security.

The structure of a DS file can be one of the following formats:

- Metadata-based simple signature that specifies the event type and contains other information that can be used to match the event and perform actions such as collecting information by using the CLI. The signature can also change configurations on the device as a workaround for certain bugs.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats above.

The following basic information is contained in a DS file:

- **ID (unique number)**—Unique key that represents a DS file that can be used to search a DS.
- **Name (ShortDescription)**—Unique description of the DS file that can be used in lists for selection.
- **Description**—Long description about the signature.
- **Revision**—Version number, which increments when the DS content is updated.
- **Event & Action**—Defines the event to be detected and the action to be performed after the event happens.

Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DSs) on a device, you must ensure that the following conditions are met:

- You must assign one or more DSs to the device. For more information on how to assign DSs to devices, see Downloading Diagnostic Signatures, on page 215.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

Note If you configure the trustpool feature, the CA certificate is not required.

Downloading Diagnostic Signatures

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have already configured an email transport method to download files on your device, you must change your assigned profile transport method to HTTPS to download and use DS.

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers.

There are two types of DS update requests to download DS files: regular and forced-download. Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is only started after there is any DS assigned to the device from DS web portal. After the assignment happens, the response to the periodic inventory message from the same device will include a field to notify device to start its periodic DS download/update. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

The DS file is digitally signed, and signature verification is performed on every downloaded DS file to make sure it is from a trusted source.

Diagnostic Signature Workflow

The diagnostic signature feature is enabled by default in Cisco software. The following is the workflow for using diagnostic signatures:

- Find the DS(es) you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
- The device downloads all assigned DS(es) or a specific DS by regular periodic download or by on-demand forced download.
- The device verifies the digital signature of every single DS. If verification passes, the device stores the DS file into a non-removable disk, such as bootflash or hard disk, so that DS files can be read after the device is reloaded. On the router, the DS file is stored in the bootflash:/call home directory.
- The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in device.

- The device monitors the event and executes the actions defined in the DS when the event happens.

Diagnostic Signature Events and Actions

The events and actions sections are the key areas used in diagnostic signatures. The event section defines all event attributes that are used for event detection. The action section lists all actions which should be performed after the event happens, such as collecting show command outputs and sending them to Smart Call Home to parse.

Diagnostic Signature Event Detection

Event detection in a DS is defined in two ways: single event detection and multiple event detection.

Single Event Detection

In single event detection, only one event detector is defined within a DS. The event specification format is one of the following two types:

- DS event specification type: syslog, periodic, configuration, Online Insertion Removal (OIR) immediate, and call home are the supported event types, where "immediate" indicates that this type of DS does not detect any events, its actions are performed once it is downloaded, and the call-home type modifies the current CLI commands defined for existing alert-group.
- The Embedded Event Manager (EEM) specification type: supports any new EEM event detector without having to modify the Cisco software.

  Other than using EEM to detect events, a DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

Multiple Event Detection

Multiple event detection involves defining two or more event detectors, two ore more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors (syslog, OIR, and IPSLA) are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if both syslog and OIR events are triggered simultaneously, or if IPSLA is triggered alone.

Diagnostic Signature Actions

The diagnostic signature (DS) file consists of various actions that must be initiated when an event occurs. The action type indicates the kind of action that will be initiated in response to a certain event.

Variables are elements within a DS that are used to customize the files.

DS actions are categorized into the following four types:

- call-home
- command
- emailto

- script

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message uses "diagnostic-signature" as its message type and DS ID as the message sub-type.

The commands defined for the DS action type initiate CLI commands that can change configuration of the device, collect show command outputs, or run any EXEC command on the device. The DS action type script executes Tcl scripts.

Diagnostic Signature Variables

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. The following are the supported DS variable types:

- System variable: variables assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two system variables: ds_hostname and ds_signature_id.
- Environment variable: values assigned manually by using the **environment** *variable-name variable-value* command in call-home diagnostic-signature configuration mode. Use the **show call-home diagnostic-signature** command to display the name and value of all DS environment variables. If the DS file contains unresolved environment variables, this DS will stay in pending status until the variable gets resolved.
- Prompt variable: values assigned manually by using the **call-home diagnostic-signature install** *ds-id* command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the DS run.
- Syslog event variable: values assigned during a syslog event detection in the DS file. This variable is valid only for syslog event detection.

How to Configure Diagnostic Signatures

- Configuring the Call Home Service for Diagnostic Signatures, on page 217
- Configuring Diagnostic Signatures, on page 219

Configuring the Call Home Service for Diagnostic Signatures

Configure the Call Home Service feature to set attributes such as the contact email address where notifications related with diagnostic signatures (DS) are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from.

You can also create a new user profile, configure correct attributes and assign it as the DS profile. For periodic downloads, the request is sent out just following full inventory message. By changing the inventory periodic configuration, the DS periodic download also gets rescheduled.

Note The predefined CiscoTAC-1 profile is enabled as a DS profile by default and we recommend that you use it. If used, you only need to change the destination transport-method to the **http** setting.

SUMMARY STEPS

1. **configure terminal**
2. **service call-home**
3. **call-home**
4. **contact-email-addr** *email-address*
5. **mail-server** {*ipv4-addr* | *name*} **priority** *number*
6. **profile** *profile-name*
7. **destination transport-method** {**email** | **http**}
8. **destination address** {**email** *address* | **http** *url*}
9. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**service call-home** **Example:** `Router(config)# service call-home`	Enables Call Home service on a device.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters call-home configuration mode for the configuration of Call Home settings.
Step 4	**contact-email-addr** *email-address* **Example:** `Router(cfg-call-home)# contact-email-addr userid@example.com`	(Optional) Assigns an email address to be used for Call Home customer contact.
Step 5	**mail-server** {*ipv4-addr* | *name*} **priority** *number* **Example:** `Router(cfg-call-home)# mail-server 10.1.1.1 priority 4`	(Optional) Configures a Simple Mail Transfer Protocol (SMTP) email server address for Call Home. This command is only used when sending email is part of the actions defined in any DS.

	Command or Action	Purpose
Step 6	**profile** *profile-name* **Example:** `Router(cfg-call-home)# profile user1`	Configures a destination profile for Call Home and enters call-home profile configuration mode.

Step 7	**destination transport-method** {**email** | **http**}
	Example:
	`Router(cfg-call-home-profile)# destination transport-method http`
		Specifies a transport method for a destination profile in the Call Home.
		Note To configure diagnostic signatures, you must use the **http** option.

Step 8	**destination address** {**email** *address* | **http** *url*}
	Example:
	`Router(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
		Configures the address type and location to which call-home messages are sent.
		Note To configure diagnostic signatures, you must use the **http** option.

Step 9	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30`	Configures a destination profile to send messages for the Inventory alert group for Call Home. • This command is used only for the periodic downloading of DS files.
Step 10	**exit** **Example:** `Router(cfg-call-home-profile)# exit`	Exits call-home profile configuration mode and returns to call-home configuration mode.

What to Do Next

Set the profile configured in the previous procedure as the DS profile and configure other DS parameters.

Configuring Diagnostic Signatures

Before You Begin

Configure the Call Home feature to set attributes for the Call Home profile. You can either use the default CiscoTAC-1 profile or use the newly-created user profile.

SUMMARY STEPS

1. **call-home**
2. **diagnostic-signature**
3. **profile** *ds-profile-name*
4. **environment** *ds_env-var-name ds-env-var-value*
5. **end**
6. **call-home diagnostic-signature** [{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*]
7. **show call-home diagnostic-signature** [*ds-id* {**actions** | **events** | **prerequisite** | **prompt** | **variables** | **failure** | **statistics** | **download**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home** **Example:** `Router(config)# call-home`	Enters call-home configuration mode for the configuration of Call Home settings.
Step 2	**diagnostic-signature** **Example:** `Router(cfg-call-home)# diagnostic-signature`	Enters call-home diagnostic signature mode.
Step 3	**profile** *ds-profile-name* **Example:** `Router(cfg-call-home-diag-sign)# profile user1`	Specifies the destination profile on a device that DS uses.
Step 4	**environment** *ds_env-var-name ds-env-var-value* **Example:** `Router(cfg-call-home-diag-sign)# environment ds_env1 envarval`	Sets the environment variable value for DS on a device.

Step 5	**end**
	Example:
	`Router(cfg-call-home-diag-sign)# end`
		Exits call-home diagnostic signature mode and returns to privileged EXEC mode.

Step 6	**call-home diagnostic-signature** [{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*] **Example:** `Router# call-home diagnostic-signature download 6030`	Downloads, installs, and uninstalls diagnostic signature files on a device.
Step 7	**show call-home diagnostic-signature** [*ds-id* {**actions** | **events** | **prerequisite** | **prompt** | **variables** | **failure** | **statistics** | **download**}]	Displays the call-home diagnostic signature information.

	Command or Action	Purpose
	Example: `Router# show call-home diagnostic-signature actions`	

Configuration Examples for Diagnostic Signatures

The following example shows how to enable the periodic downloading request for diagnostic signature (DS) files. This configuration will send download requests to the service call-home server daily at 2:30 p.m. to check for updated DS files. The transport method is set to HTTP.

```
Router> enable
Router# configure terminal
Router(config)# service call-home
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr userid@example.com
Router(cfg-call-home)# mail-server 10.1.1.1 priority 4
Router(cfg-call-home)# profile user-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Router(cfg-call-home-profile)# exit
Router(cfg-call-home)# diagnostic-signature
Router(cfg-call-home-diag-sign)# profile user1
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
Router(cfg-call-home-diag-sign)# end
```

The following is sample output from the **show call-home diagnostic-signature** command for the configuration displayed above:

```
outer# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                         Revision Status     Last Update (GMT+00:00)
-------- ------------------------------- -------- ---------- -------------------
6015     CronInterval                    1.0      registered 2013-01-16 04:49:52
6030     ActCH                           1.0      registered 2013-01-16 06:10:22
6032     MultiEvents                     1.0      registered 2013-01-16 06:10:37
6033     PureTCL                         1.0      registered 2013-01-16 06:11:48
```

Displaying Call Home Configuration Information

You can use variations of the **show call-home** command to display Call Home configuration information.

To display the configured Call Home information, perform the following:

SUMMARY STEPS

1. **show call-home**
2. **show call-home detail**
3. **show call-home alert-group**
4. **show call-home mail-server status**
5. **show call-home profile** {**all** | *name*}
6. **show call-home statistics** [**detail** | **profile** *profile_name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show call-home** **Example:** `Router# show call-home`	Displays the Call Home configuration in summary.
Step 2	**show call-home detail** **Example:** `Router# show call-home detail`	Displays the Call Home configuration in detail.
Step 3	**show call-home alert-group** **Example:** `Router# show call-home alert-group`	Displays the available alert groups and their status.
Step 4	**show call-home mail-server status** **Example:** `Router# show call-home mail-server status`	Checks and displays the availability of the configured e-mail server(s).

Step 5	**show call-home profile** {**all** | *name*}
	Example:
	`Router# show call-home profile all`
		Displays the configuration of the specified destination profile. Use the **all** keyword to display the configuration of all destination profiles.

Step 6	**show call-home statistics** [**detail** | **profile** *profile_name*] **Example:** `Router# show call-home statistics`	Displays the statistics of Call Home events.

Examples

The following examples show the sample output when using different options of the **show call-home** command.

Call Home Information in Summary

```
Router# show call-home
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.168.2.1 Priority: 1
    Mail-server[2]: Address: 223.255.254.254 Priority: 2
    http proxy: 192.168.1.1:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
Router#
```

Call Home Information in Detail

```
Router# show call-home detail
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.168.2.1 Priority: 1
    Mail-server[2]: Address: 223.255.254.254 Priority: 2
    http proxy: 192.168.1.1:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#
```

Available Call Home Alert Groups

```
Router# show call-home alert-group
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info
Router#
```

E-Mail Server Status Information

```
Router# show call-home mail-server status
Please wait. Checking for mail server status ...

    Mail-server[1]: Address: 192.168.2.1 Priority: 1 [Not Available]
    Mail-server[2]: Address: 223.255.254.254 Priority: 2 [Available]
Router#
```

Information for All Destination Profiles

```
Router# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#
```

Information for a User-Defined Destination Profile

```
Router# show call-home profile campus-noc
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Router#
```

Call Home Statistics

```
Router# show call-home statistics
Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   3                    3                    0
    Config      3                    3                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total Failed    0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total Ratelimit
      -dropped  0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Last call-home message sent time: 2011-09-26 23:26:50 GMT-08:00
Router#
```

Default Call Home Settings

The following table lists the default Call Home settings.

Table 14: Default Call Home Settings

Parameters	Default
Call Home feature status	Disabled
User-defined profile status	Active
Predefined Cisco TAC profile status	Inactive
Transport method	E-mail
Message format type	XML
Destination message size for a message sent in long text, short text, or XML format	3,145,728
Alert group status	Enabled
Call Home message severity threshold	Debug
Message rate limit for messages per minute	20
AAA Authorization	Disabled
Call Home syslog message throttling	Enabled
Data privacy level	Normal

Alert Group Trigger Events and Commands

Call Home trigger events are grouped into alert groups, with each alert group assigned commands to execute when an event occurs. The command output is included in the transmitted message. The following table lists the trigger events included in each alert group, including the severity level of each event and the executed commands for the alert group.

Table 15: Call Home Alert Groups, Events, and Actions

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Crash	SYSTEM_ CRASH	–	–	Events related to software crash. The following commands are executed: **show version** **show logging** **show region** **show inventory** **show stack** **crashinfo file** (this command shows the contents of the crashinfo file)
–	TRACEBACK	–	–	Detects software traceback events. The following commands are executed: **show version** **show logging** **show region** **show stack**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Configuration	–	–	–	User-generated request for configuration or configuration change event. The following commands are executed: **show platform** **show inventory** **show running-config all** **show startup-config** **show version**
Environmental	–	–	–	Events related to power, fan, and environment sensing elements such as temperature alarms. The following commands are executed: **show environment** **show inventory** **show platform** **show logging**
–	–	SHUT	0	Environmental Monitor initiated shutdown.
–	–	ENVCRIT	2	Temperature or voltage measurement exceeded critical threshold.
–	–	BLOWER	3	Required number of fan trays is not present.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
–	–	ENVWARN	4	Temperature or voltage measurement exceeded warning threshold.
–	–	RPSFAIL	4	Power supply may have a failed channel.
–	ENVM	PSCHANGE	6	Power supply name change.
–	–	PSLEV	6	Power supply state change.
–	–	PSOK	6	Power supply now appears to be working correctly.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Inventory	–	–	–	

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
				Inventory status should be provided whenever a unit is cold-booted or when FRUs are inserted or removed. This is considered a noncritical event, and the information is used for status and entitlement. Commands executed for all Inventory messages sent in anonymous mode and for Delta Inventory message sent in full registration mode: **show diag all eeprom detail** **show version** **show inventory oid** **show platform** Commands executed for Full Inventory message sent in full registration mode: **show platform** **show diag all eeprom detail** **show version** **show inventory oid** **show bootflash: all** **show data-corruption** **show interfaces** **show file systems** **show memory statistics**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
				show process memory **show process cpu** **show process cpu history** **show license udi** **show license detail** **show buffers**
–	HARDWARE_ REMOVAL	REMCARD	6	Card removed from slot %d, interfaces disabled.
–	HARDWARE_ INSERTION	INSCARD	6	Card inserted in slot %d, interfaces administratively shut down.
Syslog	–	–	–	Event logged to syslog. The following commands are executed: **show inventory** **show logging**
–	SYSLOG	LOG_EMERG	0	System is unusable.
–	SYSLOG	LOG_ALERT	1	Action must be taken immediately.
–	SYSLOG	LOG_CRIT	2	Critical conditions.
–	SYSLOG	LOG_ERR	3	Error conditions.
–	SYSLOG	LOG_WARNING	4	Warning conditions.
–	SYSLOG	LOG_NOTICE	5	Normal but signification condition.
–	SYSLOG	LOG_INFO	6	Informational.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
–	SYSLOG	LOG_DEBUG	7	Debug-level messages.
Test	–	TEST	–	User-generated test message. The following commands are executed: **show platform** **show inventory** **show version**

Message Contents

This section consists of tables which list the content formats of alert group messages.

This section also includes the following subsections that provide sample messages:

- Sample Syslog Alert Notification in Long-Text Format, on page 239
- Sample Syslog Alert Notification in XML Format, on page 240

The following table lists the content fields of a short text message.

Table 16: Format for a Short Text Message

Data Item	Description
Device identification	Configured device name
Date/time stamp	Time stamp of the triggering event
Error isolation message	Plain English description of triggering event
Alarm urgency level	Error level such as that applied to a system message

The following table shows the content fields that are common to all long text and XML messages. The fields specific to a particular alert group message are inserted at a point between the common fields. The insertion point is identified in the table.

Table 17: Common Fields for All Long Text and XML Messages

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD HH:MM:SS GMT+HH:MM*.	CallHome/EventTime
Message name	Name of message. Specific event names are listed in the Alert Group Trigger Events and Commands, on page 227.	For short text message only
Message type	Specifically “Call Home”.	CallHome/Event/Type
Message subtype	Specific type of message: full, delta, test	CallHome/Event/SubType
Message group	Specifically “reactive”. Optional because default is “reactive”.	For long-text message only
Severity level	Severity level of message (see Message Severity Threshold, on page 201).	Body/Block/Severity
Source ID	Product type for routing through the workflow engine. This is typically the product family name.	For long-text message only
Device ID	Unique device identifier (UDI) for end device generating message. This field should be empty if the message is nonspecific to a fabric switch. The format is *type@Sid@serial*. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: CISCO3845@C@12345678	CallHome/CustomerData/ContractData/DeviceId
Customer ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ContractData/CustomerId

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Contract ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ ContractData/CustomerId
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	CallHome/CustomerData/ ContractData/CustomerId
Server ID	If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: CISCO3845@C@12345678	For long text message only.
Message description	Short text describing the error.	CallHome/MessageDescription
Device name	Node that experienced the event. This is the host name of the device.	CallHome/CustomerData/ SystemInfo/NameName
Contact name	Name of person to contact for issues associated with the node experiencing the event.	CallHome/CustomerData/ SystemInfo/Contact
Contact e-mail	E-mail address of person identified as contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactPhoneNumber
Street address	Optional field containing street address for RMA part shipments associated with this unit.	CallHome/CustomerData/ SystemInfo/StreetAddress
Model name	Model name of the router. This is the “specific model as part of a product family name.	CallHome/Device/Cisco_Chassis/Model

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Serial number	Chassis serial number of the unit.	CallHome/Device/Cisco_Chassis/ SerialNumber
Chassis part number	Top assembly number of the chassis.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name="PartNumber"
System object ID	System Object ID that uniquely identifies the system.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name="sysObjectID"
System description	System description for the managed element.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name="sysDescr"

The following table shows the inserted fields specific to a particular alert group message.

Note The following fields may be repeated if multiple commands are executed for this alert group.

Table 18: Inserted Fields Specific to a Particular Alert Group Message

Command output name	Exact name of the issued command.	/aml/Attachments/Attachment/Name
Attachment type	Attachment type. Usually "inline".	/aml/Attachments/Attachment@type
MIME type	Normally "text" or "plain" or encoding type.	/aml/Attachments/Attachment/ Data@encoding
Command output text	Output of command automatically executed (see Alert Group Trigger Events and Commands, on page 227).	/mml/attachments/attachment/atdata

The following table shows the inserted content fields for reactive messages (system failures that require a TAC case) and proactive messages (issues that might result in degraded system performance).

Table 19: Inserted Fields for a Reactive or Proactive Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/ HardwareVersion

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Supervisor module software version	Top-level software version	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= "SoftwareVersion"
Affected FRU name	Name of the affected FRU generating the event message	CallHome/Device/Cisco_Chassis/ Cisco_Card/Model
Affected FRU serial number	Serial number of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/SerialNumber
Affected FRU part number	Part number of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/PartNumber
FRU slot	Slot number of FRU generating the event message	CallHome/Device/Cisco_Chassis/ Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/HardwareVersion
FRU software version	Software version(s) running on affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/SoftwareIdentity/ VersionString

The following table shows the inserted content fields for an inventory message.

Table 20: Inserted Fields for an Inventory Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/ HardwareVersion
Supervisor module software version	Top-level software version	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= "SoftwareVersion"
FRU name	Name of the affected FRU generating the event message	CallHome/Device/Cisco_Chassis/ Cisco_Card/Model
FRU s/n	Serial number of FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/SerialNumber
FRU part number	Part number of FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/PartNumber
FRU slot	Slot number of FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of FRU	CallHome/Device/Cisco_Chassis/ CiscoCard/HardwareVersion

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
FRU software version	Software version(s) running on FRU	CallHome/Device/Cisco_Chassis /Cisco_Card/SoftwareIdentity/ VersionString

Sample Syslog Alert Notification in Long-Text Format

The following example shows a Syslog alert notification in long-text format:

```
TimeStamp : 2014-08-13 21:41 GMT+00:00
Message Name : syslog
Message Type : Call Home
Message Group : reactive
Severity Level : 2
Source ID : ISR 4400
Device ID : ISR4451-X/K9@C@FTX1830AKF9
Customer ID :
Contract ID :
Site ID :
Server ID : ISR4451-X/K9@C@FTX1830AKF9
Event Description : *Aug 13 21:41:35.835: %CLEAR-5-COUNTERS: Clear counter on all interfaces
 by console
System Name : Router
Contact Email : admin@yourdomain.com
Contact Phone :
Street Address :
Affected Chassis : ISR4451-X/K9
Affected Chassis Serial Number : FTX1830AKF9
Affected Chassis Part No : 800-36894-03
Affected Chassis Hardware Version : 1.0
Supervisor Software Version : 15.4(20140812:034256)
Command Output Name : show logging
Attachment Type : command output
MIME Type : text/plain
Command Output Text : show logging
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 71 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 73 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 70 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (4096 bytes):

*Aug 13 21:38:04.994: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
*Aug 13 21:40:55.706: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
*Aug 13 21:41:27.042: %SYS-5-CONFIG_I: Configured from console by console
```

```
Router#
Command Output Name : show inventory
Attachment Type : command output
MIME Type : text/plain
Command Output Text : show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
PID: ISR4451-X/K9      , VID: V03, SN: FTX1830AKF9

NAME: "Power Supply Module 0", DESCR: "450W AC Power Supply for Cisco ISR4450, ISR4350"
PID: PWR-4450-AC       , VID: V01, SN: DCA1822X0G4

NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"
PID: ACS-4450-FANASSY  , VID:    , SN:

NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE   , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module R0", DESCR: "Cisco ISR4451 Route Processor"
PID: ISR4451-X/K9      , VID: V03, SN: FOC18271QLX

NAME: "module F0", DESCR: "Cisco ISR4451 Forwarding Processor"
PID: ISR4451-X/K9      , VID:    , SN:


Router#
```

Sample Syslog Alert Notification in XML Format

The following example shows a Syslog alert notification in XML format:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M4:FTX1830AKF9:53EBDBDA</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2014-08-13 21:42:50 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>ISR 4400</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G5:FTX1830AKF9:53EBDBDA</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
```

```
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2014-08-13 21:42:49 GMT+00:00</ch:EventTime>
<ch:MessageDescription>*Aug 13 21:42:49.406: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>ISR XE Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>admin@yourdomain.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>ISR4451-X/K9@C@FTX1830AKF9</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>admin@yourdomain.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>ISR4451-X/K9</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>FTX1830AKF9</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="800-36894-03" />
<rme:AD name="SoftwareVersion" value="15.4(20140812:034256)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.1707" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, ISR Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version 15.4(20140812:034256)
[v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140812_020034-ios 150]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 12-Aug-14 00:13 by mcpre" />
<rme:AD name="ServiceNumber" value="" />
<rme:AD name="ForwardAddress" value="" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[show logging
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: level debugging, 75 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 77 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.

    Trap logging: level informational, 74 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (4096 bytes):

*Aug 13 21:42:20.187: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
*Aug 13 21:42:23.364: %SYS-5-CONFIG_I: Configured from console by console
Router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
PID: ISR4451-X/K9      , VID: V03, SN: FTX1830AKF9

NAME: "Power Supply Module 0", DESCR: "450W AC Power Supply for Cisco ISR4450, ISR4350"
PID: PWR-4450-AC       , VID: V01, SN: DCA1822X0G4

NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"
PID: ACS-4450-FANASSY  , VID:    , SN:

NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE   , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module R0", DESCR: "Cisco ISR4451 Route Processor"
PID: ISR4451-X/K9      , VID: V03, SN: FOC18271QLX

NAME: "module F0", DESCR: "Cisco ISR4451 Forwarding Processor"
PID: ISR4451-X/K9      , VID:    , SN:

Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Additional References

The following sections provide references related to the Call Home feature.

Related Documents

Document Title	Description
Smart Call Home User Guide	Explains how the Smart Call Home service offers web-based access to important information on select Cisco devices and offers higher network availability, and increased operational efficiency by providing proactive diagnostics and real-time alerts.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

For information about all Cisco IOS commands, use the Command Lookup Tool at https://tools.cisco.com/Support/CLILookup/cltSearchAction.do or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

CHAPTER 16

Managing Cisco Enhanced Services and Network Interface Modules

The router supports Cisco Enhanced Services Modules (SMs) and Cisco Network Interface Modules (NIMs). The modules are inserted into the router using an adapter, or carrier card, into various slots. For more information, see the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

The following sections are included in this chapter:

Information About Cisco Enhanced Services and Network Interface Modules

The router configures, manages, and controls the supported Cisco Enhanced Services Modules (SMs) and Network Interface Modules (NIMs) using the module management facility built in its architecture. This new centralized module management facility provides a common way to control and monitor all the modules in the system regardless of their type and application. All Cisco Enhanced Service and Network Interface Modules supported on your router use standard IP protocols to interact with the host router. Cisco IOS software uses alien data path integration to switch between the modules.

- Enhanced Service Modules, on page 248

Modules Supported

For information about the interfaces and modules supported by the Cisco ISR 4400 series and Cisco ISR 4300 series routers, see http://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/relevant-interfaces-and-modules.html.

Network Interface Modules

The following Network Interface Modules are supported:

- Cisco Fourth-Generation LTE Network Interface Module, on page 246
- Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module, on page 246
- Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module, on page 246
- Cisco SSD/HDD Carrier Card NIM, on page 247
- Upgrading the SSD or HDD Firmware, on page 247
- Error Monitoring, on page 248

Cisco Fourth-Generation LTE Network Interface Module

Cisco 4G LTE NIM addresses the modular 4G LTE cellular connectivity on the Cisco 4000 Series ISRs. This is the first wireless NIM, though it is not the first wireless module in the ISR product line. The closest modular card to Cisco 4G LTE NIM is the Cisco EHWIC 4G LTE, which accepts a single LTE modem. Cisco 4G LTE NIM is feature-compatible with Cisco EHWIC 4G LTE. For more information, see the Cisco Fourth-Generation LTE Network Interface Module Software Configuration Guide.

Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module

The Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module (NIM) integrates the Layer 2 features and provides a 1-Gbps connection to the multigigabit fabric (MGF) for intermodule communication. For more information on configuring the Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch NIM, see http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html.

Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module

The Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module (NIM) is inserted into the NIM slot of the router and provides data and voice support on T1/E1 trunks. To support voice-related and other DSP features, the Cisco PVDM4 (Cisco Packet Voice Digital Signal Processor Module) is also required. See the following documents for more information:

- Installing the Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module

- Configuring the Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module
- Installing the Cisco PVDM4

Cisco SSD/HDD Carrier Card NIM

The router supports a single Cisco SSD and HDD Carrier Card NIM, which must be placed in slot 0 and subslot 1, 2, or 3.

A Cisco SSD/HDD Carrier Card NIM can be one of the following:

- Cisco SSD Carrier Card NIM—Supports one or two Solid-State Drives (SSDs).
- Cisco HDD Carrier Card NIM—Supports one Hard Disk Drive (HDD).

For more information on the hardware characteristics of the SSD/HDD Carrier Card NIM, see the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

For more information on deactivating or reactivating a SSD/HDD Carrier Card NIM, see Deactivating and Reactivating an SSD/HDD Carrier Card NIM, on page 253.

Cisco 1-, 2-, and 4-Port Serial NIM

The Cisco 1-, 2-, and 4-port Serial NIMs are multi-protocol synchronous serial network interface modules (NIMs) supported on the Cisco 4400 Series ISRs. The Cisco 1-, 2-, and 4-port Serial NIMs expand the capabilities of the router to provide connectivity for synchronous interfaces in a wide range of applications including up to 8Mbps data rate for high speed high-level data link control (HDLC). These capabilities can be utilized as Point-to-Point Cisco HDLC WAN interface or frame relay interface. The Cisco 1-, 2-, and 4-port Serial NIMs have their own serial communication controllers (SCC) and they do not rely on the host router for SCCs. For further information on configuring this NIM, see the Configuring the Cisco 1-, 2-, and 4-port Serial Network Interface Modules for the Cisco 4400 Series ISRs document.

Upgrading the SSD or HDD Firmware

You can upgrade the firmware for the SSD or HDD using the **upgrade hw-programmable module filename bootflash:***filename slot/sub-slot* command.

A typical *filename* has the form: *nim_ssd_manufacturer_firmware-version-number.bin*

The firmware file can also be available in other locations other than **bootflash:**

For example, you can provide any one of the following locations in place of **bootflash:***filename*:

- **flash:***filename*
- **harddisk:***filename*
- **usb1:***filename*

Note For a Cisco SSD carrier card NIM or Cisco HDD carrier card NIM, only slot 0 and one of the subslots 1, 2, or 3 must be used.

The following example shows how to upgrade a Micron P400m disk to firmware revision 200 using the **upgrade hw-programmable module filename bootflash:***filename slot/sub-slot* command:

```
Router# upgrade hw-programmable module filename bootflash:nim_ssd_Micr nP400m_E200.bin
Info: Trying to upgrade Module in 0/3 with nim_ssd_MicronP400m_E200.bin
Info: Current NIM-SSD disk config.
Info: Disk1: rev: 0200 model: MicronP400m-MTFDDAK200MAN
Info: Disk2: rev: 0200 model: MicronP400m-MTFDDAK200MAN
/dev/sde:
fwdownload: xfer_mode=3 min=1 max=255 size=512
...........................................................................................
 Done.
/dev/sdf:
fwdownload: xfer_mode=3 min=1 max=255 size=512
...........................................................................................
 Done.
Info: Performing post upgrade check ......
Info: Upgrade to Firmware version E200 on disk1 successful.
Info: Upgrade to Firmware version E200 on disk2 successful.
Info: Current NIM-SSD disk config.
Info: Disk1: rev: E200 model: MicronP400m
```

Error Monitoring

The drives in the Cisco SDD/HDD Carrier Card NIM are monitored for SMART errors. If a SMART error occurs, a Cisco IOS error message is displayed, as shown in the following example:

```
%IOSXE-5-PLATFORM:logger: INFO:/dev/sde:SMART error present:please do
'more bootflash:/tracelogs/smart_errors.log'.
```

You can find additional information in the error log at: bootflash:/tracelogs/smart_errors.log

Enhanced Service Modules

The following service modules are supported on the router:

- Cisco SM-1 T3/E3 Service Module, on page 248
- Cisco UCS E-Series Server, on page 249
- Cisco SM-X Layer 2/3 EtherSwitch Service Module, on page 249
- Cisco 6-Port GE SFP Service Module, on page 249

Cisco SM-1 T3/E3 Service Module

For more information, see the Cisco SM-1T3/E3 Enhanced Service Module Configuration Guide.

Cisco UCS E-Series Server

For more information, see the documentation listed in the Cisco UCS E-Series Server Roadmap.

Cisco SM-X Layer 2/3 EtherSwitch Service Module

This module provides the following features:

- Integration of Layer 2 and Layer 3 switching features and the ability of the router to use the Cisco SM-X Layer 2/3 ESM (16-port and 24-port) as an independent Layer 3 switch.
- 1 Gbps connection to the multigigabit fabric (MGF) for intermodule communication without burdening the CPU of the router.
- Up to 30 watts of power per port with the robust Power over Ethernet Plus (PoE+) feature along with IEEE 802.3AE Media Access Control Security (MACSec) port-based, hop-to-hop, encryption, and Cisco TrustSec.

For more information, see the following documents:

- Cisco SM-X Layer 2/3 EtherSwitch Service Module Configuration Guide for Cisco 4451-X ISR
- Connecting Cisco SM-X Layer 2/3 EtherSwitch Service Module to the Network

Cisco 6-Port GE SFP Service Module

The Cisco 6-port GE SFP service module is a Gigabit Ethernet module that can be inserted into the router's SM slot to provide Gigabit Ethernet features on routable external interfaces. For more information about configuring this service module, see the Software Configuration Guide for the Cisco 6-port GE SFP Service Module.

Cisco 4-port GE SFP and 1-port 10 GE SFP Service Module

The Cisco 4-port GE SFP and 1-port 10 GE SFP Service Module (SM-X-4x1GE-1x10GE) is software-configurable high-speed connectivity routing port service module for the Cisco ISR 4400 Series routers. This service module provides increased density of Ethernet interfaces on the Cisco ISR 4400 Series routers. For further information on configuring this service module, see: the Software Configuration Guide for the Cisco 6-port GE SFP Service Module and Cisco 4-port GE SFP and 1-port 10 GE SFP Service Module

Cisco 1GE-CU-SFP and 2GE-CU-SFP Network Interface Modules

The Cisco 1GE-CU-SFP and 2GE-CU-SFP Network Interface Modules (NIMs) are software-configurable high-speed connectivity routing port network interface modules for the Cisco 4000 and Cisco ISR 4300 Series Integrated Services Routers (ISR). These network interface modules provide increased density of Ethernet interfaces on the Cisco 4000 ISR. For further information on configuring this NIM, see the Configuring the Cisco 1GE-CU-SFP and 2GE-CU-SFP Network Interface Modules in Cisco 4000 Series Integrated Services Routers.

Implementing SMs and NIMs on Your Router

Downloading the Module Firmware

Module firmware must be loaded to the router to be able to use a service module. For more information, see Installing a Firmware Subpackage, on page 91.

The modules connect to the RP via the internal eth0 interface to download the firmware. Initially, the module gets an IP address for itself via BOOTP. The BOOTP also provides the address of the TFTP server used to download the image. After the image is loaded and the module is booted, the module provides an IP address for the running image via DHCP.

Installing SMs and NIMs

For more information, see "Installing and Removing NIMs and SMs" in the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

Accessing Your Module Through a Console Connection or Telnet

Before you can access the modules, you must connect to the host router through the router console or through Telnet. After you are connected to the router, you must configure an IP address on the Gigabit Ethernet interface connected to your module. Open a session to your module using the **hw-module session** command in privileged EXEC mode on the router.

To establish a connection to the module, connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router.

Use the following configuration examples to establish a connection:

- The following example shows how to open a session from the router using the **hw-module session** command:

```
Router# hw-module session slot/card
Router# hw-module session 0/1 endpoint 0

Establishing session connect to subslot 0/1
```

- The following example shows how to exit a session from the router, by pressing **Ctrl-A** followed by **Ctrl-Q** on your keyboard:

```
type ^a^q
picocom v1.4

port is        : /dev/ttyDASH2
flowcontrol    : none
```

```
baudrate is     : 9600
parity is       : none
databits are    : 8
escape is       : C-a
noinit is       : no
noreset is      : no
nolock is       : yes
send_cmd is     : ascii_xfr -s -v -l10
receive_cmd is  : rz -vv
```

Online Insertion and Removal

The router supports online insertion and removal (OIR) of Cisco Enhanced Services Modules and Cisco Network Interface Modules. You can perform the following tasks using the OIR function:

- Preparing for Online Removal of a Module, on page 251
- Deactivating a Module, on page 251
- Deactivating Modules and Interfaces in Different Command Modes, on page 252
- Deactivating and Reactivating an SSD/HDD Carrier Card NIM, on page 253
- Reactivating a Module, on page 254
- Verifying the Deactivation and Activation of a Module, on page 254

Preparing for Online Removal of a Module

The router supports the OIR of a module, independent of removing another module installed in your router. This means that an active module can remain installed in your router, while you remove another module from one of the subslots. If you are not planning to immediately replace a module, ensure that you install a blank filler plate in the subslot.

Deactivating a Module

A module can be removed from the router without first being deactivated. However, we recommend that you perform a graceful deactivation (or graceful power down) of the module before removing it. To perform a graceful deactivation, use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode.

Note When you are preparing for an OIR of a module, it is not necessary to independently shut down each of the interfaces before deactivating the module. The **hw-module subslot** *slot/subslot* **stop** command in EXEC mode automatically stops traffic on the interfaces and deactivates them along with the module in preparation for OIR. Similarly, you do not have to independently restart any of the interfaces on a module after OIR.

The following example shows how to use the **show facility-alarm status** command to verify if any critical alarm is generated when a module is removed from the system:

```
Router# show facility-alarm status
System Totals  Critical: 5  Major: 1  Minor: 0

Source                  Severity      Description [Index]
------                  --------      -------------------
```

```
Power Supply Bay 1      CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/1    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/2    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3    CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/0    INFO          Transceiver Missing [0]
xcvr container 0/0/1    INFO          Transceiver Missing [0]
xcvr container 0/0/2    INFO          Transceiver Missing [0]
xcvr container 0/0/3    INFO          Transceiver Missing [0]
V: 1.0v PCH R0/18       MAJOR         Volt Above Normal [3]
```

Note A critical alarm (Active Card Removed OIR Alarm) is generated even if a module is removed after performing graceful deactivation.

Deactivating Modules and Interfaces in Different Command Modes

You can deactivate a module and its interfaces using the **hw-module subslot** command in one of the following modes:

- If you choose to deactivate your module and its interfaces by executing the **hw-module subslot** *slot/subslot* **shutdown unpowered** command in global configuration mode, you are able to change the configuration in such a way that no matter how many times the router is rebooted, the module does not boot. This command is useful when you need to shut down a module located in a remote location and ensure that it does not boot automatically when the router is rebooted.
- If you choose to use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode, you cause the module to gracefully shut down. The module is rebooted when the **hw-module subslot** *slot/subslot* **start** command is executed.

To deactivate a module and all of its interfaces before removing the module, use one of the following commands in global configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**hw-module subslot** *slot*/*subslot* **shutdown unpowered** **Example:** Router# **hw-module subslot 0/2 shutdown unpowered**	Deactivates the module located in the specified slot and subslot of the router, where: • *slot*—Specifies the chassis slot number where the module is installed. • *subslot*—Specifies the subslot number of the chassis where the module is installed. • **shutdown**—Shuts down the specified module. • **unpowered**—Removes all interfaces on the module from the running configuration and the module is powered off.
Step 2	**hw-module subslot** *slot*/*subslot* [**reload** | **stop** | **start**] **Example:** Router# **hw-module subslot 0/2 stop**	Deactivates the module in the specified slot and subslot, where: • *slot*—Specifies the chassis slot number where the module is installed. • *subslot*—Specifies the subslot number of the chassis where the module is installed.

	Command or Action	Purpose
		• **reload—**Stops and restarts the specified module. • **stop—**Removes all interfaces from the module and the module is powered off. • **start—**Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots and the entire module initialization sequence is executed in the IOSd and Input/Output Module daemon (IOMd) processes.

Deactivating and Reactivating an SSD/HDD Carrier Card NIM

The following restrictions apply:

- Deactivating or reactivating an SSD/HDD Carrier Card NIM without an SSD or HDD disk is not supported.
- Only a single (SSD or HDD) Carrier Card NIM can be plugged into a bay. If you plug an additional (SSD or HDD) Carrier Card NIM into another bay, the module powers down and kernel, log, or error messages are displayed on the Cisco IOS console. In rare cases, the file system may get corrupted on the additional drive.

Caution Deactivation of an SSD/HDD Carrier Card NIM may cause loss of data.

To deactivate an SSD/HDD Carrier Card NIM, perform the following steps:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**virtual-service** *name* **Example:** `Router(config)# virtual-service my-kwaas-instance`	Identifies the kWAAS service (by name), supported on your router, in preparation for the router to be shut down by the **no activate** command. We recommend that you use this command before reseating or replacing an SSD or HDD.
Step 2	**no activate** **Example:** `Router(config-virt-serv)# no activate`	Shuts down the kWAAS instance on your router. kWAAS services remain installed. The service will have to be reactivated after the HDD/SSD NIM (module) is restarted.

Step 3	**hw-module subslot** *slot*/*subslot* [**reload** | **stop** | **start**]
	Example:
	`Router# hw-module subslot 0/2 stop`
	`Proceed with stop of module? [confirm]`
		Deactivates or reactivates the module in the specified slot and subslot.
		• *slot*—The chassis slot number where the module is installed.
		• *subslot*—The subslot number of the chassis where the module is installed.

	Command or Action	Purpose

	`Router#`
	`*Mar 6 15:13:23.997:`
	`%SPA_OIR-6-OFFLINECARD: SPA (NIM-SSD)`
	`offline in subslot 0/2`
	`...`
		• **reload—**Deactivates and reactivates (stops and restarts) the specified module.
		• **stop—**Removes all interfaces from the module and the module is powered off.
		• **start—**Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots and the entire module initialization sequence is executed in the IOSd and IOMd processes.

Step 4	Wait for the EN (Enable) LED to turn off, and then remove the SSD/HDD Carrier Card NIM.	

Reactivating a Module

If, after deactivating a module using the **hw-module subslot** *slot/subslot* **stop** command, you want to reactivate it without performing an OIR, use one of the following commands (in privileged EXEC mode):

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

Verifying the Deactivation and Activation of a Module

When you deactivate a module, the corresponding interfaces are also deactivated. This means that these interfaces will no longer appear in the output of the **show interface** command.

1 To verify the deactivation of a module, enter the **show hw-module subslot all oir** command in privileged EXEC configuration mode.

Observe the "Operational Status" field associated with the module that you want to verify. In the following example, the module located in subslot 1 of the router is administratively down.

```
Router# show hw-module subslot all oir

Module         Model              Operational Status

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

subslot 0/0    ISR4451-4X1GE      ok
subslot 1/0    SM-X-T1/E1         ok
```

2 To verify activation and proper operation of a module, enter the **show hw-module subslot all oir** command and observe "ok" in the **Operational Status** field as shown in the following example:

```
Router# show hw-module subslot all oir

Module         Model               Operational Status

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

subslot 0/1    NIM-8MFT-T1/E1      ok
subslot 1/0    SM-X T1/E1          ok
```

```
Router# show platform hardware backplaneswitch-manager R0 status
slot  bay   port   enable   link status   speed(Mbps)   duplex   autoneg   pause_tx
pause_rx   mtu
---------------------------------------------------------------------------------------
0      0     CP     True      Up           1000          Full    ENABLED    ENABLED
ENABLED   10240
1      0     GE1    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
1      0     GE0    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
2      0     GE1    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
2      0     GE0    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
0      1     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      1     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      2     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      2     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      3     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      3     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      4     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      4     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      0     FFP    True       Up         10000          Full    ENABLED    DISABLED
DISABLED  10240
slot  bay   port            mac    vid   modid     flags - Layer 2
------------------------------------------------------------------------------
0      0    FFP  2c54.2dd2.661b   2351       1             0x20
0      0    FFP  2c54.2dd2.661b   2352       1             0x20
0      0     CP  2c54.2dd2.661e   2351       0             0xC60
0      0     CP  2c54.2dd2.661e   2352       0             0x20
1      0    GE0  58bf.ea3a.00f6   2350       0             0x460
0      0    FFP  2c54.2dd2.661b   2350       1             0x20
1      0    GE0  58bf.ea3a.00f6   2352       0             0x20
0      0     CP  2c54.2dd2.661e   2350       0             0x20
1      0    GE0  58bf.ea3a.00f6   2351       0             0xC60
Port block masks: rows=from port, columns=to port, u=unknown unicast, m=unknown multicast,
 b=broadcast, A=all

           CP    FFP  1/0/1  1/0/0  2/0/1  2/0/0  0/1/1  0/1/0  0/2/1  0/2/0  0/3/1
0/3/0  0/4/1 0/4/0 drops
---------------------------------------------------------------------------------------
CP          -      A      um      um      um      um      um      um      um      um      um
um      um      um      1
FFP         A      -      -       -       -       -       -       -       -       -
 -      -      -      0
1/0/1      um     umb     -      umb     umb     umb     umb     umb     umb     umb     umb
umb     umb     umb     0
1/0/0      um     umb    umb      -      umb     umb     umb     umb     umb     umb     umb
umb     umb     umb     6
2/0/1      um     umb    umb     umb      -      umb     umb     umb     umb     umb     umb
umb     umb     umb     0
2/0/0      um     umb    umb     umb     umb      -      umb     umb     umb     umb     umb
umb     umb     umb     6
0/1/1      um     umb    umb     umb     umb     umb      -      umb     umb     umb     umb
umb     umb     umb     0
0/1/0      um     umb    umb     umb     umb     umb     umb      -      umb     umb     umb
umb     umb     umb     0
0/2/1      um     umb    umb     umb     umb     umb     umb     umb      -      umb     umb
umb     umb     umb     0
0/2/0      um     umb    umb     umb     umb     umb     umb     umb     umb      -      umb
umb     umb     umb     0
0/3/1      um     umb    umb     umb     umb     umb     umb     umb     umb     umb      -
umb     umb     umb     0
0/3/0      um     umb    umb     umb     umb     umb     umb     umb     umb     umb     umb
```

```
-     umb    umb     0
0/4/1      um    umb   umb    umb    umb    umb    umb    umb    umb    umb    umb
umb     -     umb     0
0/4/0      um    umb   umb    umb    umb    umb    umb    umb    umb    umb    umb
umb    umb     -      0

Port VLAN membership: [untagged vlan] U=untagged T=tagged <VLAN range begin>-<VLAN range
 end>

    CP [2352] U:0001-0001 T:0002-2351 U:2352-2352 T:2353-4095
   FFP [2352] T:0001-4095
 1/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 1/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 2/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 2/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/1/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/1/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/2/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/2/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/3/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/3/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/4/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/4/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
```

show platform hardware backplaneswitch-manager rp active ffp statistics: Example

```
Router# show platform hardware backplaneswitch-manager rp active ffp statistics
Broadcom 10G port(e.g: FFP) status:
                          Rx pkts         Rx Bytes          Tx Pkts         Tx Bytes
-----------------------------------------------------------------------------------------
All                             0                0                0                0
  =64                           0                                 0
  65~127                        0                                 0
  128~255                       0                                 0
  256~511                       0                                 0
  512~1023                      0                                 0
  1024~1518                     0                                 0
  1519~2047                     0                                 0
  2048~4095                     0                                 0
  4096~9216                     0                                 0
  9217~16383                    0                                 0
  Max                           0                                 0
Good                            0                                 0
  CoS 0                                                           0                0
  CoS 1                                                           0                0
  CoS 2                                                           0                0
  CoS 3                                                           0                0
  CoS 4                                                           0                0
  CoS 5                                                           0                0
  CoS 6                                                           0                0
  CoS 7                                                           0                0
  Unicast                       0                                 0
  Multicast                     0                                 0
  Broadcast                     0                                 0
  Control                       0
Errored
  FCS                           0                                 0
  Undersize                     0
  Ether len                     0
  Fragment                      0                                 0
  Jabber                        0
  MTU ck, good                  0
  MTU ck, bad                   0
  Tx underflow                                                                     0
  err symbol                    0
  frame err                     0
  junk                          0
Drops
  CoS 0                                                           0                0
  CoS 1                                                           0                0
  CoS 2                                                           0                0
  CoS 3                                                           0                0
  CoS 4                                                           0                0
  CoS 5                                                           0                0
  CoS 6                                                           0                0
  CoS 7                                                           0                0
  STP                           0
  backpress                     0
  congest                       0                0
  purge/cell                    0
  no destination                0
Pause PFC                       0                                 0
  CoS 0                         0
  CoS 1                         0
  CoS 2                         0
  CoS 3                         0
  CoS 4                         0
  CoS 5                         0
  CoS 6                         0
  CoS 7                         0
```

Managing Modules and Interfaces

The router supports various modules. For a list of supported modules, see Modules Supported, on page 246. The module management process involves bringing up the modules so that their resources can be utilized. This process consists of tasks such as module detection, authentication, configuration by clients, status reporting, and recovery. For detailed information about module configuration, see the module documentation referred to in the Documentation Roadmap for the Cisco 4000 Series Integrated Services Routers.

For a list of small-form-factor pluggable (SFP) modules supported on your router, see the "Installing and Upgrading Internal Modules and FRUs" section in the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

The following sections provide additional information on managing the modules and interfaces:

- Managing Module Interfaces, on page 257
- Managing Modules and Interfaces Using Backplane Switch, on page 257

Managing Module Interfaces

After a module is in service, you can control and monitor its module interface. Interface management includes configuring clients with **shut** or **no shut** commands and reporting on the state of the interface and the interface-level statistics.

Monitor the module status and other statistical information using the **show** commands listed in Monitoring and Troubleshooting Modules and Interfaces, on page 260.

Managing Modules and Interfaces Using Backplane Switch

- Backplane Ethernet Switch, on page 258
- Viewing Module and Interface Card Status on a Router, on page 258
- Viewing Backplane Switch Statistics, on page 259
- Viewing Backplane Switch Port Statistics, on page 259
- Viewing Slot Assignments, on page 260

Backplane Ethernet Switch

The backplane Ethernet switch on your router provides connectivity to Enhanced Service Modules and Network Interface Modules (NIMs). The backplane Ethernet switch facilitates all packet transfers between the host router and its pluggable modules.

The backplane Ethernet switch act as a manager for the host router and controls the module and exchanges logical flow-control information with the module to ensure accurate feedback to the router features. See Managing Modules and Interfaces, on page 257 for more information. The backplane Ethernet switch also facilitates control plane traffic flow from the host router to the modules. The backplane switch manages modules and interface cards and is used to communicate with the modules. Module drivers integrate with the backplane switch to configure packet flow and control traffic buffering.

You are not required to perform any configuration tasks on the backplane switch; all the configurations are performed from the module, which may or may not lead to changes on the backplane switch. For more information on installing an adapter, see the Hardware Installation Guide for the Cisco ISR 4000 Series Integrated Services Routers.

Note Layer 2 protocols, such as the IEEE 802.1D Spanning Tree Protocol (STP), are not supported in the backplane Ethernet switch.

Viewing Module and Interface Card Status on a Router

You can view the module and interface card details using the **show platform** command in privileged EXEC mode.

The following example shows the sample output for the **show platform** command:

```
Router# show platform
Chassis type: ISR4451/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451/K9          ok                    15:57:33
 0/0      ISR4451-4X1GE       ok                    15:55:24
 0/3      NIM-SSD             ok                    15:55:24
1         ISR4451/K9          ok                    15:57:33
 1/0      SM-1T3/E3           ok                    15:55:24
2         ISR4451/K9          ok                    15:57:33
 2/0      SM-1T3/E3           ok                    15:55:24
R0        ISR4451/K9          ok, active            15:57:33
F0        ISR4451-FP          ok, active            15:57:33
P0        Unknown             ps, fail              never
P1        XXX-XXXX-XX         ok                    15:56:58
P2        ACS-4450-ASSY       ok                    15:56:58

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         12090323            15.3(01r)S            [ciscouser-ISRRO...
1         12090323            15.3(01r)S            [ciscouser-ISRRO...
2         12090323            15.3(01r)S            [ciscouser-ISRRO...
R0        12090323            15.3(01r)S            [ciscouser-ISRRO...
F0        12090323            15.3(01r)S            [ciscouser-ISRRO...
```

Viewing Backplane Switch Statistics

Statistics reports for each slot show incoming and outgoing packets or bytes. You can use the information to check traffic flow on the various ports of the backplane switch. The following example shows a sample output for the **show platform hardware backplaneswitch-manager rp active summary** command:

```
Router# show platform hardware backplaneswitch-manager rp active summary
slot     bay       port         InBytes          InPkts         OutBytes          OutPkts
----------------------------------------------------------------------------------------
   0       0         CP            6242         9361008             6241          403209
   1       0        GE1               0               0                0               0
   1       0        GE0            6306          407477             6241         9360934
   2       0        GE1               0               0                0               0
   2       0        GE0               0               0                0               0
   0       1        GE1               0               0                0               0
   0       1        GE0               0               0                0               0
   0       2        GE1               0               0                0               0
   0       2        GE0               0               0                0               0
   0       3        GE1               0               0                0               0
   0       3        GE0               0               0                0               0
   0       4        GE1               0               0                0               0
   0       4        GE0               0               0                0               0
   0       0        FFP               0               0                0               0
   0       0        FFP               0               0                0               0
```

Viewing Backplane Switch Port Statistics

You can view statistical information related to the port connected to the backplane switch using the **show platform hardware backplaneswitch-manager rp active subslot GEO statistics** command. The following example displays statistical information related to the backplane switch and ports connected to it:

```
Router# show platform hardware backplaneswitch-manager rp active subslot 1/0 GE0 statistics
Broadcom 1G port(e.g: NIM, ESM, CP) status:
                          Rx pkts         Rx Bytes          Tx Pkts         Tx Bytes
-----------------------------------------------------------------------------------------
All                          6306           407477             6241          9360934
  =64                        6237                                72
  65~127                       66                                 3
  128~255                       0                                 0
  256~511                       1                                 3
  512~1023                      2                                 0
  1024~1518                     0                              6163
  1519~2047                     0                                 0
  2048~4095                     0                                 0
  4096~9216                     0                                 0
Good                         6306                              6241
  CoS 0                                                        6171          9356426
  CoS 1                                                           0                0
  CoS 2                                                           0                0
  CoS 3                                                           0                0
  CoS 4                                                           0                0
  CoS 5                                                           0                0
  CoS 6                                                          70             4508
  CoS 7                                                           0                0
  Unicast                    6294                              6241
  Multicast                     6                                 0
  Broadcast                     6                                 0
  Control                       0                                 0
  VLAN                          0                                 0
Errored
  FCS                           0                                 0
  Runts                         0                0
  Undersize                     0
  Ether len                     0
  Fragment                      0                                 0
  Jabber                        0                                 0
  MTU                           0
Drops
  CoS 0                                                           0                0
  CoS 1                                                           0                0
  CoS 2                                                           0                0
  CoS 3                                                           0                0
  CoS 4                                                           0                0
  CoS 5                                                           0                0
  CoS 6                                                           0                0
  CoS 7                                                           0                0
  STP                           0
  backpress                     0
  congest                       0                0
  purge/cell                    0
  no destination               65
Pause                           0                                 0
```

Viewing Slot Assignments

Use the **show inventory** command in privileged EXEC mode to view the slot assignments, as shown in the following example:

```
Router# show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
PID: ISR4451/K9        , VID: V01, SN: FGL163910CM

NAME: "Power Supply Module 1", DESCR: "Cisco 4451-X ISR 450W AC Power Supply"
PID: XXX-XXXX-XX       , VID: XXX, SN: DCA1623X05N

NAME: "Fan Tray", DESCR: "Cisco 4451-X ISR Fan tray"
PID: ACS-4450-FANASSY  , VID:    , SN:

NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451/K9        , VID:    , SN:

NAME: "NIM subslot 0/1", DESCR: " NIM-1MFT-T1/E1 - T1/E1 Serial Module"
PID:  NIM-1MFT-T1/E1  , VID: V01, SN: FOC16254E71

NAME: "subslot 0/1 db module 0", DESCR: "PVDM4-TDM-280 Voice DSP Module"
PID: PVDM4-TDM-280     , VID: V01, SN: FOC16290GRT

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE   , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9        , VID:    , SN:

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9        , VID:    , SN:

NAME: "SM subslot 2/0", DESCR: "SM-X-1T3/E3 - Clear T3/E3 Serial Module"
PID: SM-1T3/E3         , VID: V01, SN: FOC15495HSE

NAME: "module R0", DESCR: "Cisco ISR 4451-X Route Processor"
PID: ISR4451/K9        , VID: V01, SN: FOC163679GH

NAME: "module F0", DESCR: "Cisco ISR4451-X Forwarding Processor"
PID: ISR4451/K9        , VID:    , SN:
```

Monitoring and Troubleshooting Modules and Interfaces

Use the following commands in global configuration mode to monitor and troubleshoot the modules and interfaces:

- **show platform**
- **show platform software backplaneswitch-manager RP [active [detail]]**
- **show platform hardware backplaneswitch-manager RPactive CP statistics**
- **show platform hardware backplaneswitch-manager RP active summary**
- **show platform hardware backplaneswitch-manager [R0 [status] | RP]**
- **show diag all eeprom details**

show platform

```
Router# show platform
Chassis type: ISR4451/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451/K9          ok                    15:57:33
 0/0      ISR4451-4X1GE       ok                    15:55:24
1         ISR4451/K9          ok                    15:57:33
 1/0      SM-1T3/E3           ok                    15:55:24
2         ISR4451/K9          ok                    15:57:33
 2/0      SM-1T3/E3           ok                    15:55:24
R0        ISR4451/K9          ok, active            15:57:33
F0        ISR4451-FP          ok, active            15:57:33
P0        Unknown             ps, fail              never
P1        XXX-XXXX-XX         ok                    15:56:58
P2        ACS-4450-FANASSY    ok                    15:56:58

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         12090323            15.3(01r)S            [ciscouser-ISRRO...
1         12090323            15.3(01r)S            [ciscouser-ISRRO...
2         12090323            15.3(01r)S            [ciscouser-ISRRO...
R0        12090323            15.3(01r)S            [ciscouser-ISRRO...
F0        12090323            15.3(01r)S            [ciscouser-ISRRO...
```

Table 21: show platform Field Descriptions

Field	Description
Slot	Slot number
Type	Type of module
State	Status of module
Insert Time	Time since the module has been up and running

show platform software backplaneswitch-manager RP [active [detail]]

```
Router# show platform software backplaneswitch-manager RP active detail
BSM Software Display

 module port   port type  alien type    traf type
-------------------------------------------------
       0/1/0       NGIO       TRUNK         NGIO
       0/1/1       NGIO       TRUNK         NGIO
       0/2/0       NGIO       TRUNK         NGIO
       0/2/1       NGIO       TRUNK         NGIO
       0/3/0        NGIO       TRUNK         NGIO
       0/3/1       ALIEN       TRUNK         NGIO
       0/4/0        NGIO       TRUNK         NGIO
       0/4/1        NGIO       TRUNK         NGIO
       1/0/0        NGIO       TRUNK         NGIO
       1/0/1        NGIO       TRUNK         NGIO
       2/0/0        NGIO       TRUNK         NGIO
       2/0/1        NGIO       TRUNK         NGIO
```

show platform hardware backplaneswitch-manager RPactive CP statistics

```
Router# show platform hardware backplaneswitch-manager RP active CP statistics
Broadcom 1G port(e.g:  NIM, NGSM, CP) status:
                          Rx pkts         Rx Bytes          Tx Pkts         Tx Bytes
-----------------------------------------------------------------------------------------
All                          6242          9361008             6241           403209
  =64                          72                              6178
  65~127                        4                                60
  128~255                       0                                 0
  256~511                       3                                 1
  512~1023                      0                                 2
  1024~1518                  6163                                 0
  1519~2047                     0                                 0
  2048~4095                     0                                 0
  4096~9216                     0                                 0
Good                         6242                              6241
  CoS 0                                                           0                0
  CoS 1                                                           0                0
  CoS 2                                                           0                0
  CoS 3                                                        6241           403209
  CoS 4                                                           0                0
  CoS 5                                                           0                0
  CoS 6                                                           0                0
  CoS 7                                                           0                0
  Unicast                    6241                              6235
  Multicast                     1                                 0
  Broadcast                     0                                 6
  Control                       0                                 0
  VLAN                          0                                 0
Errored
  FCS                           0                                 0
  Runts                         0                0
  Undersize                     0
  Ether len                     0
  Fragment                      0                                 0
  Jabber                        0                                 0
  MTU                           0
Drops
  CoS 0                                                           0                0
  CoS 1                                                           0                0
  CoS 2                                                           0                0
  CoS 3                                                           0                0
  CoS 4                                                           0                0
  CoS 5                                                           0                0
  CoS 6                                                           0                0
  CoS 7                                                           0                0
  STP                           0
  backpress                     0
  congest                       0                0
  purge/cell                    0
  no destination                1
Pause                           0                                 0
```

show platform hardware backplaneswitch-manager RP active summary

```
Router# show platform hardware backplaneswitch-manager RP active summary
  slot     bay          port           InBytes            InPkts         OutBytes  OutPkts

------------------------------------------------------------------------------------------
     0       0            CP               242                 0                 0   0
     1       0           GE1                 0                 0                 0   0
     1       0           GE0                 0                 0                 0   0
     2       0           GE1                 0                 0                 0   0
     2       0           GE0                 0                 0                 0   0
     0       1           GE1                 0                 0                 0   0
     0       1           GE0                 0                 0                 0   0
     0       2           GE1                 0                 0                 0   0
     0       2           GE0                 0                 0                 0   0
     0       3           GE1                 0                 0                 0   0
     0       3           GE0                 0                 0                 0   0
     0       4           GE1                 0                 0                 0   0
     0       4           GE0                 0                 0                 0   0
     0       0           FFP                 0                 0                 0   0
```

show platform hardware backplaneswitch-manager [R0 [status] | RP]

```
Router# show platform hardware backplaneswitch-manager R0 status
slot  bay   port   enable   link status   speed(Mbps)   duplex   autoneg   pause_tx
pause_rx   mtu
------------------------------------------------------------------------------------------
0      0     CP     True      Up           1000          Full    ENABLED    ENABLED
ENABLED   10240
1      0     GE1    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
1      0     GE0    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
2      0     GE1    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
2      0     GE0    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
0      1     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      1     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      2     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      2     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      3     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      3     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      4     GE1    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      4     GE0    True     Down          1000          Full    DISABLED   ENABLED
ENABLED   10240
0      0     FFP    True       Up         10000          Full    ENABLED    DISABLED
DISABLED  10240
slot  bay   port            mac    vid   modid     flags - Layer 2
------------------------------------------------------------------------------
0      0    FFP  2c54.2dd2.661b   2351       1             0x20
0      0    FFP  2c54.2dd2.661b   2352       1             0x20
0      0     CP  2c54.2dd2.661e   2351       0             0xC60
0      0     CP  2c54.2dd2.661e   2352       0             0x20
1      0    GE0  58bf.ea3a.00f6   2350       0             0x460
0      0    FFP  2c54.2dd2.661b   2350       1             0x20
1      0    GE0  58bf.ea3a.00f6   2352       0             0x20
0      0     CP  2c54.2dd2.661e   2350       0             0x20
1      0    GE0  58bf.ea3a.00f6   2351       0             0xC60
Port block masks: rows=from port, columns=to port, u=unknown unicast, m=unknown multicast,
 b=broadcast, A=all

           CP    FFP  1/0/1  1/0/0  2/0/1  2/0/0  0/1/1  0/1/0  0/2/1  0/2/0  0/3/1  0/3/0
  0/4/1 0/4/0 drops
------------------------------------------------------------------------------------------
CP           -     A     um     um     um     um     um     um     um     um     um     um
    um      um     1
FFP         A      -     -      -      -      -      -      -      -      -      -      -
     -      -      0
1/0/1       um    umb    -     umb    umb    umb    umb    umb    umb    umb    umb    umb
   umb    umb      0
1/0/0       um    umb   umb     -     umb    umb    umb    umb    umb    umb    umb    umb
   umb    umb      6
```

```
2/0/1      um    umb   umb    umb     -     umb    umb    umb    umb    umb    umb    umb
   umb    umb     0
2/0/0      um    umb   umb    umb    umb     -     umb    umb    umb    umb    umb    umb
   umb    umb     6
0/1/1      um    umb   umb    umb    umb    umb     -     umb    umb    umb    umb    umb
   umb    umb     0
0/1/0      um    umb   umb    umb    umb    umb    umb      -    umb    umb    umb    umb
   umb    umb     0
0/2/1      um    umb   umb    umb    umb    umb    umb    umb     -     umb    umb    umb
   umb    umb     0
0/2/0      um    umb   umb    umb    umb    umb    umb    umb    umb    -      umb    umb
   umb    umb     0
0/3/1      um    umb   umb    umb    umb    umb    umb    umb    umb    umb     -     umb
   umb    umb     0
0/3/0      um    umb   umb    umb    umb    umb    umb    umb    umb    umb    umb     -
   umb    umb     0
0/4/1      um    umb   umb    umb    umb    umb    umb    umb    umb    umb    umb    umb
    -     umb     0
0/4/0      um    umb   umb    umb    umb    umb    umb    umb    umb    umb    umb    umb
   umb     -      0

Port VLAN membership: [untagged vlan] U=untagged T=tagged <VLAN range begin>-<VLAN range
end>

    CP [2352] U:0001-0001 T:0002-2351 U:2352-2352 T:2353-4095
   FFP [2352] T:0001-4095
 1/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 1/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 2/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 2/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/1/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/1/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/2/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/2/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/3/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/3/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/4/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/4/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
```

show diag all eeprom details

```
Router# show diag all eeprom details
MIDPLANE EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        PCB Serial Number        : FOC15520B7L
        Controller Type          : 1902
        Hardware Revision        : 1.0
        PCB Part Number          : 73-13854-02
        Top Assy. Part Number    : 800-36894-01
        Board Revision           : 05
        Deviation Number         : 123968
        Fab Version              : 02
        Product Identifier (PID) : ISR4451/K9
        Version Identifier (VID) : V01
        CLEI Code                : TDBTDBTDBT
        Processor type           : D0
        Chassis Serial Number    : FGL1601129D
        Chassis MAC Address      : 30f7.0d53.c7e0
        MAC Address block size   : 144
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Asset ID                 : P1B-R2C
Power/Fan Module P0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1509
        Unknown Field (type 00DF): 1.85.1.236.1
        Deviation Number         : 0
        PCB Serial Number        : DCA1547X037
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Version Identifier (VID) : XXX
        Product Identifier (PID) : XXX-XXXX-XX
        CLEI Code                : 0000000000
        Environment Monitor Data : 41 01 C2 42 00 05 F8 00
                                   50 01 F4 1B 58 03 E8 1F
                                   4A 05 DC 21 34 07 D0 21
                                   FC 09 C4 22 60 0B B8 22
                                   92 0D AC 22 D8 0F A0 22
                                   F8 11 94 22 F6 13 88 23
                                   3C 15 7C 23 28 17 70 23
                                   00 19 64 22 D8 1B 58 22
                                   C4 1D 4C 22 BA 1F 40 22
                                   A6 21 34 22 9C 23 28 22
                                   92 25 1C 22 88 27 10 22
                                   60
        Board Revision           : P0
Power/Fan Module P1 EEPROM data is not initialized

Power/Fan Module P2 EEPROM data is not initialized

Slot R0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        PCB Serial Number        : FOC15520B7L
        Controller Type          : 1902
        Hardware Revision        : 1.0
        PCB Part Number          : 73-13854-02
        Top Assy. Part Number    : 800-36894-01
        Board Revision           : 05
        Deviation Number         : 123968
        Fab Version              : 02
        Product Identifier (PID) : ISR4451/K9
        Version Identifier (VID) : V01
        CLEI Code                : TDBTDBTDBT
        Processor type           : D0
        Chassis Serial Number    : FGL1601129D
        Chassis MAC Address      : 30f7.0d53.c7e0
        MAC Address block size   : 144
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Asset ID                 : P1B-R2C
        Asset ID                 :
Slot F0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 3567
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-FP
        Version Identifier (VID) : V00
        PCB Serial Number        : FP123456789
        Asset ID                 :
Slot 0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
Slot 1 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
Slot 2 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
SPA EEPROM data for subslot 0/0:

        EEPROM version           : 5
        Compatible Type          : 0xFF
        Controller Type          : 1902
        Hardware Revision        : 2.2
        Boot Timeout             : 400 msecs
        PCB Serial Number        : JAB092709EL
        PCB Part Number          : 73-8700-01
        PCB Revision             : A0
        Fab Version              : 01
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 78409
        Product Identifier (PID) : ISR4451-4X1GE
        Version Identifier (VID) : V01
        Top Assy. Part Number    : 68-2236-01
        Top Assy. Revision       : A0
        IDPROM Format Revision   : 36
        System Clock Frequency   : 00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00
        CLEI Code                : CNUIAHSAAA
        Base MAC Address         : 00 00 00 00 00 00
        MAC Address block size   : 0
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
              Calibration values :
        Power Consumption        : 13100 mWatts (Maximum)
        Environment Monitor Data : 03 30 0C E4 46 32 09 C4
                                   46 32 05 DC 46 32 05 DC
                                   46 32 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 FE 02 F9 6E
        Processor Label          : 00 00 00 00 00 00 00
        Platform features        : 00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00
        Asset ID                 :
        Asset Alias              :
SPA EEPROM data for subslot 0/1 is not available

SPA EEPROM data for subslot 0/2 is not available

SPA EEPROM data for subslot 0/3 is not available
SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 1/0 is not available

SPA EEPROM data for subslot 1/1 is not available

SPA EEPROM data for subslot 1/2 is not available

SPA EEPROM data for subslot 1/3 is not available

SPA EEPROM data for subslot 1/4 is not available

SPA EEPROM data for subslot 2/0 is not available

SPA EEPROM data for subslot 2/1 is not available

SPA EEPROM data for subslot 2/2 is not available

SPA EEPROM data for subslot 2/3 is not available

SPA EEPROM data for subslot 2/4 is not available
```

Configuration Examples

This section provides examples of deactivating and activating modules.

Deactivating a Module Configuration: Example

You can deactivate a module to perform OIR of that module. The following example shows how to deactivate a module (and its interfaces) and remove power to the module. In this example, the module is installed in subslot 0 of the router.

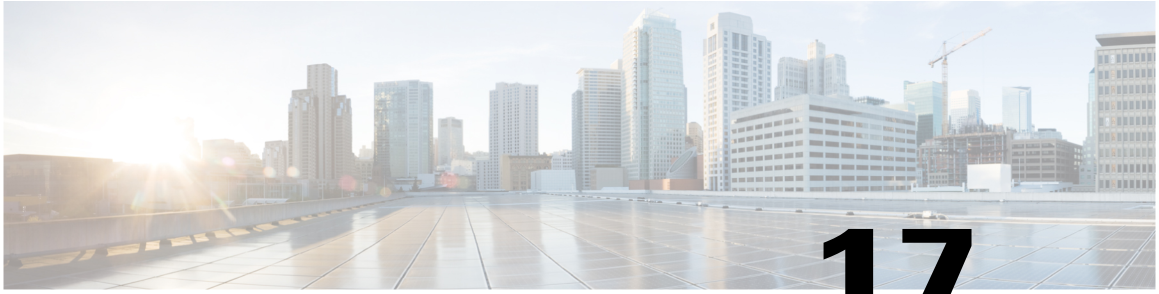
```
Router(config)# hw-module slot 1 subslot 1/0 shutdown unpowered
```

Activating a Module Configuration: Example

You can activate a module if you have previously deactivated it. If you have not deactivated a module and its interfaces during OIR, then the module is automatically reactivated upon reactivation of the router.

The following example shows how to activate a module. In this example, the module is installed in subslot 0, located in slot 1 of the router:

```
Router(config)# hw-module slot 1 subslot 1/0 start
```



CHAPTER 17

SFP Auto-Detect and Auto-Failover

Cisco 4000 Series Integrated Services Routers (ISRs) provide a Front Panel Gigabit Ethernet (FPGE) port that supports copper and fiber concurrent connections. Media can be configured for failover redundancy when the network goes down. This feature is supported only on Cisco ISR platforms.

This chapter includes this section:

Cellular IPv6 Address

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:

- 2001:CDBA:0000:0000:0000:0000:3257:9652
- 2001:CDBA::3257:9652 (zeros can be omitted)

IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). The table below lists compressed IPv6 address formats.

An IPv6 address prefix, in the format ipv6-prefix/prefix-length, can be used to represent bit-wise contiguous blocks of the entire address space. The ipv6-prefix must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:cdba::3257:9652 /64 is a valid IPv6 prefix.

IPv6 Unicast Routing

An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.

Cisco 4000 Series ISR supports the following address types:

- Global Address, on page 270

Link-Lock Address

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. An link-local address is automatically configured on the cellular interface when an IPv6 address is enabled.

After the data call is established, the link-local address on the celluar interface is updated with the host generated link-local address that consists of the link-local prefix FF80::/10 (1111 1110 10) and the auto-generated interface identifier from the USB hardware address. The figure below shows the structure of a link-local address.

Global Address

A global IPv6 unicast address is defined by a global routing prefix, a subnet ID, and an interface ID. The routing prefix is obtained from the PGW. The Interface Identifier is automatically generated from the USB hardware address using the interface identifier in the modified EUI-64 format. The USB hardware address changes after the router reloads.

Configuring Cellular IPv6 Address

To configure the cellular IPv6 address, perform these steps:

SUMMARY STEPS

1. **configure terminal**
2. **interface Cellular** {**type**|**number**}
3. ip address negotiated
4. encapsulation slip
5. load-interval*seonds*
6. dialer in-band
7. dialer idle-timeout *seonds*
8. dialer string string
9. dialer-groupgroup-number
10. no peer default ip address
11. ipv6 address autoconfig
12. async mode interactive
13. routing dynamic
14. **dialer-listdialer-groupprotocolprotocol-name** {**permit** |deny|**list** |*access-list-number* | *access-group* }
15. **ipv6 route** *ipv6-prefix/prefix-length 128*
16. **End**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 2	**interface Cellular** {**type**|**number**}
	Example:
	`Router(config)# interface cellular 0/1/0`
		Specifies the cellular interface.

Step 3	ip address negotiated **Example:** `Router(config-if)# ipv6 address negotiated`	Specifies that the IP address for a particular interface is dynamically obtained.
Step 4	encapsulation slip **Example:** `Router(config-if)# encapsulation slip`	Specifies Serial Line Internet Protocol (SLIP) encapsulation for an interface configured for dial-on-demand routing (DDR).
Step 5	load-interval*seonds* **Example:** `Router(config-if)# load-interval 30`	Specifies the length of time for which data is used to compute load statistics.
Step 6	dialer in-band **Example:** `Router(config-if)# dialer in-band`	Enables DDR and configures the specified serial interface to use in-band dialing.
Step 7	dialer idle-timeout *seonds* **Example:** `Router(config-if)# dialer idle-timeout 0`	Specifies the dialer idle timeout period.
Step 8	dialer string string **Example:** `Router(config-if)# dialer string lte`	Specifies the number or string to dial.
Step 9	dialer-groupgroup-number **Example:** `Router(config-if)# dialer-group 1`	Specifies the number of the dialer access group to which the specific interface belongs.
Step 10	no peer default ip address **Example:** `Router(config-if)# no peer default ip address`	Removes the default address from your configuration.

	Command or Action	Purpose
Step 11	ipv6 address autoconfig **Example:** `Router(config-if)# ipv6 address autoconfig`	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.
Step 12	async mode interactive **Example:** `Router(config-if)# async mode interactive`	Please provide the inputs?
Step 13	routing dynamic **Example:** `Router(config-if)#routing dynamic`	Enables the router to pass routing updates to other routers through an interface.

Step 14	**dialer-listdialer-groupprotocolprotocol-name** {**permit** |deny|**list** |*access-list-number* | *access-group* }
	Example:
	`Router(config)# dialer-list 1 protocol ipv6 permit`
		Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.

Step 15	**ipv6 route** *ipv6-prefix/prefix-length 128* **Example:** `Router(config)#ipv6 route 2001:1234:1234::3/128 Cellular0/1/0`	
Step 16	**End** **Example:** `Router(config-if)#end`	Exits to global configuration mode.

Examples

The following example shows the Cellular IPv6 configuration .

```
Router(config)# interface Cellular0/0/0
ip address negotiated
encapsulation slip
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic
!
interface Cellular0/1/0
ip address negotiated
encapsulation slip
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
```

```
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic

dialer-list 1 protocol ipv6 permit
ipv6 route 2001:1234:1234::/64 Cellular0/1/0
ipv6 route 2001:4321:4321::5/128 Cellular0/1/1
```

CHAPTER 18

Cellular IPv6 Address

This chapter provides an overview of the IPv6 addresses and describes how to configure Cellular IPv6 address on Cisco 4000 series ISRs.

This chapter includes this section:

CHAPTER 19

Configuring Voice Functionality

This chapter provides information about configuring voice functionality on the Cisco 4000 Series Integrated Services Routers (ISRs).

This chapter includes these sections:

Call Waiting

With the Call Waiting feature, you can receive a second call while you are on the phone with another call. When you receive a second call, you hear a call-waiting tone (a tone with a 300 ms duration). Caller ID appears on phones that support caller ID. You can use hookflash to answer a waiting call and place the previously active call on hold. By using hookflash, you can toggle between the active and a call that is on hold. If the Call Waiting feature is disabled, and you hang up the current call, the second call will hear a busy tone. For more information on Call Waiting, see the http://www.cisco.com/c/en/us/td/docs/ios/voice/sip/configuration/guide/15_0/sip_15_0_book/sip_cg-hookflash.html#wp999028

Call Transfers

Call transfers are when active calls are put on hold while a second call is established between two users. After you establish the second call and terminate the active call, the call on hold will hear a ringback. The Call Transfer feature supports all three types of call transfers—blind, semi-attended, and attended. For more information on Call Transfers, see the http://www.cisco.com/c/en/us/td/docs/ios/voice/sip/configuration/guide/15_0/sip_15_0_book/sip_cg-hookflash.html#wp999084

E1 R2 Signaling Configuration

To configure the E1 R2, perform these steps:

Before You Begin

Before you attempt this configuration, ensure that you meet these prerequisites:

- R2 signaling applies only to E1 controllers.
- In order to run R2 signaling on Cisco 4000 Series ISRs, this hardware is required:
- NIM-MFT-1T1/E1 or NIM-2MFT-T1/E1 or NIM-4MFT-T1/E1or NIM-8MFT-T1/E1 or NIM-1CE1T1-PRI or NIM-2CE1T1-PRI or NIM-8CE1T1-PRI
- Define the command ds0-group on the E1 controllers of Cisco 4000 Series ISRs.
- Cisco IOS XE software release 15.5 (2)

SUMMARY STEPS

1. Set up the controller E1 that connects to the private automatic branch exchange (PBX) or switch.
2. For E1 framing, choose either **CRC** or **non-CRC**
3. For E1 linecoding, choose either **HDB3** or **AMI**.
4. For the E1 clock source, choose either internal or line. Note that different PBXs have different requirements on the clock source.
5. Configure line signaling.
6. Configure interregister signaling.
7. Customize the configuration with the cas-custom command.

DETAILED STEPS

Step 1 Set up the controller E1 that connects to the private automatic branch exchange (PBX) or switch.
Ensure that the framing and linecoding of the E1 are properly set.

Step 2 For E1 framing, choose either **CRC** or **non-CRC**

Step 3 For E1 linecoding, choose either **HDB3** or **AMI**.

Step 4 For the E1 clock source, choose either internal or line. Note that different PBXs have different requirements on the clock source.

Step 5 Configure line signaling.

```
(config)# controller E1 0/2/0

 (config-controller)#ds0-group 1 timeslots 1 type ?
...
r2-analog        R2 ITU Q411
r2-digital       R2 ITU Q421
r2-pulse         R2 ITU Supplement 7
...
```

Step 6 Configure interregister signaling.

```
(config)# controller E1 0/2/0
 eefje(config)# controller E1 0/2/0
 eefje(config-controller)#ds0-group 1 timeslots 1 type r2-digital ?
dtmf               DTMF tone signaling
r2-compelled       R2 Compelled Register Signaling
r2-non-compelled   R2 Non Compelled Register Signaling
r2-semi-compelled  R2 Semi Compelled Register Signaling

...
```

The Cisco implementation of R2 signaling has Dialed Number Identification Service (DNIS) support enabled by default. If you enable the Automatic Number Identification (ANI) option, the collection of DNIS information is still performed. Specification of the ANI option does not disable DNIS collection. DNIS is the number that is called and ANI is the number of the caller. For example, if you configure a router called A to call a router called B, then the DNIS number is assigned to router B and the ANI number is assigned to router A. ANI is similar to caller ID.

Step 7 Customize the configuration with the cas-custom command.

```
(config)# controller E1 0/2/0

(config-controller)#ds0-group 1 timeslots 1 type r2-digital r2-compelled ani
cas-custom 1
  country brazil
  metering
  answer-signal group-b 1

voice-port 0/2/0:1
!
dial-peer voice 200 pots
destination-pattern 43200
direct-inward-dial
port 0/2/0:1

dial-peer voice 3925 voip
destination-pattern 39...
session target ipv4:1.5.25.41
...
```

R2 Configurations

The configurations have been modified in order to show only the information that this document discusses.

Configured for R2 Digital Non-Compelled

```
hostname eefje
!
controller E1 0
 clock source line primary
 dso-group 1 timeslots 1-15 type r2-digital r2-non-compelled
 cas-custom 1

!--- For more information on these commands
!--- refer to
ds0-group
 and
cas-custom.

!
```

```
voice-port 0:1
 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
cptone
.

!
dial-peer voice 123 pots
 destination-pattern 123
 direct-inward-dial
 port 0:1
 prefix 123
!
dial-peer voice 567 voip
 destination-pattern 567
 session target ipv4:2.0.0.2
```

Configured for R2 Digital Semi-Compelled

```
hostname eefje
!
controller E1 0
 clock source line primary
 ds0-group 1 timeslots 1-15 type r2-digital r2-semi-compelled
 cas-custom 1

!--- For more information on these commands
!---  refer to
ds0-group
 and
cas-custom
.

!
voice-port 0:1
 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
cptone
.

dial-peer voice 123 pots
 destination-pattern 123
 direct-inward-dial
 port 0:1
 prefix 123
!
dial-peer voice 567 voip
 destination-pattern 567
 session target ipv4:2.0.0.2
```

Configured for R2 Digital Compelled ANI

```
hostname eefje
! controller E1 0 clock source line primary ds0-group
1 timeslots 1-15 type r2-digital r2-compelled ani cas-custom 1

!--- For more information on these commands
!---  refer to
ds0-group
 and
cas-custom
.

voice-port 0:1 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
cptone
.

dial-peer voice 123 pots destination-pattern 123 direct-inward-dial port
```

```
0:1 prefix 123
!
dial-peer voice 567 voip destination-pattern 567 session
target ipv4:2.0.0.2
```

Sample Debug Command Output

This example shows the output for the **debug vpm sig** command.

```
(config-controller)#debug vpm sig
Syslog logging: enabled
(0 messages dropped, 9 messages rate-limited, 1 flushes, 0 overruns,
 xml disabled, filtering disabled)No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging:  level debugging, 163274 messages logged, xml disabled,filtering disabled

Exception Logging: size (4096 bytes)    Count and timestamp logging messages: disabled
Persistent logging: disabledNo active filter modules.
Trap logging: level informational, 172 message lines logged
Logging Source-Interface:
VRF Name:Log Buffer (4096 bytes):0): DSX (E1 0/2/0:0): STATE: R2_IN_COLLECT_DNIS R2 Got
Event 1
*Jan 29 21:32:22.258:r2_reg_generate_digits(0/2/0:1(1)): Tx digit '1'
*Jan 29 21:32:22.369: htsp_digit_ready(0/2/0:1(1)): Rx digit='#'
*Jan 29 21:32:22.369: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0):STATE: R2_IN_COLLECT_DNIS
R2 Got Event R2_TONE_OFF
*Jan 29 21:32:22.369: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '#'
*Jan 29 21:32:22.569: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:25.258: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0):STATE: R2_IN_COLLECT_DNIS
R2 Got Event R2_TONE_TIMER
*Jan 29 21:32:25.258: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '3#'
*Jan 29 21:32:25.520: htsp_digit_ready_up(0/2/0:1(1)): Rx digit='1'
*Jan 29 21:32:25.520: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_CATEGORY R2
Got Event 1
*Jan 29 21:32:25.520: Enter r2_comp_category
*Jan 29 21:32:25.520: R2 Event : 1
*Jan 29 21:32:25.520:  ####### collect_call_enable = 0
*Jan 29 21:32:25.520: ######## Not Sending B7 ##################
*Jan 29 21:32:25.520: r2_reg_event_proc(0/2/0:1(1)) ADDR_INFO_COLLECTED (DNIS=39001,
ANI=39700)
*Jan 29 21:32:25.520: r2_reg_process_event: [0/2/0:1(1), R2_REG_COLLECTING,
E_R2_REG_ADDR_COLLECTED(89)]
*Jan 29 21:32:25.520: r2_reg_ic_addr_collected(0/2/0:1(1))htsp_switch_ind
*Jan 29 21:32:25.521: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_SETUP_ACK]
*Jan 29 21:32:25.521: r2_q421_ic_setup_ack(0/2/0:1(1)) E_HTSP_SETUP_ACK
*Jan 29 21:32:25.521: r2_reg_switch(0/2/0:1(1))
*Jan 29 21:32:25.521: r2_reg_process_event: [0/2/0:1(1), R2_REG_WAIT_FOR_SWITCH,
E_R2_REG_SWITCH(96)]
*Jan 29 21:32:25.521: r2_reg_ic_switched(0/2/0:1(1))
*Jan 29 21:32:25.522: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_PROCEEDING]
*Jan 29 21:32:25.530:htsp_call_bridged invoked
*Jan 29 21:32:25.530: r2_reg_event_proc(0/2/0:1(1)) ALERTING RECEIVED
*Jan 29 21:32:25.530: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_WAIT_REMOTE_ALERT
 R2 Got Event R2_ALERTING
*Jan 29 21:32:25.530:rx R2_ALERTING in r2_comp_wait_remote_alert
*Jan 29 21:32:25.530: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '1'htsp_alert_notify
*Jan 29 21:32:25.531:r2_reg_event_proc(0/2/0:1(1)) ALERTING RECEIVED
*Jan 29 21:32:25.531: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_COMPLETE R2
Got Event R2_ALERTING
*Jan 29 21:32:25.540: htsp_dsp_message: RESP_SIG_STATUS: state=0x0 timestamp=0
systime=80352360
*Jan 29 21:32:25.540:htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER, E_DSP_SIG_0000]
*Jan 29 21:32:25.651: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:25.751: htsp_digit_ready(0/2/0:1(1)): Rx digit='#'
*Jan 29 21:32:25.751: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_COMPLETE R2
Got Event R2_TONE_OFF
*Jan 29 21:32:25.751: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '#'
*Jan 29 21:32:25.961: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:26.752: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_WAIT_GUARD R2
```

```
 Got Event R2_TONE_TIMER
*Jan 29 21:32:26.752: R2_IN_CONNECT: call end dial
*Jan 29 21:32:26.752: r2_reg_end_dial(0/2/0:1(1))htsp_call_service_msghtsp_call_service_msg
 not EFXS (11)htsp_call_service_msghtsp_call_service_msg not EFXS (11)
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:51.909: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER, E_HTSP_CONNECT]
*Jan 29 21:32:51.909: r2_q421_ic_answer(0/2/0:1(1)) E_HTSP_CONNECT
*Jan 29 21:32:51.909: r2_q421_ic_answer(0/2/0:1(1)) Tx ANSWER seizure: delay 0 ms,elapsed
32419 msvnm_dsp_set_sig_state:[R2 Q.421 0/2/0:1(1)] set signal state = 0x4
*Jan 29 21:32:51.910: r2_reg_channel_connected(0/2/0:1(1))
*Jan 29 21:32:51.910: r2_reg_process_event: [0/2/0:1(1), R2_REG_WAIT_FOR_CONNECT,
E_R2_REG_CONNECT(90)]
*Jan 29 21:32:51.910: r2_reg_connect(0/2/0:1(1))htsp_call_service_msghtsp_call_service_msg
 not EFXS (11)
```

This example shows the output for the **debug vtsp all** command.

```
(config-controller)#debug vtsp all
Log Buffer (4096 bytes)::S_R2_DIALING_COMP, event:E_VTSP_DIGIT_END]
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_digit:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_TSP_R2_DIAL]
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_dial:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dial_nopush:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/ds_do_dial:     Digits To
Dial=#
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_dial_done_cb:
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_VTSP_DSM_DIALING_COMPLETE]
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_dialing_done:
*Jan 29 21:56:34.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_TSP_R2_END_DIAL]
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/ds_end_dial:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_digit_pop:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_digit_pop:     Digit
Reporting=FALSE
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_alert_dial_complete:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
Stop Time=80497275
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
Stop Time=80497275
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.692: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
    Feature ID=0, Feature Status=1
*Jan 29 21:56:34.692: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.692:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
    Feature ID=0, Feature Status=1
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.693:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
    Feature ID=0, Feature Status=1
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.693:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
```

```
 Name
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 Number 39701
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 oct3a  30
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_ALERTING, event:E_CC_CONNECT]
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_alert_connect:    Progress
 Indication=2
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_ring_noan_timer_stop:
   Timer Stop Time=80499620
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_CONNECT, event:E_CC_SERVICE_MSG]
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
Stop Time=80499620
*Jan 29 21:56:58.144: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_fpi_event_cb:
Event=E_DSMP_FPI_ENABLE_TDM_RTCP
```

Feature Group D Configuration

To configure the Feature Group D signaling, perform these steps:

Before You Begin

The Feature Group D signaling is supported on Cisco 4000 Series Integrated Services Routers from IOS XE release 15.5 (2). Feature Group D service is a trunk side connection that enables telephone customers to choose their long distance network and use the same number of digits irrespective of carrier they use. Routers interface with interexchange carriers using Feature Group D to support voice traffic in the carrier environment.

Before you attempt this configuration, ensure that you meet these prerequisites:

- The platform must be using Digital T1/E1 Packet Voice Trunk Network Modules.
- The Digital T1/E1 Packet Voice Trunk Network Module can have one or two slots for voice/WAN Interface Network Modules (NIMs); NIM supports one to eight ports. Only the dual-mode (voice/WAN) multiple trunk cards are supported in the digital E1 packet voice trunk network module, not older VICs.
- Drop-and-Insert capability is supported only between two ports on the same multiple card.

SUMMARY STEPS

1. **configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. **voice-card slot/subslot**
3. **controller T1/E1 slot/subslot/port**
4. **framing** {*sf* | *esf* }
5. **linecode** {*b8zs* | *ami*}
6. **ds0-group** *ds0-group-no***timeslots** *timeslot-list type*{*e&m-fgd* | *fgd-eana*}
7. **no shutdown**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]}
	Example:
	`Router(config)# configure terminal`
		Enters global configuration mode.

Step 2	**voice-card slot/subslot** **Example:** `Router(config)# voice-card slot/subslot`	Enters voice card interface configuration mode and specify the slot location by using a value from 0 to 5, depending upon your router.
Step 3	**controller T1/E1 slot/subslot/port** **Example:** `Router(config)# controller T1 slot/subslot/port`	Enters controller configuration mode for the T1 controller at the specified slot/port location. Valid values for slot and port are 0 and 1.

Step 4	**framing** {*sf* | *esf* }
	Example:
	`Router(config)# framing {sf | esf}`
		Sets the framing according to your service provider's instructions. Choose Extended Superframe (ESF) format or Superframe (SF) format.

Step 5	**linecode** {*b8zs* | *ami*}	Sets the line encoding according to your service provider's instructions. Bipolar-8 zero substitution (B8ZS) encodes a sequence of eight zeros in a unique binary sequence to detect line coding violations. Alternate mark inversion (AMI) represents zeros using a 01 during each bit cell, and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independent of the data stream.
Step 6	**ds0-group** *ds0-group-no***timeslots** *timeslot-list type*{*e&m-fgd* | *fgd-eana*}	Defines the T1 channels for use by compressed voice calls as well as the signaling method the router uses to connect to the PBX or CO. ds0-group-no is a value from 0 to 23 that identifies the DS0 group. Note The ds0-group command automatically creates a logical voice port that is numbered as follows: slot/port:ds0-group-no. Although only one voice port is created, applicable calls are routed to any channel in the group. timeslot-list is a single number, numbers separated by commas, or a pair of numbers separated by a hyphen to indicate a range of timeslots. For T1, allowable values are from 1 to 24. To map individual DS0 timeslots, define additional groups. The system maps additional voice ports for each defined group. The signaling method selection for type depends on the connection that you are making. The e&m-fgd setting allows E&M interface connections for PBX trunk lines (tie lines) and telephone equipment to use feature

	Command or Action	Purpose
		group D switched-access service. The fgd-eana setting supports the exchange access North American (EANA) signaling.
Step 7	**no shutdown**	Activates the controller.
Step 8	**exit**	Exits controller configuration mode. Skip the next step if you are not setting up Drop and Insert .

Media and Signaling Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature implements voice security features that include signaling authentication along with media and signaling encryption on MGCP gateways. For more information on Media and Signaling Authentication and Encryption Feature, see the http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/mgcp/configuration/15-mt/vm-15-mt-book/vm-gw-med-sig.html

Multicast Music-on-Hold

The Music-on-Hold (MOH) feature enables you to subscribe to a music streaming service when you are using a Cisco IOS MGCP voice gateway. Music streams from an MOH server to the voice interfaces of on-net and off-net callers that have been placed on hold. Cisco Communications Manager supports the capability to place callers on hold with music supplied from a streaming multicast MOH server.

By means of a preconfigured multicast address on the Cisco Unified Communications Manager or gateway, the gateway can "listen" for Real-Time Transport Protocol (RTP) packets that are broadcast from a default router in the network and can relay the packets to designated voice interfaces in the network. You can initiate the call on hold. However, you cannot initiate music on hold on a MGCP controlled analog phone. Whenever a called party places a calling party on hold, Cisco Communications Manager requests the MOH server to stream RTP packets to the "on-hold" interface through the preconfigured multicast address. In this way, RTP packets are relayed to appropriately configured voice interfaces that have been placed on hold. When you configure a multicast address on a gateway, the gateway sends an Internet Gateway Management Protocol (IGMP) "join" message to the default router, indicating to the default router that the gateway is ready to receive RTP multicast packets.

Multiple MOH servers can be present in the same network, but each server must have a different Class D IP address, and the address must be configured in Cisco Communications Manager and the MGCP voice gateways. For more information on configuring MOH, see the http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cminterop/configuration/15-0m/vc-15-0m-book/vc-ucm-mgcp-gw.html#GUID-A3461142-2F05-4420-AEE6-032FCA3B7952

CHAPTER 20

Configuration Examples

This chapter provides examples of configuring common networking tasks on the router. The examples in this chapter are provided for illustrative purposes only; little or no context is given with these examples. For more information, see Installing the Software, on page 67.

When reading this section, also be aware that networking configurations are complex and can be configured in many ways. The examples in this section show one method of accomplishing a configuration.

This chapter contains the following examples:

Copying the Consolidated Package from the TFTP Server to the Router

The following example shows how to copy the consolidated package from the TFTP server to the router:

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul  2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 17:48:41 +00:00  .prst_sync
324481  drwx        4096   Jul  2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul  2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 17:49:14 +00:00  tracelogs
32449  drwx        4096   Jul  2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul  2 2012 15:27:08 +00:00  vman_fdb
```

```
7451738112 bytes total (7015186432 bytes free)
Router# copy tftp bootflash:
Address or name of remote host []? 10.81.116.4
Source filename []? rtp-isr4400-54/isr4400.bin
Destination filename [isr4400.bin]?
Accessing tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin...
Loading rtp-isr4400-54/isr4400.bin from 10.81.116.4 (via GigabitEthernet0): !!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 424317088 bytes]

424317088 bytes copied in 371.118 secs (1143348 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 17:48:41 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:05:07 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096 Jul 31 2012 19:15:39 +00:00   .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin

7451738112 bytes total (6590910464 bytes free)
```

Configuring the Router to Boot Using the Consolidated Package Stored on the Router

The following example shows how to configure the router to boot using the consolidated package stored on the router:

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 17:48:41 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:05:07 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096 Jul 31 2012 19:15:39 +00:00   .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin

7451738112 bytes total (6590910464 bytes free)


Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# boot system bootflash:isr4400.bin
Router(config)# config-register 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system bootflash:isr4400.bin
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
```

```
Sep 13 18:08:36.311 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit
with reload chassis code


Initializing Hardware ...

System integrity status: c0000600
Failures detected:
 Boot FPGA corrupt

Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2012  by cisco Systems, Inc.
Compiled Mon 06/18/2012 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory

File size is 0x194a90a0
Located isr4400.bin
Image size 424317088 inode num 13, bks cnt 103594 blk size 8*512
###########################################################################################
Boot image size = 424317088 (0x194a90a0) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
 calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
 expected   7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5133 msec
Image validated
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (local/local): load_modules took: 2 seconds, expected

max time 2 seconds

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706


Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version

15.3(20120910:013018) [mcp_dev-BLD-BLD_MCP_DEV_LATEST_20120910_000023-ios 153]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Sun 09-Sep-12 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Warning:  the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133589K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Press RETURN to get started!
```

Extracting the Subpackages from a Consolidated Package into the Same File System

The following example shows how to extract the subpackages from a consolidated package into the same file system.

After entering the **request platform software package expand file bootflash:isr4400.bin** command (note that the **to** option is not used) the subpackages are extracted from the consolidated package into **bootflash:**

```
Router> enable
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:13:31 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin

7451738112 bytes total (6590029824 bytes free)
Router# request platform software package expand file bootflash:isr4400.bin
Verifying parameters
```

```
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:16:49 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin
778756  -rw-   112911096  Sep 13 2012 18:15:49 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778757  -rw-     2220784  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778758  -rw-      371440  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778759  -rw-     8080112  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778760  -rw-     9331440  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778761  -rw-      379632  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         778754  -rw-       10540  Sep 13 2012 18:15:48 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
778762  -rw-    27218680  Sep 13 2012 18:15:50 +00:00
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778763  -rw-    78938264  Sep 13 2012 18:15:50 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778764  -rw-    45177592  Sep 13 2012 18:15:50 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778765  -rw-   114662144  Sep 13 2012 18:16:01 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778766  -rw-    26360568  Sep 13 2012 18:16:03 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778767  -rw-    13091576  Sep 13 2012 18:16:06 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778755  -rw-       11349  Sep 13 2012 18:16:06 +00:00  packages.conf

7451738112 bytes total (6150725632 bytes free)
```

Extracting the Subpackages from a Consolidated Package into a Different File System

The following example shows how to extract the subpackages from a consolidated package into a different file system.

The initial **dir usb0:** command shows that there are no subpackages in the **bootflash:** directory.

After the **request platform software package expand file usb0:isr4400.bin to bootflash:** command is entered, the subpackages are displayed in the **bootflash:** directory. The isr4400.bin consolidated package file is in the **usb0:** directory.

```
Router# dir usb0:
Directory of usb0:/

  121  -rwx   424317088  Sep 13 2012 18:27:50 +00:00  isr4400.bin

7988666368 bytes total (7564341248 bytes free)

Router# dir bootflash:
```

```
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:41:51 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb

7451738112 bytes total (6590418944 bytes free)
Router# request platform software package expand file usb0:isr4400.bin to bootflash:
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.
Router# dir bootflash:
Directory of bootflash:/
11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:46:52 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454276  -rw-   112911096  Sep 13 2012 18:46:05 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454277  -rw-     2220784  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454278  -rw-      371440  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454279  -rw-     8080112  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454280  -rw-     9331440  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454281  -rw-      379632  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         454274  -rw-       10540  Sep 13 2012 18:46:05 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
454282  -rw-    27218680  Sep 13 2012 18:46:06 +00:00
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454283  -rw-    78938264  Sep 13 2012 18:46:06 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454284  -rw-    45177592  Sep 13 2012 18:46:06 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454285  -rw-   114662144  Sep 13 2012 18:46:16 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454286  -rw-    26360568  Sep 13 2012 18:46:19 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454287  -rw-    13091576  Sep 13 2012 18:46:21 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6575869952 bytes free)
```

Configuring the Router to Boot Using Subpackages

After placing the provisioning file and subpackage files in a directory and booting the router, we recommend that you do not rename, delete, or alter any of these files. Renaming, deleting, or altering the files can lead to unpredictable router problems and behaviors. Each version of a consolidated package contains subpackages that are similar to those shown in the following table. However, each version of a consolidated package may contain different versions of each subpackage.

Table 22: Subpackages

Subpackage	Description
RPBase	Provides the operating system software for the Route Processor. This is the only bootable package.
RPControl	Controls the control plane processes that act as the interface between the Cisco IOS process and the rest of the platform.
RPAccess	Exports processing of restricted components, such as Secure Socket Layer (SSL), Secure Shell (SSH), and other security features.
RPIOS	Provides the Cisco IOS kernel, where Cisco IOS XE features are stored and run. Each consolidated package has a different version of RPIOS.
ESPBase	Provides the Embedded Services Processor (ESP) operating system and control processes, and ESP software.
SIPBase	Provides control processes.
SIPSPA	Provides Input/Output (I/O) drivers.
Firmware	Firmware subpackage. The name of the subpackage includes the module type, which either refers to a Network Information Module (NIM) or Cisco Enhanced Service Module.

The following example shows how to configure the router to boot using subpackages:

The **dir bootflash:** command confirms that all subpackages and the provisioning file are in the same file system, as shown in the following example:

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:46:52 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454276  -rw-   112911096  Sep 13 2012 18:46:05 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454277  -rw-     2220784  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454278  -rw-      371440  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454279  -rw-     8080112  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454280  -rw-     9331440  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454281  -rw-      379632  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         454274  -rw-       10540  Sep 13 2012 18:46:05 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
454282  -rw-    27218680  Sep 13 2012 18:46:06 +00:00
```

```
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454283  -rw-    78938264  Sep 13 2012 18:46:06 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454284  -rw-    45177592  Sep 13 2012 18:46:06 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454285  -rw-   114662144  Sep 13 2012 18:46:16 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454286  -rw-    26360568  Sep 13 2012 18:46:19 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454287  -rw-    13091576  Sep 13 2012 18:46:21 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6575869952 bytes free)

Router# show running | include boot
boot-start-marker
boot-end-marker
license boot level adventerprise
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# boot system bootflash:packages.conf
Router(config)# config-register 0x2102
Router(config)# exit
Router# show running | include boot
boot-start-marker
boot system bootflash:packages.conf
boot-end-marker
license boot level adventerprise
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 18:49:39.720 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with
 reload chassis code


Initializing Hardware ...

System integrity status: c0000600
Failures detected:
 Boot FPGA corrupt


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2012  by cisco Systems, Inc.
Compiled Mon 06/18/2012 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory

File size is 0x00002c55
Located packages.conf
Image size 11349 inode num 454275, bks cnt 3 blk size 8*512
#
File size is 0x04b48098
Located isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
Image size 78938264 inode num 454283, bks cnt 19273 blk size 8*512
################################################################################################################################################################################################################################################################################################################################
```

```
Boot image size = 78938264 (0x4b48098) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
 calculated dbe960a6:d239245c:76d93622:d6c31a41:40e9e420
 expected   dbe960a6:d239245c:76d93622:d6c31a41:40e9e420
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 1159 msec
Image validated

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
 15.3(20120910:013018) [mcp_dev-BLD-BLD_MCP_DEV_LATEST_20120910_000023-ios 153]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 09-Sep-12 21:28 by mcpre



Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Warning:  the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133589K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
```

```
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Press RETURN to get started!

Router>
Router> en
Router# show version
Cisco IOS XE Software, Version BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ext
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
15.4(20140527:095327)
[v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]


IOS XE Version: BLD_V154_3_S_XE313_THROTTLE_LATEST

Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 1 minute
Uptime for this control processor is 4 minutes
 --More--         System returned to ROM by reload
System image file is "bootflash:packages.conf"
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: adventerprise
License Type: EvalRightToUse
 --More--         Next reload license Level: adventerprise

cisco ISR4451/K9 (2RU) processor with 1133589K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Configuration register is 0x2102

Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
```

```
373153  drwx      114688  Sep 13 2012 18:54:03 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454276  -rw-   112911096  Sep 13 2012 18:46:05 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454277  -rw-     2220784  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454278  -rw-      371440  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454279  -rw-     8080112  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454280  -rw-     9331440  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454281  -rw-      379632  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         454274  -rw-       10540  Sep 13 2012 18:46:05 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
454282  -rw-    27218680  Sep 13 2012 18:46:06 +00:00
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454283  -rw-    78938264  Sep 13 2012 18:46:06 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454284  -rw-    45177592  Sep 13 2012 18:46:06 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454285  -rw-   114662144  Sep 13 2012 18:46:16 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454286  -rw-    26360568  Sep 13 2012 18:46:19 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454287  -rw-    13091576  Sep 13 2012 18:46:21 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6574940160 bytes free)

Router# del isr4400*
Delete filename [isr4400*]?
Delete bootflash:/isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
[confirm]
Delete bootflash:/isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
[confirm]
Delete bootflash:/isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
[confirm]
Delete bootflash:/isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf?
[confirm]
Delete bootflash:/isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
[confirm]
Delete bootflash:/isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:54:03 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6574952448 bytes free)
Router# del packages.conf
Delete filename [packages.conf]?
Delete bootflash:/packages.conf? [confirm]
Router# copy tftp bootflash:
```

```
Address or name of remote host []? 10.81.116.4
Source filename []? rtp-isr4400-54/isr4400.bin
Destination filename [isr4400.bin]?
Accessing tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin...
Loading rtp-isr4400-54/isr4400.bin from 10.81.116.4 (via GigabitEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 424317088 bytes]

424317088 bytes copied in 351.758 secs (1206276 bytes/sec)
```

Backing Up Configuration Files

This section provides the following examples:

- Copying a Startup Configuration File to BootFlash, on page 298
- Copying a Startup Configuration File to a USB Flash Drive, on page 299
- Copying a Startup Configuration File to a TFTP Server, on page 299

Copying a Startup Configuration File to BootFlash

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul  2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul  2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul  2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 19:03:19 +00:00  tracelogs
32449  drwx        4096   Jul  2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul  2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 19:02:50 +00:00  isr4400.bin

7451738112 bytes total (6150721536 bytes free)
Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?
1367 bytes copied in 0.116 secs (11784 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul  2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul  2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul  2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 19:03:19 +00:00  tracelogs
32449  drwx        4096   Jul  2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul  2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 19:02:50 +00:00  isr4400.bin
   14  -rw-        1367  Sep 13 2012 19:03:57 +00:00  startup-config

7451738112 bytes total (6150717440 bytes free)
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.18.40.33
Destination filename [router-confg]? startup-config
!!
1367 bytes copied in 0.040 secs (34175 bytes/sec)
Router# exit
```

```
Router con0 is now available


Press RETURN to get started.
```

Copying a Startup Configuration File to a USB Flash Drive

```
Router# dir usb0:
Directory of usb0:/

No files in directory

4094840832 bytes total (4094836736 bytes free)
Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?
1644 bytes copied in 0.248 secs (6629 bytes/sec)
Router# dir usb0:
Directory of usb0:/

3097__-rwx________1644__ Oct 3 2012 14:53:50 +00:00__startup-config

4094840832 bytes total (4094832640 bytes free)
Router#
```

Copying a Startup Configuration File to a TFTP Server

```
Router# copy nvram:startup-config tftp:
Address or name of remote host []? 172.18.40.4
Destination filename [router-confg]?
!!
3274 bytes copied in 0.039 secs (83949 bytes/sec)
Router#
```

Displaying Digitally Signed Cisco Software Signature Information

In this example, authenticity details for a consolidated package are displayed on the screen:

```
router# show software authenticity running
PACKAGE isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
-------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48E17
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
----------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DA3
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48E98
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-rpaccess.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
---------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DB4
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DBE
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DC7
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D74
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-espbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D64
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-sipbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D94
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-sipspa.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
-------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D7F
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

SYSTEM IMAGE
------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48F33
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : System Bootstrap, Version 12.2(20121015:145923
ROMMON
------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50801108
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : System Bootstrap, Version 12.2(20121015:145923
Microloader
-----------
Image type                    : Release
    Signer Information
        Common Name           : CiscoSystems
        Organization Name     : CiscoSystems
    Certificate Serial Number : bace997bdd9882f8569e5b599328a448
    Hash Algorithm            : HMAC-SHA256
    Verifier Information
        Verifier Name         : Hardware Anchor
        Verifier Version      : F01001R06.02c4c06f82012-09-17
```

Obtaining the Description of a Module or Consolidated Package

In this example, internal details of the consolidated package are displayed on the screen:

```
router# request platform software package describe file
bootflash:isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
Package: isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
  Size: 79755832
  Timestamp: 2013-01-15 15:46:59 UTC
  Canonical path: /bootflash/isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg

  Raw disk-file SHA1sum:
    5cd5916a216b147e3d9e33c0dc5afb18d86bda94

  Digital Signature Verified
  Computed SHA1sum:
    de80d5920819d224113b81a1d64b17449859952e
  Contained SHA1sum:
    de80d5920819d224113b81a1d64b17449859952e
  Hashes match. Package is valid.

  Header size:     760 bytes
  Package type:    30001
  Package flags:   0
  Header version:  1

  Internal package information:
    Name: rp_base
    BuildTime: 2013-01-14_14.55
    ReleaseDate: Mon-14-Jan-13-16:27
    BootArchitecture: i686
    RouteProcessor: overlord
    Platform: ISR
    User: mcpre
    PackageName: rpbase
    Build: BLD_MCP_DEV_LATEST_20130114_162711
    CardTypes:

  Package is bootable on RP when specified
  by packages provisioning file.
```

APPENDIX A

Unsupported Commands

The Cisco 4000 Series routers contain a series of commands with the **logging** or **platform** keywords that either produce no output or produce output that is not useful for customer purposes. Such commands that are not useful for customer purposes are considered as unsupported commands. You will not find any further Cisco documentation for the unsupported commands.

The following is a list of unsupported commands for the Cisco 4000 Series routers:

- clear logging onboard slot f0 dram
- clear logging onboard slot f0 voltage
- clear logging onboard slot f0 temperature
- show logging onboard slot f0 dram
- show logging onboard slot f0 serdes
- show logging onboard slot f0 status
- show logging onboard slot f0 temperature
- show logging onboard slot f0 uptime
- show logging onboard slot f0 uptime latest
- show logging onboard slot f0 voltage
- show logging onboard slot 0 dram
- show logging onboard slot 0 serdes
- show logging onboard slot 0 status
- show logging onboard slot 0 temperature
- show logging onboard slot 0 uptime
- show logging onboard slot 0 uptime latest
- show logging onboard slot 0 voltage
- show platform software adjacency r0 special
- show platform software adjacency rp active special
- show platform software ethernet rp active l2cp

- show platform software ethernet rp active l2cp interface GigabitEthernet0
- show platform software ethernet rp active loopback
- show platform software ethernet rp active vfi
- show platform software ethernet r0 vfi
- show platform software ethernet r0 vfi id 0
- show platform software ethernet r0 vfi name GigabitEthernet0
- show platform software ethernet r0 l2cp
- show platform software ethernet r0 l2cp interface GigabitEthernet0
- show platform software ethernet r0 bridge-domain statistics
- show platform software flow r0 exporter name GigabitEthernet0
- show platform software flow r0 exporter statistics
- show platform software flow r0 global
- show platform software flow r0 flow-def
- show platform software flow r0 interface
- show platform software flow r0 ios
- show platform software flow r0 monitor
- show platform software flow r0 sampler
- show platform hardware qfp active classification feature-manager label GigabitEthernet 0 0
- show platform software interface f0 del-track
- show platform software interface fp active del-track
- show platform software rg r0 services
- show platform software rg r0 services rg-id 0
- show platform software rg r0 services rg-id 0 verbose
- show platform software rg r0 services verbose
- show platform software rg r0 statistics
- show platform software rg rp active services
- show platform software rg rp active services rg-id 0
- show platform software rg rp active services rg-id 0 verbose
- show platform software rg rp active statistics
- show platform hardware slot 0 dram statistics
- show platform hardware slot f0 dram statistics
- show platform hardware slot 0 eobc interface primary rmon
- show platform hardware slot 0 eobc interface primary status

- show platform hardware slot 0 eobc interface standby rmon
- show platform hardware slot 0 eobc interface standby status
- show platform hardware slot f0 eobc interface primary rmon
- show platform hardware slot f0 eobc interface primary status
- show platform hardware slot f0 eobc interface standby rmon
- show platform hardware slot f0 eobc interface standby status
- show platform hardware slot f0 sensor consumer
- show platform hardware slot f0 sensor producer