Configuration Fundamentals Configuration Guide, Cisco IOS Release 15.1S

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

CONTENTS

Using the Cisco IOS Command-Line Interface

The Cisco IOS command-line interface (CLI) is the primary user interface used for configuring, monitoring, and maintaining Cisco devices. This user interface allows you to directly and simply execute Cisco IOS commands, whether using a router console or terminal, or using remote access methods.

This chapter describes the basic features of the Cisco IOS CLI and how to use them. Topics covered include an introduction to Cisco IOS command modes, navigation and editing features, help features, and command history features.

Additional user interfaces include Setup mode (used for first-time startup), the Cisco Web Browser, and user menus configured by a system administrator. For information about Setup mode, see Using Setup Mode to Configure a Cisco Networking Device and Using AutoInstall to Remotely Configure Cisco Networking Devices. For information on issuing commands using the Cisco Web Browser, see “Using the Cisco Web Browser User Interface”. For information on user menus, see “Managing Connections, Menus, and System Banners”.

For a complete description of the user interface commands in this chapter, see the *Cisco IOS Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the Cisco IOS Master Command List, All Releases .

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Cisco IOS CLI Command Modes Overview

To aid in the configuration of Cisco devices, the Cisco IOS command-line interface is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of router and network operations. The commands available to you at any given time depend on the mode you are in. Entering a question mark (**?**) at the system prompt (router prompt) allows you to obtain a list of commands available for each command mode.

The use of specific commands allows you to navigate from one command mode to another. The standard order that a user would access the modes is as follows: user EXEC mode; privileged EXEC mode; global configuration mode; specific configuration modes; configuration submodes; and configuration subsubmodes.

When you start a session on a router, you generally begin in user EXEC mode, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of Exec commands are available in user EXEC mode. This level of access is reserved for tasks that do not change the configuration of the router, such as determining the router status.

In order to have access to all commands, you must enter privileged EXEC mode, which is the second level of access for the EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. In privileged EXEC mode, you can enter any EXEC command, because privileged EXEC mode is a superset of the user EXEC mode commands.

Most EXEC mode commands are one-time commands, such as **show** or **more** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. EXEC mode commands are not saved across reboots of the router.

From privileged EXEC mode, you can enter global configuration mode. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots.

From global configuration mode you can enter a variety of protocol-specific or feature-specific configuration modes. The CLI hierarchy requires that you enter these specific configuration modes only through global configuration mode. As an example, this chapter describes interface configuration mode, a commonly used configuration mode.

From configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode. As an example, this chapter describes the subinterface configuration mode, a submode of the interface configuration mode.

ROM monitor mode is a separate mode used when the router cannot boot properly. If your system (router, switch, or access server) does not find a valid system image to load when it is booting, the system will enter ROM monitor mode. ROM monitor (ROMMON) mode can also be accessed by interrupting the boot sequence during startup.

The following sections contain detailed information on these command modes:

The table that follows these sections and summarizes the main Cisco IOS command modes.

Cisco IOS CLI Task List

Getting Context-Sensitive Help

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

To get help specific to a command mode, a command name, a keyword, or an argument, use any of the following commands:

Command	Purpose
(*prompt*)# **help**	Displays a brief description of the help system.
(*prompt*)# *abbreviated-command-entry***?**	Lists commands in the current mode that begin with a particular character string.
(*prompt*)# *abbreviated-command-entry* <**Tab**>	Completes a partial command name.
(*prompt*)# **?**	Lists all commands available in the command mode.
(*prompt*)# *command***?**	Lists the available syntax options (arguments and keywords) for the command.
(*prompt*)# *command keyword* **?**	Lists the next available syntax option for the command.

Note that the system prompt will vary depending on which configuration mode you are in.

When context-sensitive help is used, the space (or lack of a space) before the question mark (**?**) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (**?**). Do not include a space. This form of help is called word help, because it completes a word for you. For more information, see the “Completing a Partial Command Name ” section later in this chapter.

To list keywords or arguments, enter a question mark (**?**) in place of a keyword or argument. Include a space before the**?**. This form of help is called command syntax help, because it shows you which keywords or arguments are available based on the command, keywords, and arguments you already have entered.

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the **configureterminal**command to **configt**. Because the abbreviated form of the command is unique, the router will accept the abbreviated form and execute the command.

Entering the**help** command (available in any command mode) will provide the following description of the help system:

```
Router#
 help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
```

```
be empty and you must back up until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

As described in the **help** command output, you can use the question mark (**?**) to complete a partial command name (partial help), or to obtain a list of arguments or keywords that will complete the current command.

The following example illustrates how the context-sensitive help feature enables you to create an access list from configuration mode.

Enter the letters **co** at the system prompt followed by a question mark (**?**). Do not leave a space between the last letter and thequestion mark. The system provides the commands that begin with **co**.

```
Router# co?
configure  connect  copy
```

Enter the **configure** command followed by a space and aquestion mark to list the keywords for the command and a brief explanation:

```
Router# configure ?
  memory    Configure from NV memory
  network   Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  terminal  Configure from the terminal
  <cr>
```

The <cr> symbol ("cr" stands for carriage return) appears in the list to indicate that one of your options is to press the Return or Enter key to execute the command, without adding any keywords. In this example, the output indicates that your options for the configure command are **configurememory** (configure from NVRAM), **configurenetwork** (configure from a file on the network), **configureoverwrite-network** (configure from a file on the network and replace the file in NVRAM), or **configureterminal** (configure manually from the terminal connection). For most commands, the <cr> symbol is used to indicate that you can execute the command with the syntax you have already entered. However, the configure command is a special case, because the CLI will prompt you for the missing syntax:

```
Router# configure
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

The default response for the ? prompt is indicated in the CLI output by a bracketed option at the end of the line. In the preceding example, pressing the Enter (or Return) key is equivalent to typing in the word "terminal."

Enter the **configureterminal** command to enter global configuration mode:

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

The CLI provides error isolation in the form of an error indicator, a caret symbol (^). The ^ symbol appears at the point in the command string where the user has entered incorrect or unrecognized command syntax. For example, the caret symbol in the following output shows the letter that was mistyped in the command:

```
Router# configure terminal
```

```
                     ^
% Invalid input detected at '^' marker.
Router#
```

Note that an error message (indicated by the % symbol) appears on the screen to alert you to the error marker.

Enter the **access-list** command followed by a space and a question mark to list the available options for the command:

```
Router(config)# access-list ?
 <1-99>            IP standard access list
 <100-199>         IP extended access list
 <1100-1199>       Extended 48-bit MAC address access list
 <1300-1999>       IP standard access list (expanded range)
 <200-299>         Protocol type-code access list
 <2000-2699>       IP extended access list (expanded range)
 <700-799>         48-bit MAC address access list
 dynamic-extended  Extend the dynamic ACL absolute timer
 rate-limit        Simple rate-limit specific access list
```

The two numbers within the angle brackets represent an inclusive range. Enter the access list number **99** and then enter another question mark to see the arguments that apply to the keyword and brief explanations:

```
Router(config)# access-list 99 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
```

Enter the **deny** argument followed by a question mark (**?**)to list additional options:

```
Router(config)# access-list 99 deny ?
  A.B.C.D  Address to match
```

Generally, uppercase letters represent variables (arguments). Enter the IP address followed by a question mark (**?**) to list additional options:

```
Router(config)# access-list 99 deny 172.31.134.0 ?
  A.B.C.D  Mask of bits to ignore
  <cr>
```

In this output, A.B.C.D indicates that use of a wildcard mask is allowed. The wildcard mask is a method for matching IP addresses or ranges of IP addresses. For example, a wildcard mask of 0.0.0.255 matches any number in the range from 0 to 255 that appears in the fourth octet of an IP address.

Enter the wildcard mask followed by a question mark (**?**) to list further options:

```
Router(config)# access-list 99 deny 172.31.134.0 0.0.0.255 ?
<cr>
```

The <cr> symbol by itself indicates there are no more keywords or arguments. Press Enter (or Return) to execute the command.:

```
Router(config)# access-list 99 deny 172.31.134.0 0.0.0.255
```

The system adds an entry to access list 99 that denies access to all hosts on subnet 172.31.134.0, while ignoring bits for IP addresses that end in 0 to 255.

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 feature or function. Use the command without the **no**keyword to reenable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the

noiprouting form of the **iprouting** command. To reenable it, use the plain **iprouting** form. The Cisco IOS software command reference publications describe the function of the **no** form of the command whenever a **no** form is available.

Many CLI commands also have a**default** form. By issuing the **default***command-name* command, you can configure the command to its default setting. The Cisco IOS software command reference documents generally describe the function of the **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.

Using Command History

The Cisco IOS CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. To use the command history feature, perform any of the tasks described in the following sections:

Using CLI Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the Cisco IOS CLI. The following subsections describe these features:

Searching and Filtering CLI Output

The Cisco IOS CLI provides ways of searching through large amounts of command output and filtering output to exclude information you do not need. These features are enabled for**show** and **more** commands, which generally display large amounts of data.

Note **Show** and **more** commands are always entered in user EXEC or privileged EXEC.

When output continues beyond what is displayed on your screen, the Cisco IOS CLI displays a --More-- prompt. Pressing Return displays the next line; pressing the Spacebar displays the next screen of output. The CLI String Search feature allows you to search or filter output from --More-- prompts.

Using the Cisco IOS CLI Examples

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

EXEC Commands in Configuration Mode

Beginning in Cisco IOS Release 12.1(11b)E, EXEC-level Cisco IOS commands (such as **show**, **clear**, and **debug** commands) can be entered within any configuration mode (such as global configuration mode) by issuing the **do**command followed by the desired EXEC command. This feature provides the convenience of entering EXEC-level commands without needing to exit the current configuration mode.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EXEC Commands in Configuration Mode

You must have your network up and running with Cisco IOS Release 12.1(11b)E or a later release installed.

How to Enter EXEC Commands in Configuration Mode

Using the do Command in Configuration Mode

To execute an EXEC-level command in any configuration mode (including configuration submodes), complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **do** *command*

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	**do** *command*
	Example:
	`Router(config)# configuration command`
		Allows you to execute any EXEC mode command from within any configuration mode.
		command --The EXEC command to be executed.

Using the do Command in Interface Configuration Mode

To execute an EXEC-level command for a specific interface on a router, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot /port*
4. **do** *command*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Example: `Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot /port* **Example:** `Router(config)# interface serial 3/0`	The syntax for this command varies according to your platform and Cisco IOS release. For complete information, refer to the "Additional References" section. • The slot/port argument identifies the slot and port on the router where you are entering **do** commands.

Step 4	**do** *command*
	Example:
	`Router(config-if)# do show interfaces serial 3/0`
		Allows you to execute any EXEC mode command from within any configuration mode on a specific interface.
		command --The EXEC command to be executed.

Configuration Examples for EXEC Commands in Configuration Mode

Example do show interface Command

The following example shows how to execute the EXEC-level **showinterface** command from within global configuration mode:

```
Router(config)# do show interfaces serial 3/0
Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
```

Example do clear vpdn tunnel Command

The following example shows how to execute the EXEC-level **clearvpdntunnel** command from within VPDN configuration mode:

```
Router(config-vpdn)# do clear vpdn tunnel
Router(config-vpdn)#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS configuration commands	*Cisco IOS Configuration Fundamentals Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified	--

MIBs

MIB	MIBs Link
• No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these	http://www.cisco.com/cisco/web/support/index.html

Description	Link
resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	

Restrictions for EXEC Commands in Configuration Mode

You cannot use the **do** command to execute the **configureterminal** EXEC command because issuing the **configureterminal**command changes the mode to configuration mode.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

show Command Output Redirection

The show Command Output Redirection feature provides the capability to redirect output from Cisco IOS command-line interface (CLI) **show** commands and **more** commands to a file.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About show Command Output Redirection

This feature enhances the **show** commands in the Cisco IOS CLI to allow large amounts of data output to be written directly to a file for later reference. This file can be saved on local or remote storage devices such as Flash, a SAN Disk, or an external memory device.

For each **show** command issued, a new file can be created, or the output can be appended to an existing file. Command output can optionally be displayed on-screen while being redirected to a file by using the **tee** keyword. Redirection is available using a pipe (|) character after any **show** command, combined with the followingkeywords:

Output redirection keywords:

Keyword	Usage
append	Append redirected output to URL (URLs supporting append operation only)

Keyword	Usage
begin	Begin with the line that matches
count	Count number of lines which match regexp
exclude	Exclude lines that match
format	Format the output using the specified spec file
include	Include lines that match
redirect	Redirect output to URL
tee	Copy output to URL

These extenstions can also be added to **more** commands.

How to Use the show Command Enhancement

No configuration tasks are associated with this enhancement. For usage guidelines, see the command reference documents listed in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS configuration commands	*Cisco IOS Configuration Fundamentals Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified	--

MIBs

MIB	MIBs Link
• No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for show Command Output Redirection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for the show Command Ouput Redirection Feature

Feature Name	Releases	Feature Information
show Command Output Redirection	12.0(21)S 12.2(13)T	• The show Command Output Redirection feature provides the capability to redirect output from Cisco IOS

Feature Name	Releases	Feature Information
		command-line interface (CLI) **show** commands and **more** commands to a file. The following commands were introduced or modified: **show**, and**more**.

Overview Basic Configuration of a Cisco Networking Device

Cisco IOS software provides two features, AutoInstall and Setup mode, to simplify configuring a Cisco IOS-based networking device. AutoInstall enables automatic loading of device configuration files from a remote location and can be used to configure several devices concurrently. Setup is an interactive Cisco IOS software command-line interface (CLI) mode that guides you through a basic (also called a startup) configuration but limits you to configuring a single device at a time. AutoInstall is an automatic process for the device that is being configured; Setup is a manual process for the device that is being configured.

This module provides an introduction to each feature and directs you to modules that describe the features in detail and explain how to use them.

The terms initial configuration and startup configuration are used interchangeably.

Prerequisites for Basic Configuration of a Cisco Networking Device

Prerequisites for Cisco IOS AutoInstall

- Using AutoInstall to Remotely Configure Cisco Networking Devices module is written specifically for networking devices running Cisco IOS Release 12.4(1) or newer. However most of the information in this document can be used to configure networking devices that support AutoInstall and are not running Cisco IOS release 12.4(1) or newer. The two key differences that you must allow for are:
    - Some Cisco networking devices use BOOTP instead of DHCP to request IP address addresses over LAN interfaces. Enabling BOOTP support on your DHCP server will resolve this issue.
    - Some Cisco networking devices use a DHCP client identifier format that is different from the format used by networking devices running Cisco IOS release 12.4(1) or newer. This document only explains the DHCP client identifier format used by networking devices running Cisco IOS

release 12.4(1) or newer. Use the process described in the “Determining the Value for the DHCP Client Identifier Automatically” section in Using AutoInstall to Remotely Configure Cisco Networking Devices module to determine the DHCP client identifier format that your Cisco networking device is using.

- No configuration file resides in NVRAM on the networking device that is being configured with AutoInstall.
- The configuration files that you want to load on to the networking device using AutoInstall reside on a TFTP server that is connected to the network. In most cases there is more than one file; for example, a network file with the IP-to-hostname mappings and a device-specific configuration file.
- You have someone at the remote site to connect the networking device that is being configured with AutoInstall to the network and power it on.
- The network has the IP connectivity necessary to permit the networking device to load configuration files from the TFTP server during the AutoInstall process.
- A DHCP server is available on the network to provide IP addresses to networking devices that are using AutoInstall over a LAN connection.

Prerequisites for Cisco IOS Setup Mode

- A terminal is connected to the console port of the device being configured.
- You know the interfaces you want to configure.
- You know the routing protocols you want to enable.

For information about routing protocols, see the *Cisco IOS IP Routing Protocols Configuration Guide* .

- You know whether the device you are configuring will perform bridging.
- You know whether the device you are configuring has protocol translation installed.
- You have network addresses for the protocols being configured.

For information about network addresses, see the *Cisco IOS IP Addressing Services Configuration Guide*.

- You have a password strategy for your network environment.

For information about passwords and device security, see “Configuring Security with Passwords, Privilege Levels, and Login User names for CLI Sessions on Networking Devices” in the *Cisco IOS Security Configuration Guide* .

- You have or have access to documentation for the product you want to configure.

Restrictions for Basic Configuration of a Cisco Networking Device

Restrictions for Cisco IOS AutoInstall

- (Serial interfaces only) AutoInstall over a serial interface using either HDLC or Frame Relay can be performed only over the first serial port on a new device (serial interface 0 or serial interface x/0).
- (LAN interfaces only) Only LAN Token Ring interfaces that set ring speed with physical jumpers support AutoInstall.

Restrictions for Cisco IOS Setup Mode

- Setup mode is hardware dependent. You must follow instructions for the specific product you want to configure, as described in documentation for that product.

- Some configuration parameters apply only when a networking device has the protocol translation option. If a device does not have protocol translation, Setup does not prompt for these parameters.

Information About Basic Configuration of a Cisco Networking Device

Before you configure a networking device with a basic configuration, you should understand the following concepts and decide whether AutoInstall or Setup mode is the best method, based on your requirements.

- Comparison of Cisco IOS AutoInstall and Cisco IOS Setup Mode, page 21
- Cisco IOS AutoInstall, page 21
- Cisco IOS Setup Mode, page 21

Comparison of Cisco IOS AutoInstall and Cisco IOS Setup Mode

Cisco IOS AutoInstall enables automatic loading of device configuration files from a remote location and can be used to configure several devices concurrently. Setup is an interactive Cisco IOS software CLI mode that guides you through a basic (also called a startup) configuration but limits you to configuring a single device at a time. AutoInstall is an automatic process; Setup is a manual process.

Cisco IOS AutoInstall

AutoInstall is the Cisco IOS software feature that enables the configuration of a remote networking device from a central location. The configuration files must be stored on a TFTP server that is accessible by the devices that you are using AutoInstall to setup.

AutoInstall is supported over Ethernet, Token Ring, and FDDI interfaces for LANs, serial interfaces using High-Level Data Link Control (HDLC) encapsulation, serial interfaces using Frame Relay encapsulation for WANs, and WIC-1-DSU-T1v2 cards (No other T1E1 card supports Autoinstall.).

AutoInstall is designed to facilitate central management of installations at remote sites. The AutoInstall process begins when a Cisco IOS software-based device is turned on and a valid configuration file is not found in NVRAM. AutoInstall may not start if the networking device has Cisco Router and Security Device Manager (SDM) or Cisco Network Assistant already installed. In this case, to enable AutoInstall you need to disable SDM.

Using AutoInstall to Remotely Configure Cisco Networking Devices module describes how AutoInstall functions, how to disable SDM, and how to configure devices to use AutoInstall.

Cisco IOS Setup Mode

Cisco IOS Setup mode enables you to build an initial configuration file using the Cisco IOS CLI or System Configuration Dialog. The dialog guides you through initial configuration and is useful when you are unfamiliar with Cisco products or the CLI and when configuration changes do not require the level of detail the CLI provides.

Setup starts automatically when a device has no configuration file in NVRAM and is not preconfigured from the factory to use Cisco SDM. When setup completes, it presents the System Configuration Dialog. This dialog guides you through an initial configuration with prompts for basic information about your device and network and then creates an initial configuration file. After the file is created, you can use the CLI to perform additional configuration.

Using Setup Mode to Configure a Cisco Networking Device describes how to use Setup to build a basic configuration and to make configuration changes.

Where to Go Next

Proceed to either Using AutoInstall to Remotely Configure Cisco Networking Devices module or Using Setup Mode to Configure a Cisco Networking Device.

Additional References

This section provides references related to the basic configuration of a Cisco networking device.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuration fundamentals commands	*Cisco IOS Configuration Fundamentals Command Reference*
Configuring a networking device for the first time using the Cisco IOS software feature AutoInstall.	Using AutoInstall to Remotely Configure Cisco Networking Devices module in *Cisco IOS Configuration Fundamentals Configuration Guide*
Configuring a networking device using Cisco IOS Setup mode	Using Setup Mode to Configure a Cisco Networking Device module in *Cisco IOS Configuration Fundamentals Configuration Guide*

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

Feature Information for Overview Basic Configuration of a Cisco Networking Device

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Overview: Basic Configuration of a Cisco Networking Device

Feature Name	Releases	Feature Information
Overview: Basic Configuration of a Cisco Networking Device	12.4(3)	Cisco IOS software provides two features, AutoInstall and Setup mode, to simplify configuring a Cisco IOS-based networking device. AutoInstall enables automatic loading of device configuration files from a remote location and can be used to configure several devices concurrently. Setup is an interactive Cisco IOS software command-line interface (CLI) mode that guides you through a basic (also called a startup) configuration but limits you to configuring a single device at a time. AutoInstall is an automatic process for the device that is being configured; Setup is a manual process for the device that is being configured.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Using Setup Mode to Configure a Cisco Networking Device

Setup mode provides an interactive menu to help you to create an initial configuration file for a new networking device, or a device that you have erased the startup-config file from NVRAM. The nteractive menu guides you through initial configuration and is useful when you are unfamiliar with Cisco products or the command line interface (CLI) and when configuration changes do not require the level of detail the CLI provides. Setup mode can also be used to modify an existing configuration.

This section describes how to use the System Configuration Dialog to prepare a Cisco networking device for full configuration and how you can make configuration changes after an initial configuration is complete. To improve readability, filenames are enclosed in quotation marks. Also, the terms device and networking device mean a router, switch, or other device running Cisco IOS software. The terms initial configuration and startup configuration are used interchangeably.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Using Cisco IOS Setup Mode to Configure a Cisco Networking Device

- You have read the “Basic Configuration of a Cisco Networking Device Overview” module.
- An ASCII terminal is connected to the console port of the device being configured.
- You know the interfaces you want to configure.
- You know the routing protocols you want to enable.

For information about routing protocols, see the *Cisco IOS IP Routing Protocols Configuration Guide* , Release 12.4.

- You know whether the device you are configuring will perform bridging.
- You know whether the device you are configuring has protocol translation installed.
- You have network addresses for the protocols being configured.

For information about network addresses, see the *Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4.

- You have a password strategy for your network environment.

For information about passwords and device security, see “Configuring Security with Passwords, Privilege Levels, and Login User names for CLI Sessions on Networking Devices” module in the *Cisco IOS Security Configuration Guide*, Release 12.4.

- You have or have access to documentation for the product you want to configure.

Restrictions for Using Cisco IOS Setup Mode to Configure a Cisco Networking Device

- Setup mode is hardware dependent. You must follow instructions for the specific product you want to configure, as described in documentation for that product.
- Some configuration parameters apply only when a networking device has the protocol translation option. If a device does not have protocol translation, Setup does not prompt for these parameters.

Information About Using Cisco IOS Setup Mode to Configure a Cisco Networking Device

Cisco IOS Setup Mode

Cisco IOS Setup mode enables you to build an initial configuration file using the Cisco IOS CLI or System Configuration Dialog. The dialog guides you through initial configuration and is useful when you are unfamiliar with Cisco products or the CLI and when configuration changes do not require the level of detail the CLI provides.

Setup starts automatically when a device has no configuration file in NVRAM and is not preconfigured from the factory to use Cisco Router and Security Device Manager (SDM). When setup completes, it presents the System Configuration Dialog. This dialog guides you through an initial configuration with prompts for basic information about your device and network and then creates an initial configuration file. After the file is created, you can use the CLI to perform additional configuration.

Cisco Router and Security Device Manager

Cisco SDM is a web-based device management tool for configuring Cisco IOS network connections and security features on networking devices. SDM provides a default configuration and various wizards to guide you step by step through configuring a Cisco networking device, additional LAN or WAN connections, and VPN connections; creating firewalls; and performing security audits.

In addition to building an initial configuration, SDM provides an Advanced Mode through which you can configure advanced features such as Firewall Policy and Network Address Translation (NAT).

Some Cisco products ship from the factory with SDM installed. If SDM is preinstalled on your device and you want to use Setup to configure an initial configuration, you first must disable the SDM default configuration.

System Configuration Dialog

The *System Configuration Dialog* is an interactive CLI mode that prompts you for information needed to build an initial configuration for a Cisco networking device. Like the CLI, the System Configuration Dialog provides help text at each prompt. To access this help text, you enter a question mark (**?**) at the prompt.

The prompts in the System Configuration Dialog vary depending on hardware, installed interface modules, and software image. To use the dialog for an initial configuration, you need to refer to product-specific documentation.

The values shown in square brackets next to prompts reflect the current settings. These may be default settings from the factory or the latest settings configured on the device. To accept these settings, you press **Enter** on the keyboard.

You can exit (**Ctrl-C**) the System Configuration Dialog and return to privileged EXEC mode without making changes and without going through the entire dialog. If you exit the dialog but want to continue with setup, you can issue the **setup** command in privileged EXEC mode.

When you complete all the steps in the dialog, the device displays the modified configuration file and asks if you want to use that file. You must answer yes or no; there is no default for this prompt. If you answer yes, the file is saved to NVRAM as the startup configuration. If you answer no, the file is not saved and you must start at the beginning of the dialog if you want to build another initial configuration.

In addition to being a quick and easy way to perform an initial configuration, the System Configuration Dialog also is useful for performing basic configuration changes after an initial configuration has been performed.

Benefits of Using Cisco IOS Setup Mode

The System Configuration Dialog in Cisco IOS Setup mode can be a valuable tool for users who are unfamiliar with Cisco products or the CLI. The dialog guides users through the configuration process with prompts for basic information to get the device operational. When general configuration changes are needed, the dialog also is an alternative method to the detail-level CLI.

How to Use Cisco IOS Setup Mode to Configure a Cisco Networking Device and Make Configuration Changes

This section describes how to use the System Configuration Dialog to build an initial configuration file and to make configuration changes after a startup configuration has been loaded.

- Disabling the SDM Default Configuration File, page 28
- Using the System Configuration Dialog to Create an Initial Configuration File, page 29
- Using the System Configuration Dialog to Make Configuration Changes, page 33
- Verifying the Configuration, page 35
- Configuration Examples for Using Cisco IOS Setup Mode to Configure a Cisco Networking Device, page 38

Disabling the SDM Default Configuration File

Perform this task if SDM was preinstalled on your device and you want to use Setup to build an initial configuration file. SDM remains on the device.

Perform this task if SDM was pre installed on your device and you want to use AutoInstall to configure the device instead. SDM remains on the device.

SUMMARY STEPS

1. Connect the console cable, shipped with your device, from the console port on the device to a serial port on your PC. Refer to the hardware installation guide for the device for instructions.
2. Connect the power supply to the device, plug the power supply into a power outlet, and turn on the device. Refer to the quick start guide for the device for instructions.
3. Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:
4. **enable**
5. **erase startup-config**
6. **reload**

DETAILED STEPS

Step 1 Connect the console cable, shipped with your device, from the console port on the device to a serial port on your PC. Refer to the hardware installation guide for the device for instructions.

Step 2 Connect the power supply to the device, plug the power supply into a power outlet, and turn on the device. Refer to the quick start guide for the device for instructions.

Step 3 Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:

- 9600 baud
- 8 data bits, no parity, 1 stop bit
- No flow control

Step 4 **enable**
Enter privileged EXEC mode.

enable

Example:

```
Router> enable
Router#
```

Step 5 **erase startup-config**

Erases the existing configuration in NVRAM.

Example:

```
Router# erase startup-config
```

Step 6 **reload**

Initiates the reload process. The router will initiate the AutoInstall process after it finishes the reload process.

Example:

```
Router# reload
```

Using the System Configuration Dialog to Create an Initial Configuration File

Perform this task to create an initial configuration for a Cisco networking device.

If SDM is installed, you must disable its default configuration file before using Setup.

Note The System Configuration Dialog does not allow you to randomly select or enter parameters for configuration. You must move through the dialog step by step until the screen shows the information you want to change.

SUMMARY STEPS

1. **Power on the device.**
2. **Enter yes at the prompt to enter the initial configuration dialogue.**
3. **If you are prompted to continue with the configuration dialogue, enter yes** at**thepromptttocontinuethedialog(thisstepmightnotappear)**.
4. The basic management screen is displayed:
5. Enter a hostname for the device. This example uses Router.
6. Enter an enable secret password. This password is encrypted and cannot be seen when viewing the configuration.
7. Enter an enable password that is different from the enable secret password. An enable password is not encrypted and can be seen when viewing the configuration:
8. Enter a virtual terminal password. This password allows access to the device through only the console port.
9. Respond to the following prompts as appropriate for your network. In this example, the current setting [no] is accepted by pressing **Enter**.
10. Select an interface to connect the router to the management network:
11. Respond to the prompts as appropriate for your network. In this example, IP is configured: an IP address is entered and the current subnet mask is accepted. The screen displays the command script created.
12. Enter **2orpressEnter**to save the configuration file to NVRAM and exit.

DETAILED STEPS

Step 1 **Power on the device.**

Step 2 **Enter yes at the prompt to enter the initial configuration dialogue.**

If the following messages appear at the end of the startup sequence, the System Configuration Dialog was invoked automatically:

Example:

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: yes
```

The screen displays the following:

Example:

```
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
```

Step 3 **If you are prompted to continue with the configuration dialogue, enter yes** at**thepromptttocontinuethedialog(thisstepmightnotappear)**.

Example:

```
Continue with configuration dialog? [yes/no]: yes
```

Step 4 The basic management screen is displayed:

Example:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]:
```

Enter **yes** to enter basic management setup:

Example:

```
Would you like to enter basic management setup? [yes/no]: yes
The screen displays the following:
Configuring global parameters:
Enter host name [R1]:
```

Step 5 Enter a hostname for the device. This example uses Router.

Example:

```
Configuring global parameters:
Enter host name [R1]: Router
The screen displays the following:
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret:
```

Step 6 Enter an enable secret password. This password is encrypted and cannot be seen when viewing the configuration.

Example:

```
Enter enable secret: 1g2j3mm
```

The screen displays the following:

Example:

```
The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password:
```

Step 7 Enter an enable password that is different from the enable secret password. An enable password is not encrypted and can be seen when viewing the configuration:

Example:

```
  Enter enable password: cts54tnl
```

The screen displays the following:

Example:

```
The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password:
```

Step 8 Enter a virtual terminal password. This password allows access to the device through only the console port.

Example:

```
  Enter virtual terminal password: tls6gato
```

The screen displays the following:

Example:

```
Configure SNMP Network Management? [no]:
```

Step 9 Respond to the following prompts as appropriate for your network. In this example, the current setting [no] is accepted by pressing **Enter**.

Example:

```
Configure SNMP Network Management? [no]:
```

A summary of the available interfaces displays. The interface numbering that appears depends on the type of platform and on the installed interface modules and cards.

Example:

```
Current interface summary
Interface                  IP-Address      OK? Method Status                Prol
Ethernet0/0                unassigned      YES NVRAM  administratively down dow
Ethernet1/0                unassigned      YES NVRAM  administratively down dow
Serial2/0                  unassigned      YES NVRAM  administratively down dow
Serial3/0                  unassigned      YES NVRAM  administratively down dow
Loopback0                  1.1.1.1         YES NVRAM  up                    up
Enter interface name used to connect to the
management network from the above interface summary:
```

Step 10 Select an interface to connect the router to the management network:

Example:

```
Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0
```

Step 11 Respond to the prompts as appropriate for your network. In this example, IP is configured: an IP address is entered and the current subnet mask is accepted. The screen displays the command script created.

Example:

```
Configuring interface Ethernet0/0:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 172.17.1.1
    Subnet mask for this interface [255.255.0.0] :
    Class B network is 172.17.0.0, 16 subnet bits; mask is /16
The following configuration command script was created:
hostname Router
enable secret 5 $1$1Gg9$GuxXfUUBBfVqGvlW4psIm1
enable password cts54tnl
line vty 0 4
password tls6gato
no snmp-server
!
no ip routing
!
interface Ethernet0/0
no shutdown
ip address 172.17.1.1 255.255.0.0
!
interface Ethernet1/0
shutdown
no ip address
```

```
!
interface Serial2/0
shutdown
no ip address
!
interface Serial3/0
shutdown
no ip address
!
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:
```

Step 12 Enter **2orpressEnter**to save the configuration file to NVRAM and exit.

Example:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 2
```

The screen displays the following:

Example:

```
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
Router#
00:01:32: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:01:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed p
```

- What to Do Next, page 33

What to Do Next

Proceed to the “Verifying the Configuration” section.

Using the System Configuration Dialog to Make Configuration Changes

The *System Configuration Dialog* is an alternative to the CLI when configuration changes do not require the level of detail the CLI provides. For example, you can use the System Configuration Dialog to add a protocol suite, make addressing scheme changes, or configure a newly installed interface. Although you can use configuration modes available through the CLI to make these changes, the *System Configuration Dialog* provides you a high-level view of the configuration and guides you through the configuration process.

When you add or modify hardware and need to update a configuration, refer to documentation for your platform for details about physical and logical port assignments.

Note The System Configuration Dialog does not allow you to randomly select or enter parameters for configuration. You must move through the dialog step by step until the screen shows the information you want to change.

SUMMARY STEPS

1. **enable**
2. **setup**
3. **Follow Steps 3 through 12 in** the **Detailed Steps in the preceding "Using the System Configuration Dialog to Create an Initial Configuration File" section on page 5 .**
4. Verify the configuration is modified correctly. Refer to the "Verifying the Configuration" section.

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode.

Example:

```
Router> enable
Router#
```

Step 2 **setup**

The **setup** command puts the router in **setup** mode.

Example:

```
Router# setup
```

The screen displays the following:

Example:

```
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
```

Enter yes at**thepromptocontinuethedialog**.

Example:

```
Continue with configuration dialog? [yes/no]: yes

The screen displays the following:
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]:
```

Step 3 **Follow Steps 3 through 12 in** the **Detailed Steps in the preceding "Using the System Configuration Dialog to Create an Initial Configuration File" section on page 5 .**

Step 4 Verify the configuration is modified correctly. Refer to the "Verifying the Configuration" section.

Verifying the Configuration

Perform this task to verify that the configuration you created using the System Configuration Dialog is operating correctly.

SUMMARY STEPS

1. **show interfaces**
2. **show ip interface brief**
3. **show configuration**

DETAILED STEPS

Step 1 **show interfaces**
This command verifies that the interfaces are operating correctly and that they and the line protocol are in the correct state: up or down.

Step 2 **show ip interface brief**
This command displays a summary status of the interfaces configured for IP.

Step 3 **show configuration**
This command verifies that the correct hostname and password were configured.

Example

This example is the verification of the configuration file created in the “Using the System Configuration Dialog to Create an Initial Configuration File” section.

```
Router# show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc03.6c00 (bia aabb.cc03.6c00)
  Internet address is 172.17.1.1/16
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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 input packets with dribble condition detected
     11 packets output, 1648 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

```
Ethernet1/0 is administratively down, line protocol is down
  Hardware is AmdP2, address is aabb.cc03.6c01 (bia aabb.cc03.6c01)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  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
     1 carrier transitions     DCD=up  DSR=up  DTR=down  RTS=down  CTS=up
Serial3/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  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
     1 carrier transitions     DCD=down  DSR=down  DTR=up  RTS=up  CTS=down
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 1.1.1.1/32
  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
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  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
Router# show ip interface brief
Interface                  IP-Address      OK? Method Status                Prol
Ethernet0/0                172.17.1.1      YES manual up                    up
Ethernet1/0                unassigned      YES manual administratively down dow
Serial2/0                  unassigned      YES manual administratively down dow
Serial3/0                  unassigned      YES manual administratively down dow
Loopback0                  1.1.1.1         YES NVRAM  up                    up
Router# show configuration
Using 1029 out of 8192 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$1Gg9$GuxXfUUBBfVqGvlW4psIm1
enable password cts54tnl
!
no aaa new-model
!
resource manager
!
clock timezone PST -8
ip subnet-zero
no ip routing
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 no ip route-cache
!
interface Ethernet0/0
 ip address 172.17.1.1 255.255.0.0
 no ip route-cache
!
interface Ethernet1/0
 no ip address
 no ip route-cache
 shutdown
!
interface Serial2/0
 no ip address
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 no ip route-cache
 shutdown
 serial restart-delay 0
!
!
ip classless
no ip http server
!
!
!
!
control-plane
!
!
line con 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 password tls6gato
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

Configuration Examples for Using Cisco IOS Setup Mode to Configure a Cisco Networking Device

- Example Configuring Ethernet Interface 0 Using the System Configuration Dialog, page 38

Example Configuring Ethernet Interface 0 Using the System Configuration Dialog

In the following example, the System Configuration Dialog is used to configure Ethernet interface 0 with an IP address.

Note Prompts and the order in which they appear on the screen vary depending on the platform and the interfaces installed in the device.

```
R1# setup
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
  Enter host name [R1]: Router
  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: 1g2j3mmc
  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: cts54tnl
  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: tls6gato
  Configure SNMP Network Management? [no]:
Current interface summary
Interface                  IP-Address      OK? Method Status                Prol
Ethernet0/0                172.17.1.1      YES manual up                    up
Ethernet1/0                unassigned      YES manual administratively down dow
Serial2/0                  unassigned      YES manual administratively down dow
Serial3/0                  unassigned      YES manual administratively down dow
Loopback0                  1.1.1.1         YES NVRAM  up                    up
Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0
Configuring interface Ethernet0/0:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 172.17.1.1
    Subnet mask for this interface [255.255.0.0] :
    Class B network is 172.17.0.0, 16 subnet bits; mask is /16
The following configuration command script was created:
hostname Router
enable secret 5 $1$1Gg9$GuxXfUUBBfVqGvlW4psIm1
enable password cts54tnl
line vty 0 4
password tls6gato
no snmp-server
!
no ip routing
!
interface Ethernet0/0
no shutdown
ip address 172.17.1.1 255.255.0.0
!
interface Ethernet1/0
shutdown
no ip address
!
interface Serial2/0
shutdown
no ip address
!
interface Serial3/0
shutdown
no ip address
!
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
Router#
00:01:32: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:01:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed p
```

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Using AutoInstall to Remotely Configure Cisco Networking Devices

AutoInstall enables remote, automatic configuration of networking devices. AutoInstall is typically used to set up new networking devices remotely. You can, however, use AutoInstall to configure existing networking devices after you remove the configuration file from their NVRAM. The AutoInstall process uses preexisting configuration files that are stored on a TFTP server.

In this module the term networking device means a router that runs Cisco IOS software. Also, the following terms are used interchangeably:

- initial configuration and startup configuration
- *set up* and *configure*

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Using AutoInstall to Remotely Configure Cisco Networking Devices

- You have read Overview: Basic Configuration of a Cisco Networking Device module in the Cisco IOS Configuration Fundamentals Configuration Guide.
- This document is written specifically for networking devices running Cisco IOS Release 12.4(1) or newer. However most of the information in this document can be used to configure networking devices that support AutoInstall and are not running Cisco IOS release 12.4(1) or newer. The two key differences that you must allow for are:
    - Some Cisco networking devices use BOOTP instead of DHCP to request IP address addresses over LAN interfaces. Enabling BOOTP support on your DHCP server will resolve this issue.
    - Some Cisco networking devices use a DHCP client identifier format that is different from the format used by networking devices running Cisco IOS release 12.4(1) or newer. This document only explains the DHCP client identifier format used by networking devices running Cisco IOS release 12.4(1) or newer. Use the process described in Determining the Value for the DHCP Client Identifier Automatically to determine the DHCP client identifier format that your Cisco networking device is using.
- No configuration file resides in NVRAM on the networking device that is being configured with AutoInstall.
- The configuration files that you want to load on to the networking device using AutoInstall reside on a TFTP server that is connected to the network. In most cases there is more than one file; for example, a network file with the IP-to-hostname mappings and a device-specific configuration file.
- You have someone at the remote site to connect the networking device that is being configured with AutoInstall to the network and power it on.
- The network has the IP connectivity necessary to permit the networking device to load configuration files from the TFTP server during the AutoInstall process.
- A DHCP server is available on the network to provide IP addresses to networking devices that are using AutoInstall over a LAN connection.

Restrictions for Using AutoInstall to Remotely Configure Cisco Networking Devices

- (Serial interfaces only) AutoInstall over a serial interface using either HDLC or Frame Relay can be performed only over the first serial port on a new device (serial interface 0 or serial interface x/0).
- (LAN interfaces only) Only LAN Token Ring interfaces that set ring speed with physical jumpers support AutoInstall.
- AutoInstall does not automatically run on a T1 interface. For AutoInstall to work on a T1 interface, you have to manually configure the T1 interface to create a serial interface and then assign an IP address and network mask to that serial interface.

Information About Using AutoInstall to Remotely Configure Cisco Networking Devices

AutoInstall Overview

AutoInstall can be used to load a final full configuration, or a partial temporary configuration, on to a networking device that is being configured with AutoInstall.

Tip When you use AutoInstall to load a partial temporary configuration, you must finish configuring the device manually.

Services and Servers Used by AutoInstall Dynamic Assignment of IP Addresses

The network must be able to provide the dynamic assignment of an IP address to the networking device that is being configured with AutoInstall. The type of IP address assignment server that is used depends on the type of connection that the networking that is being configured with AutoInstall has to the network.

AutoInstall uses these types of IP address servers:

DHCP Servers

Networking devices using AutoInstall over a LAN connection require a DHCP server to provide an IP address dynamically. This requirement applies to Ethernet, Token Ring, and FDDI interfaces. The network must be configured to provide IP connectivity between the DHCP server and any devices that are using AutoInstall over LAN connections.

DHCP (defined in RFC 2131) is an extension of the functionality provided by the Bootstrap Protocol (defined in RFC 951). DHCP provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options such as a router (gateway) IP address, a TFTP server IP address, the name of a boot file to load, and the domain name to use. DHCP servers can be configured on routers, UNIX servers, Microsoft Windows-based servers, and other platforms.

DHCP servers typically assign IP addresses from a pool of IP addresses randomly. It is possible for a device that uses DHCP to obtain its IP address to have a different IP address every time it is connected to the network. This behavior creates a problem for the AutoInstall process when you want to ensure that a particular device is assigned a specific hostname during the AutoInstall process. For example, if you are installing routers on different floors in a remote site and each router is supposed to be assigned a name that indicates its location, such as **ChicagoHQ-1st** and **ChicagoHQ-2nd**, you need to ensure that each device gets the IP address that will be mapped to its correct hostname.

The process of ensuring that a device is assigned a specific IP address is referred to as *creating a reservation* . A reservation is a manually configured relationship between an IP address and a physical layer address of a LAN interface on the device. Many Cisco IOS-based devices do not use their MAC address when they request an IP address via DHCP. They use a much longer client identifier instead. Due to the complexity of identifying the client identifier so that you can preconfigure a reservation, and the complexity of finding out if the new device uses its MAC address or the client identifier, we recommend that you allow a new device to obtain an IP address without using a DHCP reservation first in order to discover if the device is using its MAC address or a client identifier. When you have learned how the new device is identifying itself to the DHCP server, you can make a note of the format and create a reservation for it. The next time the new device is rebooted it should obtain the IP address that you reserved to ensure that the new device is assigned the correct hostname. Refer to the information on creating DHCP reservations that was provided with your DHCP server software. The process for creating reservations using Cisco IOS based DHCP servers is explained in the Using AutoInstall to Set Up Devices Connected to LANs section. This section includes instructions for identifying the client identifier before the device is connected to the network so that you can preconfigure the DHCP reservations.

Note This document uses a Cisco router as the DHCP server for using AutoInstall to configure LAN-connected networking devices. If you are using a different device as your DHCP server ensure that you have the user documentation for it available in the event that you need help configuring it.

Note There are several configuration parameters such as TFTP server addresses, DNS server addresses, domain names and so on, that can be provided to LAN-connected clients by DHCP servers during the process of assigning IP addresses to clients. These parameters are not required by AutoInstall, therefore they are not included in this document. If you know how to use these parameters, you can include them in your DHCP server configuration when you are using AutoInstall to set up your networking devices.

For more information on DHCP services visit the IETF RFC site (http://www.ietf.org/rfc.html) and look for RFCs about DHCP. Most server operating systems support DHCP servers. Refer to the documentation that was provided with your operating system for more information.

SLARP Servers

A router that is being configured with AutoInstall over a serial interface using HDLC encapsulation will send a Serial Line ARP (SLARP) request for an IP address over the serial interface that is connected to the staging router.

The serial interface of the staging router must be configured with an IP address in which the host portion is 1 or 2, such as 192.168.10.1 or 192.168.10.2. The staging router will send a SLARP response to the router that is being configured with AutoInstall that contains the value that the staging router is not using. For example, if the interface on the staging router that is connected to the router that is being configured with

AutoInstall is using 192.168.10.1 as its IP address, the staging router will send a SLARP response with a value of 192.168.10.2 to the router that is being configured with AutoInstall.

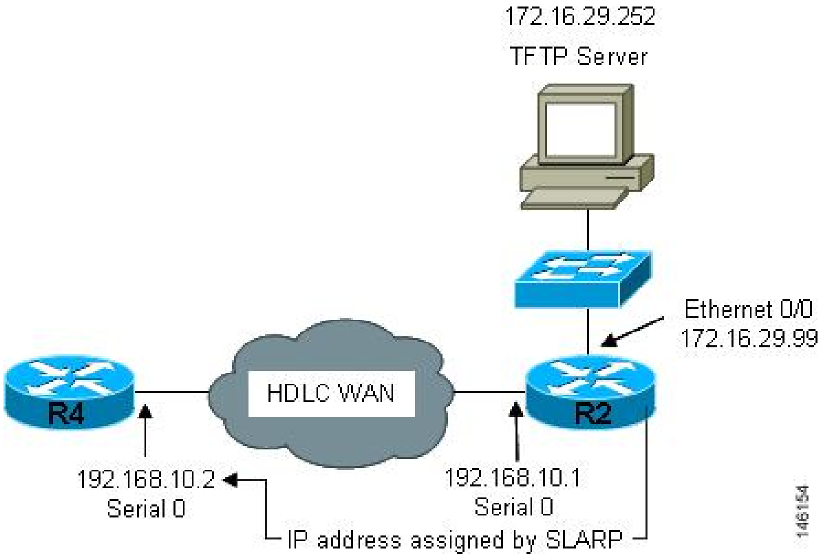
Tip

If you are using a mask of 255.255.255.252 on the serial interface of the staging router SLARP will assign the available IP host address to the new device. For example, if you assign IP address 198.162.10.5 255.255.255.252 to serial 0 on the staging router, SLARP will assign 198.162.10.6 to the new device. If you assign IP addresses 198.162.10.6 255.255.255.252 to serial 0 on the staging router SLARP will assign 198.162.10.5 to the new device.

The figure below shows an example of SLARP.

In the figure below, the IP address of serial interface 0 on the staging router (R2) is 192.168.10.1. SLARP therefore assigns the IP address 192.168.10.2 to serial interface 0 on the new device.

Figure 1: Using SLARP to Assign an IP Address to a New Device



Note

AutoInstall over a serial interface using HDLC can be performed only over the first serial port on a new device (serial interface 0 or serial interface x/0). The staging router and new device must be directly connected using the first serial interface port on the new device; for example, serial 0/0 or if the first serial port is in the second slot of the device, serial 2/0.

Tip

The IP address that is assigned to the router that is being configured with AutoInstall by SLARP from the staging router is the IP address that you must use in the **ip host** *hostname ip-address*command in the AutoInstall network-confg or cisconet.cfg file to ensure that the router that is being configured with AutoInstall is assigned the correct hostname so that it can request its host-specific configuration file.

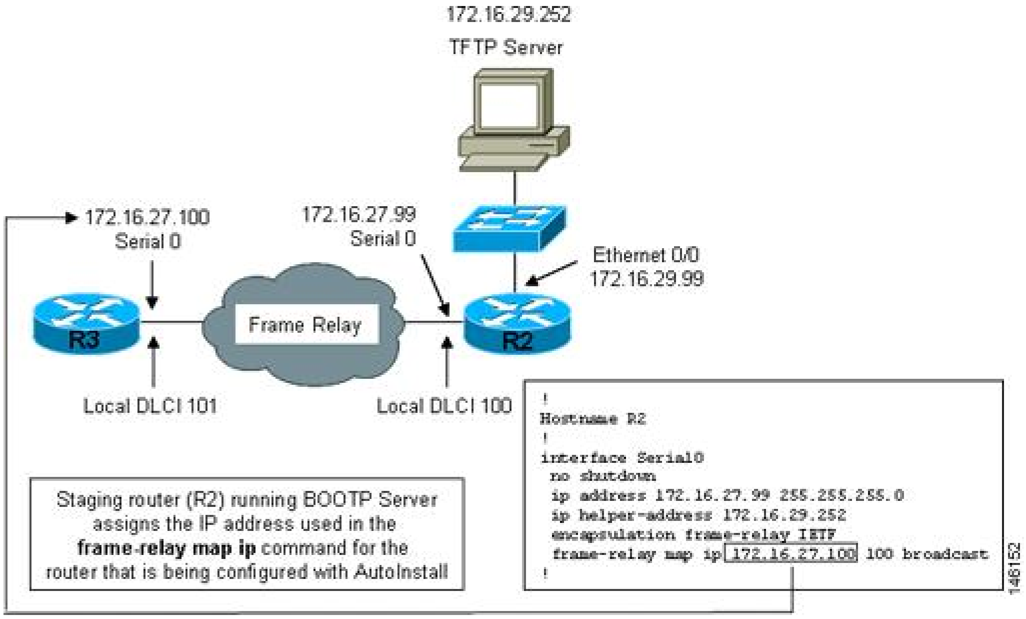
BOOTP Servers

A router that is being configured with AutoInstall over a serial interface using Frame Relay encapsulation will send a BOOTP request for an IP address over the serial interface that is connected to the staging router.

The staging router learns the correct IP address to provide in its BOOTP response to the router that is being configured with AutoInstall by examining the **frame-relay map ip** *ip-address dlci* command that is configured on the interface that it is using to connect to the router that is being configured with AutoInstall.

In the figure below R2 is the staging router. R2 has the **frame-relay map ip 172.16.27.100 100** broadcast command configured on interface serial 0. When R2 receives the BOOTP request for an IP address from R3 during the AutoInstall process, R3 will reply with 172.16.27.100.

Figure 2: Example of Using BOOTP for Autoinstall Over a Frame Relay Network


172.16.29.252
TFTP Server
172.16.27.100
Serial 0
172.16.27.99
Serial 0
Ethernet 0/0
172.16.29.99
Frame Relay
R3
R2
Local DLCI 101
Local DLCI 100
Staging router (R2) running BOOTP Server assigns the IP address used in the **frame-relay map ip** command for the router that is being configured with AutoInstall
146152

```
!
Hostname R2
!
interface Serial0
 no shutdown
 ip address 172.16.27.99 255.255.255.0
 ip helper-address 172.16.29.252
 encapsulation frame-relay IETF
 frame-relay map ip 172.16.27.100 100 broadcast
!
```

Tip

The limitation imposed by SLARP in which the IP addresses for the new device and the staging router must end in either .1 or .2 does not apply to BOOTP. BOOTP for AutoInstall over Frame Relay supports all host addresses for the IP address subnet that is assigned to the Frame Relay circuit between the router that is being configured with AutoInstall and the staging router.

Tip

The IP address that is assigned to the router that is being configured with AutoInstall by BOOTP from the staging router is the IP address that you must use in the **ip host** *hostname ip-address*command in the AutoInstall network-confg or cisconet.cfg file to ensure that the router that is being configured with AutoInstall is assigned the correct hostname so that it can request its host-specific configuration file.

Note AutoInstall over a serial interface using Frame Relay encapsulation can be performed only over the first serial port on a new device (serial interface 0 or serial interface x/0). The staging router and new device must be directly connected using the first serial interface port on the new device; for example, serial 0/0 or if the first serial port is in the second slot of the device, serial 2/0.

Services and Servers Used by AutoInstall IP-to-Hostname Mapping

If you want the networking device to load a full configuration file during the AutoInstall process, the networking device must be able to determine its hostname so that it can request the configuration file that you created specifically for it.

The following caveats apply to the provisioning of IP address to hostname mapping for AutoInstall:

- Any networking device that is being configured with AutoInstall can determine its hostname by loading one of the AutoInstall network configuration files (network-confg or cisconet.cfg) from the TFTP server that contain the **iphost***hostnameip-address* commands. For example, to map host R3 to IP address 198.162.100.3, the network-confg or cisconet.cfg file must contain the **iphostr3198.162.100.3** command.
- A networking device that is being configured with AutoInstall over a LAN interface can also determine its hostname by querying a DNS server. If the DNS server is not connected to the same LAN the device must learn the IP address of the DNS server from the DHCP server during the process of obtaining its dynamically assigned IP address from the DHCP server.

DNS Servers

DNS servers are used to provide a network service that maps hostnames to IP addresses and IP addresses to hostnames (reverse DNS lookups). Anytime that you use a hostname to initiate an IP connection to a host, your PC must determine the IP address that is assigned to the hostname that you want to contact. For example, when you visit Cisco’s website (http://www.cisco.com/) your PC sends a DNS query to a DNS server to discover the current IP address that can be used to contact Cisco’s website.

For more information on DNS services visit the IETF RFC site (http://www.ietf.org/rfc.html) and look for RFCs about DNS. The Name Server LookUp tool (nslookup) is very useful for learning more about DNS. There are several excellent websites available about nslookup that you can find by searching for them.

Services and Servers Used by AutoInstall Storage and Transmission of Configuration Files

TFTP is a protocol used to transfer files between devices on a network. A TFTP server is a device that uses TFTP to transfer files to devices. TFTP servers can be configured on UNIX servers, Microsoft Windows-based PCs and servers, and other platforms.

Tip If you do not have a TFTP server available you can configure a Cisco IOS-based router as a TFTP server using the **tftp-serverfile-system**:*filename* command. Refer to the Configuring Basic File Transfer Services feature for more information on configuring your router as a TFTP server.

Cisco routers use TFTP to load the configuration files that are required for AutoInstall. You must have a TFTP server deployed in your network to provide file storage and file transmission services to the devices that will be using AutoInstall.

For more information on TFTP services visit the IETF RFC site (http://www.ietf.org/rfc.html) and look for RFCs about TFTP. There are several excellent websites available about TFTP that you can find by searching for them. Several freeware and shareware versions of TFTP servers for various operating systems and hardware platforms are available from the Internet.

The following caveats apply to the provisioning of TFTP servers for AutoInstall:

- Devices using AutoInstall over a LAN--If the TFTP server and the devices using AutoInstall are on different LAN segments, you must either configure the **iphelper-address***address* command on all of the interfaces that will receive TFTP session initialization requests from the devices that are using AutoInstall.
- Devices using AutoInstall over a WAN--If the devices using AutoInstall are connected to a WAN, you must configure the **iphelper-address***address* command on all of the interfaces that will receive TFTP session initialization requests from devices that are using AutoInstall.

ip helper-address

If the new device does not learn the IP address of the TFTP server via DHCP option 150, it will transmit the TFTP session initialization requests as network layer broadcasts using the IP destination broadcast address of 255.255.255.255. Routers block network layer broadcast datagrams which prevents the TFTP session initialization requests from reaching the TFTP server, and AutoInstall will fail. The solution to this problem is to use the **iphelper-address***address* command. The **iphelper-address***address* command changes the broadcast address of TFTP session initialization request from 255.255.255.255 to the address that is configured with the *address* argument. For example, the **iphelper-address172.16.29.252** command will change IP destination broadcast address of 255.255.255.255 to 172.16.29.252.

Networking Devices Used by AutoInstall

Device That Is Being Configured with AutoInstall

A device that is being configured with AutoInstall can be any Cisco IOS-based router that supports AutoInstall and does not have a configuration file in its NVRAM.

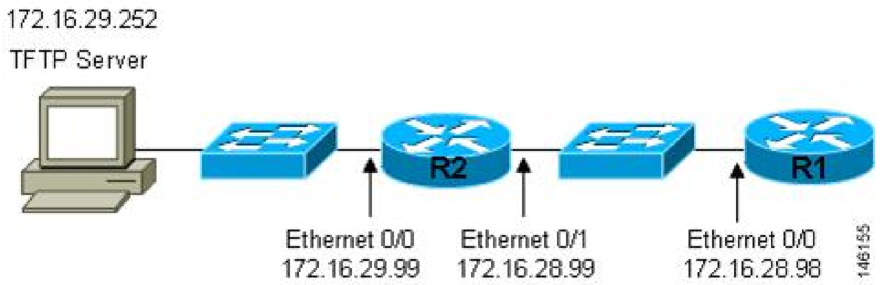
Staging Router

A staging router acts as an intermediary between the TFTP server (to which it must have IP connectivity) and a device that is being configured with AutoInstall when the new device and the TFTP server are connected to different networks. In the figure below R1 requires a staging router because it is connected to a different LAN segment than the TFTP server.

Staging routers are required in the following situations:

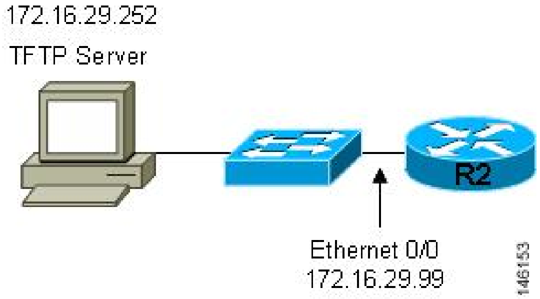
- Devices using AutoInstall over a LAN--If the TFTP and/or DHCP servers and the devices using AutoInstall are on different LAN segments you must use a staging router.
- Devices using AutoInstall over a WAN--If the devices using AutoInstall are connected to a WAN, you must configure the **ip helper-address** *address* command on all of the directly connected interfaces that will receive TFTP session initialization requests from the devices that are using AutoInstall.

Figure 3: Example of AutoInstall That Requires a Staging Router



Staging routers are not required when the new device that is being configured with AutoInstall is connected to the same LAN segment as the TFTP and DHCP servers. In the figure below R2 does not require a staging server to use AutoInstall because it is on the same LAN segment as the TFTP server.

Figure 4: Example of AutoInstall That Does Not Require a Staging Router



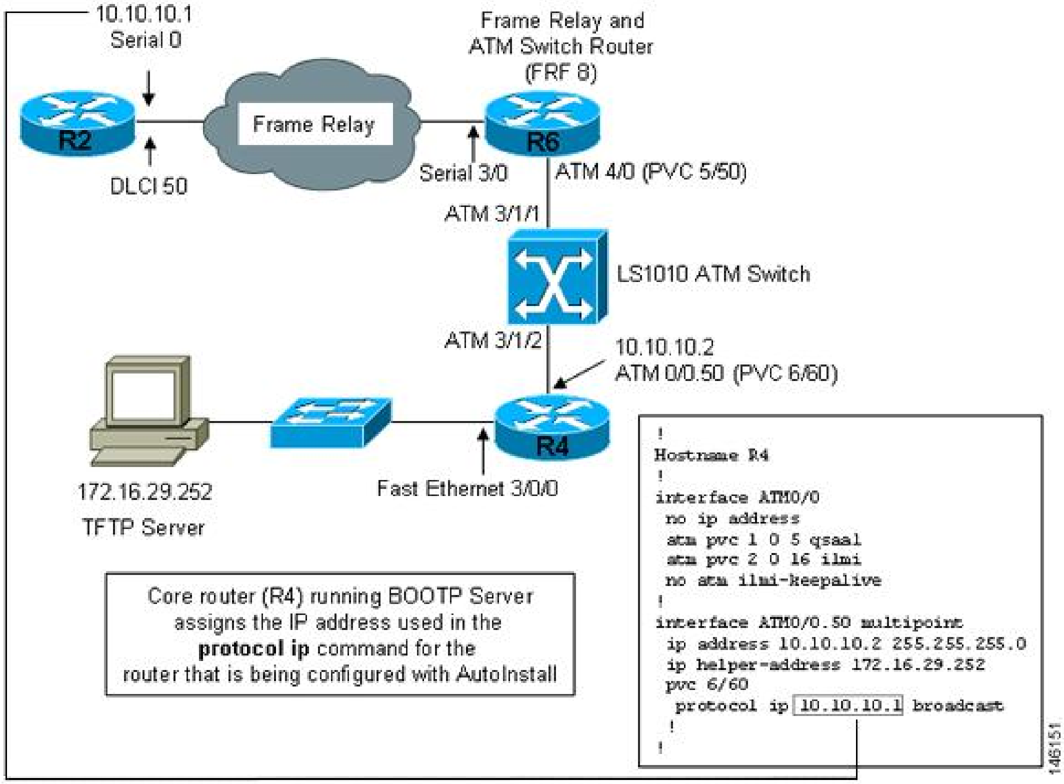
Intermediate Frame Relay-ATM Switching Device

An intermediate Frame Relay-ATM switching device is one that can perform both routing and switching operations. Frame Relay-ATM switching devices are used to connect Frame Relay and ATM networks.

The AutoInstall over Frame Relay-ATM Interworking Connections feature modifies the AutoInstall process to use Frame Relay encapsulation defined by the IETF standard instead of the Frame Relay encapsulation defined by Cisco.

The figure below shows an example topology using AutoInstall over Frame Relay-ATM Interworking Connections. Router R6 does the Frame Relay to ATM Service Internetworking (FRF8) conversion for Frame Relay DLCI 50 to ATM VPI/VCI 5/50. The LS1010 switch routes the VPI/VCI combination used by R6 (5/50) to the VPI/VCI combination used by R4 (6/60).

Figure 5: Example Topology for AutoInstall over Frame Relay-ATM Interworking Connections



Core router (R4) running BOOTP Server assigns the IP address used in the **protocol ip** command for the router that is being configured with AutoInstall

```
!
Hostname R4
!
interface ATM0/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 no atm ilmi-keepalive
!
interface ATM0/0.50 multipoint
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 172.16.29.252
 pvc 6/60
  protocol ip 10.10.10.1 broadcast
  !
!
```

Configuration Files Used by AutoInstall

A configuration file executes predefined commands and settings that enable a device to function in a network. The type of configuration file you choose determines many aspects of how you set up the network for AutoInstall.

Network Configuration File

The network configuration file is the first file that the AutoInstall process attempts to use. After the device has obtained an IP address it will try to discover its hostname by attempting to download a network configuration file that contains IP address to host name mappings.

If you want the device to learn its hostname from the network-confg file so that it can download a host-specific configuration file, you must add an entry for the device in the network-confg network configuration file. The syntax for the entry is **iphost***hostnameip-address* where *hostname* is the name that you want the host to use and *ip-address* is the address that the host will receive from the IP address server. For example, if you want the new device to use the name Australia, and the IP address that was dynamically assigned the new device is 172.16.29.103, you need to create an entry in the network configuration file that contains the **iphostaustralia172.16.29.103**command.

The file names used for the network configuration file are network-confg or cisconet.cfg. Routers running AutoInstall will try to load the network-confg from the TFTP server first. If the network-confg is not found on the TFTP server, the AutoInstall process will attempt to load the cisconet.cfg file. The cisconet.cfg filename was used by DOS-based TFTP servers that only supported the old 8.3 file naming convention. We recommend that you use the network-confg filename to avoid the delay that is created when AutoInstall has to timeout attempting to load the network-confg before it attempts to load the cisconet.cfg file.

If you use AutoInstall to set up multiple devices, you can create one network configuration file that contains an entry for each of the devices.

Host-Specific Configuration File

Host-specific configuration files are a full configuration for each new device. If you decide to use host-specific files, you must create a separate file for each new device that you are using AutoInstall to set up.

The filenames used for the host-specific configuration files are *name-confg* or *name.cfg* where the word name is replaced by the hostname of the router. For example, the filename for a router named hqrouter is hqrouter-confg or hqrouter.cfg.

Routers running AutoInstall will try to load the host-specific configuration filename using the format *name-confg* from the TFTP server first. If the *name-confg* file is not found on the TFTP server, the AutoInstall process will attempt to load the *name.cfg* file. The *name.cfg* file name format was used by DOS based TFTP servers that only supported the old 8.3 file naming convention. We recommend that you use the *name-confg* filename to avoid the delay that is created when AutoInstall has to timeout attempting to load the *name-confg* before it attempts to load the *name.cfg* file.

Tip If you use the *name.cfg* format for host-specific configuration files the filenames for hostnames that are longer than 8 characters must be truncated to the first eight characters. For example, the filename for a device with the hostname australia must be truncated to australi.cfg. When AutoInstall maps the IP address assigned to the new router to its hostname of australia in the network configuration file, AutoInstall will attempt to download a host-specific file with the name australi.cfg after it fails to load the host-specific filename austrailia-confg.

Tip Cisco recommends that you use the host-specific file option for setting up new devices to ensure that each new device is set up properly.

Default Configuration File (Optional)

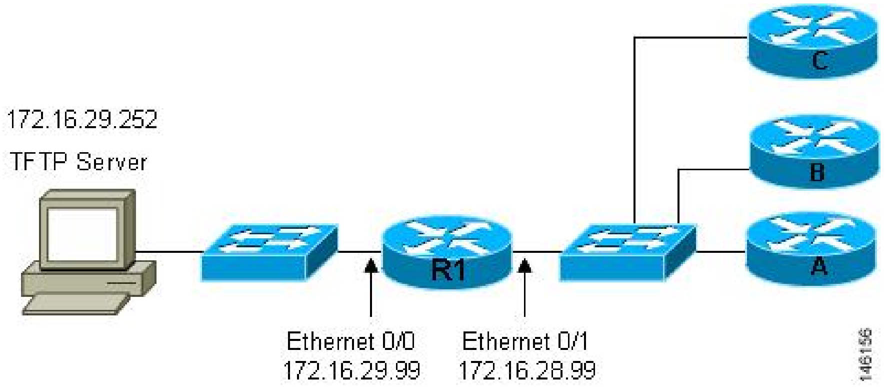
A default configuration file, which includes minimum configuration information allows you to telnet to the new device and configure it manually.

Tip If the new device has learned its hostname after it loaded the network configuration file the default configuration file is not used. You must use the host-specific file instead to configure features such as passwords for remote CLI sessions.

The figure below is an example of using the default configuration file to stage new routers for remote manual configuration. Routers A, B, and C are new routers that will be added to the network one at a time. You connect the first router and wait for it to load the default configuration file. The default configuration file must have enough information in it to allow the new router to communicate with the PC that you will be using to finish its configuration using a Telnet session. After the default configuration file is loaded on the new router, you can use Telnet to connect to the router to complete its configuration. You must assign a new, unique IP address to its interfaces so that the default configuration file can be used for configuring the next router.

Caution Failure to change the IP addresses in the router that you are configuring remotely with Telnet will result in duplicate IP addresses on the LAN when the next router loads the default configuration file. In this situation you will not be able to use Telnet to connect to either router. You must disconnect one of the routers before you can resolve this problem.

Figure 6: Example of Using the Default Configuration File To Stage Routers For Remote Manual Configuration



Tip You must include the commands for configuring passwords for remote Telnet access and access to privileged EXEC mode if you are going to access the routers remotely to complete their configurations save their configuration files to NVRAM.

The filenames used for the default network configuration file are router-confg or router.cfg. Routers running AutoInstall will try to load the router-confg from the TFTP server first. If the router-confg is not found on the TFTP server the AutoInstall process will attempt to load the router.cfg file. The router.cfg file name was used by DOS-based TFTP servers that only supported the old 8.3 file naming convention. We recommend that you use the router-confg filename to avoid the delay that is created when AutoInstall has to timeout while attempting to load the router-confg before it attempts to load the router.cfg file.

If you are using AutoInstall to configure LAN-attached devices, you can specify a different default boot filename in DHCP Option 067.

Configuration Options for AutoInstall

You can provision your network to support AutoInstall using several different combinations of devices and services. For example:

- You can provision all of the services required for AutoInstall (except dynamic IP address assignment using SLARP or BOOTP that must be preformed by a Cisco router) on one network server, or you can provision each service on a different network server.
- You can provision the DHCP service on a Cisco router.
- The device using AutoInstall can determine its IP address from a DNS server, or you can use one of the AutoInstall network configuration files (network-confg or cisconet.cfg) that contain the **iphost***hostnameip-address* commands.
- You can use provision AutoInstall to load a full configuration or a partial configuration onto a device that is using AutoInstall.

This module focuses on some of the most common methods for provisioning AutoInstall. Refer to the How to Use AutoInstall to Remotely Configure Cisco Networking Devices for information on the most common methods for provisioning AutoInstall.

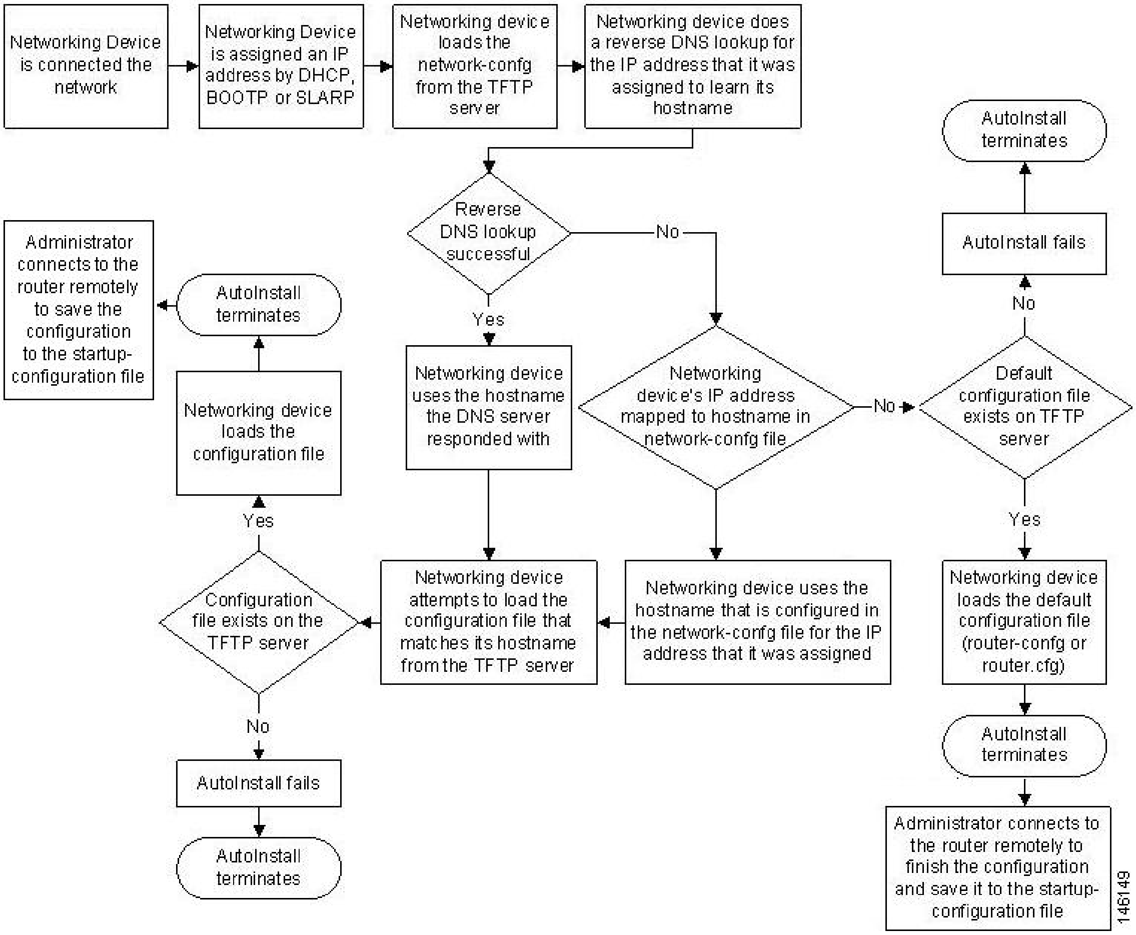
The AutoInstall Process

The AutoInstall process begins when a networking device that does not have any files in its NVRAM is connected to the network.

Timesaver You can decrease the time that the AutoInstall process takes to complete by only connecting the interface on the networking device that you want to use for AutoInstall until the AutoInstall process has finished. For example, if you want the networking device to perform AutoInstall over a WAN interface and you connect its LAN interfaces and its WAN interfaces the networking device will attempt to perform AutoInstall over the LAN interfaces before it attempts to use the WAN interfaces. Leaving the LAN interfaces disconnected until the AutoInstall process is finished causes the networking device to initiate the AutoInstall process over its WAN interface immediately.

The following figure shows the basic flow of the AutoInstall process.

Figure 7: AutoInstall Process Flowchart


Networking Device is connected the network
Networking Device is assigned an IP address by DHCP, BOOTP or SLARP
Networking device loads the network-confg from the TFTP server
Networking device does a reverse DNS lookup for the IP address that it was assigned to learn its hostname
AutoInstall terminates
Reverse DNS lookup successful
No
AutoInstall fails
Administrator connects to the router remotely to save the configuration to the startup-configuration file
AutoInstall terminates
Yes
No
Networking device loads the configuration file
Networking device uses the hostname the DNS server responded with
Networking device's IP address mapped to hostname in network-confg file
No
Default configuration file exists on TFTP server
Yes
Yes
Configuration file exists on the TFTP server
Networking device attempts to load the configuration file that matches its hostname from the TFTP server
Networking device uses the hostname that is configured in the network-confg file for the IP address that it was assigned
Networking device loads the default configuration file (router-confg or router.cfg)
No
AutoInstall terminates
AutoInstall fails
AutoInstall terminates
Administrator connects to the router remotely to finish the configuration and save it to the startup-configuration file
146149

Benefits of Using AutoInstall to Remotely Configure a Cisco Networking Device

AutoInstall facilitates the deployment of Cisco routers by allowing you to manage the setup procedure for routers from a central location. The person responsible for physically installing the router does not require specific networking skills. The ability to physically install the router, connect the power and networking cables, and power it on are the only skills required by the installer. The configuration files are stored and managed on a central TFTP server. By using AutoInstall one skilled network technician based at a central site can manage the deployment of several routers in a short period of time.

- AutoInstall Using DHCP for LAN Interfaces, page 54
- AutoInstall over Frame Relay-ATM Interworking Connections, page 54

AutoInstall Using DHCP for LAN Interfaces

The AutoInstall Using DHCP for LAN Interfaces feature enhances the benefits of AutoInstall by replacing the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces (specifically Ethernet, Token Ring, and FDDI interfaces).

DHCP (defined in RFC 2131) is an extension of the functionality provided by the BOOTP (defined in RFC 951). DHCP provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options. In Cisco IOS Release 12.1(5)T, and later releases, the IP address procurement phase of the AutoInstall process is now accomplished using DHCP for Ethernet, Token Ring, and FDDI interfaces. Prior to this release, IP addresses for LAN interfaces were obtained using BOOTP or RARP during the AutoInstall process. Additionally, this feature allows for the uploading of configuration files using unicast TFTP.

AutoInstall over Frame Relay-ATM Interworking Connections

The AutoInstall over Frame Relay-ATM Interworking Connections feature further enhances the benefits of AutoInstall by allowing you to use a router with an ATM interface as a BOOTP server for new routers being connected at remote locations.

How to Use AutoInstall to Remotely Configure Cisco Networking Devices

This section describes the how to prepare a router for AutoInstall, how to use AutoInstall with Frame Relay to ATM Service Internetworking, and how to use AutoInstall for new routers connected to LANs. Additional examples for using AutoInstall for new routers connected to LANs, HDLC WANs, and Frame Relay networks that do not use Frame Relay to ATM Service Internetworking, are provided in the Configuration Examples for Using AutoInstall to Remotely Configure Cisco Networking Devices section.

In most cases you need to configure a staging router through which a new device running AutoInstall sends TFTP, BOOTP, and DNS requests.

Tip In all cases, you must verify and save the configuration on the networking device after the AutoInstall process is complete. If you do not save the configuration, you must repeat the entire process.

- Disabling the SDM Default Configuration File, page 55
- Using AutoInstall with Frame Relay to ATM Service Internetworking Example, page 56
- Using AutoInstall to Set Up Devices Connected to LANs Example, page 70

Disabling the SDM Default Configuration File

Perform this task if Security Device Manager (SDM) was preinstalled on your device and you want to use AutoInstall to configure the device instead. SDM remains on the device.

SUMMARY STEPS

1. Connect the console cable, shipped with your device, from the console port on the device to a serial port on your PC. Refer to the hardware installation guide for the device for instructions.
2. Connect the power supply to the device, plug the power supply into a power outlet, and turn on the device. Refer to the quick start guide for the device for instructions.
3. Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:
4. **enable**
5. **erase startup-config**
6. **reload**

DETAILED STEPS

Step 1 Connect the console cable, shipped with your device, from the console port on the device to a serial port on your PC. Refer to the hardware installation guide for the device for instructions.

Step 2 Connect the power supply to the device, plug the power supply into a power outlet, and turn on the device. Refer to the quick start guide for the device for instructions.

Step 3 Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:

- 9600 baud
- 8 data bits, no parity, 1 stop bit
- No flow control

Step 4 **enable**
Enter privileged EXEC mode.

enable

Example:

```
Router> enable
Router#
```

Step 5 **erase startup-config**
Erases the existing configuration in NVRAM.

Example:

```
Router# erase startup-config
```

Step 6 **reload**

Initiates the reload process. The router will initiate the AutoInstall process after it finishes the reload process.

Example:

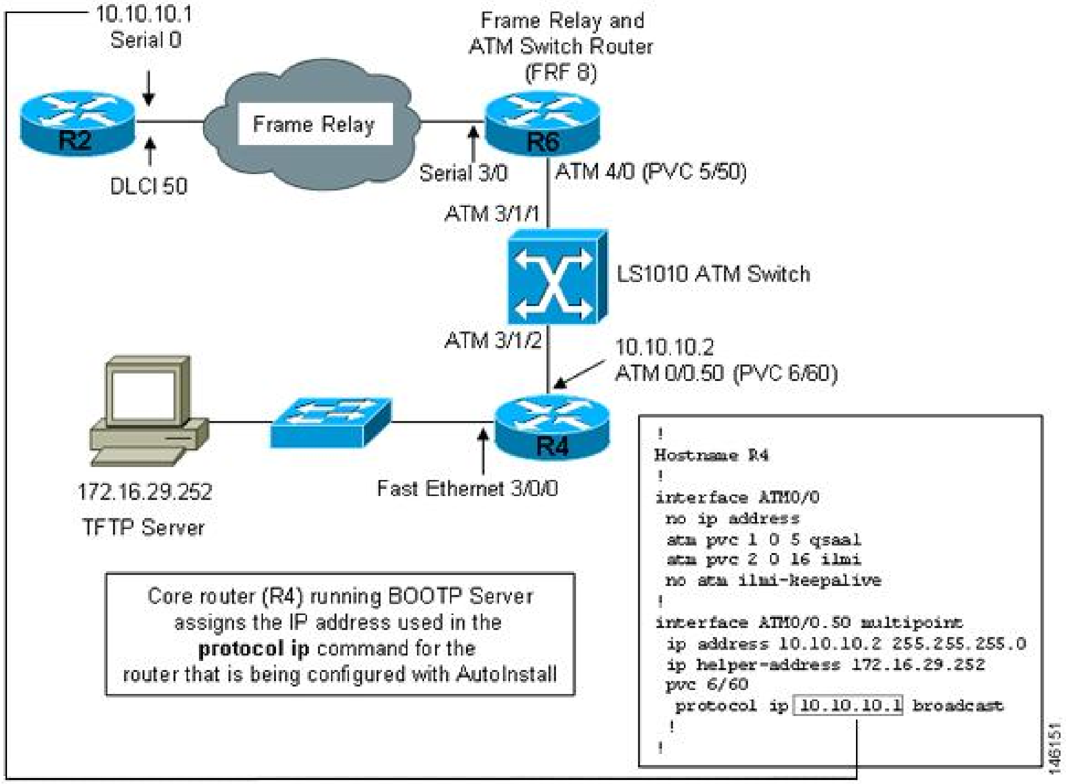
```
Router# reload
```

Using AutoInstall with Frame Relay to ATM Service Internetworking Example

Refer to the figure below for the sample network used in this task. Perform this task to configure routers R6, R4, and the LS1010 ATM switch so that AutoInstall can be used with Frame Relay to ATM Service Internetworking (FRF8) to set up router R2.

Note The IP address that will be assigned to Serial 0 on R2 (10.10.10.1/24) during and after the AutoInstall process and the IP address that is assigned to ATM 0/0.50 on R4 (10.10.10.2/24) are on the same subnet (10.10.10.0/24). Using IP addresses on the same subnet is required because the interfaces on R6 and the LS10101 switch are switching the IP packets between R2 and R4 at Layer 2.

Figure 8: Example Topology for AutoInstall over Frame Relay/ATM Interworking Connections



```
!
Hostname R4
!
interface ATM0/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 no atm ilmi-keepalive
!
interface ATM0/0.50 multipoint
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 172.16.29.252
 pvc 6/60
  protocol ip 10.10.10.1 broadcast
  !
!
```

Configuring R6 for Frame Relay to ATM Service Internetworking

Router R6 does the Frame Relay to ATM Service Internetworking (FRF8) conversion for Frame Relay DLCI 50 to ATM VPI/VCI 5/50.

Note The serial interface and the ATM interface on R6 that are used for ATM Service Internetworking (FRF8) do not have IP addresses because they are used as Layer 2 switching interfaces in this configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **interface serial** *interface-number*
5. **no ip address**
6. **encapsulation frame-relay ietf**
7. **frame-relay interface-dlci** *dlci* **switched**
8. exit
9. **frame-relay lmi-type ansi**
10. **frame-relay intf-type dce**
11. **exit**
12. **interface atm** *interface-number*
13. **no ip address**
14. **pvc** *vpi* / *vci* **qsaal**
15. **pvc** *vpi* / *vci* **ilmi**
16. **no atm ilmi-keepalive**
17. **pvc** *vpi* / *vci*
18. **encapsulation aal5mux fr-atm-srv**
19. **exit**
20. **exit**
21. **connect** *name* **serial** *slot* / *port dlci* **atm** *slot* / *port vpi* / *vci* **service-interworking**
22. **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	**hostname** *hostname* **Example:** `Router(config)# hostname R6`	Changes the name of the host (router) to R6.

	Command or Action	Purpose
Step 4	**interface serial** *interface-number* **Example:** `R6(config)# interface serial 3/0`	Specifies the serial interface that connects to the router that is being set up with AutoInstall and enters interface configuration mode.
Step 5	**no ip address** **Example:** `R6(config-if)# no ip address`	Removes an existing IP address. **Note** This interface is used as a layer 2 switch interface in this configuration. It is not an IP layer 3 endpoint. Therefore it does not require an IP address.
Step 6	**encapsulation frame-relay ietf** **Example:** `R6(config-if)# encapsulation frame-relay IETF`	Enables and specifies the Frame Relay encapsulation method. **Note** Only the Frame Relay commands and keywords required for this task are described in this task. For more information on the other Frame Relay commands and keywords, refer to the Cisco IOS Wide-Area Networking Command Reference.
Step 7	**frame-relay interface-dlci** *dlci* **switched** **Example:** `R6(config-if)# frame-relay interface-dlci 50 switched`	Specifies that the Frame Relay data-link connection identifier (DLCI) is switched and enters Frame Relay DLCI configuration mode.
Step 8	exit **Example:** `R6(config-fr-dlci)# exit`	Exits Frame Relay DLCI configuration mode and enters interface configuration mode.
Step 9	**frame-relay lmi-type ansi** **Example:** `Router(config-if)# frame-relay lmi-type ansi`	Specifies that the router should use Annex D defined by American National Standards Institute (ANSI) standard T1.617 as the LMI type.
Step 10	**frame-relay intf-type dce** **Example:** `R6(config-if)# frame-relay intf-type dce`	Specifies that the router functions as a switch connected to a router.
Step 11	**exit** **Example:** `R6(config-if)# exit`	Returns to global configuration mode.
Step 12	**interface atm** *interface-number* **Example:** `R6(config)# interface ATM4/0`	Specifies the ATM interface and enters interface configuration mode.

	Command or Action	Purpose
		Note Only the ATM commands and keywords required for this task are described in this task. For more information on the other Frame Relay commands and keywords refer to the Cisco IOS Asynchronous Transfer Mode Command Reference.
Step 13	**no ip address** **Example:** `R6(config-if)# no ip address`	Removes an existing IP address. **Note** This interface is used as a layer 2 switch interface in this configuration. It is not an IP layer 3 endpoint. Therefore it does not require an IP address.
Step 14	**pvc** *vpi* / *vci* **qsaal** **Example:** `R6(config-if)# pvc 0 5 qsaal`	Configures a PVC for QSAAL1 signaling.
Step 15	**pvc** *vpi* / *vci* **ilmi** **Example:** `R6(config-if)# pvc 0 16 ilmi`	Configures a PVC for ILMI signaling.
Step 16	**no atm ilmi-keepalive** **Example:** `R6(config-if)# no atm ilmi-keepalive`	Disables ATM ILMI keep alives.
Step 17	**pvc** *vpi* / *vci* **Example:** `R6(config-if)# pvc 5/50`	Configures the PVC. When configuring PVCs, configure the lowest available VPI and VCI numbers first and enters interface ATM VC configuration mode. **Note** VCIs 0 to 31 on all VPIs are reserved.
Step 18	**encapsulation aal5mux fr-atm-srv** **Example:** `R6(config-if-atm-vc)# encapsulation aal5mux fr-atm-srv`	Enables the Frame Relay and ATM internetworking service.
Step 19	**exit** **Example:** `R6(config-if-atm-vc)# exit`	Exits interface ATM VC configuration mode and returns to interface configuration mode.
Step 20	**exit** **Example:** `R6(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 21	**connect** *name* **serial** *slot* / *port dlci* **atm** *slot* / *port vpi* / *vci* **service-interworking** **Example:** `R6(config)# connect r2 serial3/0 50 ATM4/0 5/50 service-interworking`	Creates the connection between the Frame Relay DLCI and the ATM PVC for the Frame Relay and ATM internetworking service and enters FRF .8 configuration mode.

Step 22	**end**
	Example:
	`R6(config-frf8)# end`
		Returns to privileged EXEC mode.

Verifying Frame Relay to ATM Service Internetworking on R6

Use the **showconnectionnamer2** command to verify whether the Service Interworking Connection is up.

The output of the **showconnectionnamer2** command indicates that the Service Interworking Connection is up.

```
R6# show connection name r2
FR/ATM Service Interworking Connection: r2
  Status    - UP
  Segment 1 - Serial3/0 DLCI 50
  Segment 2 - ATM4/0 VPI 5 VCI 50
Interworking Parameters -
    service translation
    efci-bit 0
    de-bit map-clp
    clp-bit map-de
```

Configuring R4 for Frame Relay to ATM Service Internetworking

R4 is one of the endpoints for Frame Relay to ATM Service Internetworking in this task. R2 is the other endpoint. R4 is not directly connected to the Frame Relay network. Therefore R4 requires only the ATM commands to act as the endpoint for Frame Relay to ATM Service Internetworking.

R4 is the core router that connects to the LAN with the TFTP server. R4 is the BOOTP server that will provide the IP address required for R2 (10.10.10.1/24) when R2 runs AutoInstall.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **interface ethernet** *module* / *slot* / *port*
5. **ip address** *ip-address mask*
6. **exit**
7. **interface atm** *interface-number*
8. **no ip address**
9. **pvc** *vpi* / *vci* **qsaal**
10. **pvc** *vpi* / *vci* **ilmi**
11. **no atm ilmi-keepalive**
12. **exit**
13. **interface atm** *slot* / *port* .*subinterface-number***multipoint**
14. **ip address** *ip-address mask*
15. **ip helper-address** *ip-address*
16. **pvc** *vpi* / *vci*
17. **protocol ip** *ip-address* **broadcast**
18. **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	**hostname** *hostname* **Example:** `Router(config)# hostname R4`	Changes the name of the host (router) to R4.
Step 4	**interface ethernet** *module* / *slot* / *port* **Example:** `R4(config)# interface ethernet 3/0/0`	Species the Ethernet interface and enters interface configuration mode.

	Command or Action	Purpose
Step 5	**ip address** *ip-address mask* **Example:** `R4(config-if)# ip address 172.16.29.97 255.255.255.0`	Specifies the IP address for the interface.
Step 6	**exit** **Example:** `R4(config-if)# exit`	Returns to global configuration mode.
Step 7	**interface atm** *interface-number* **Example:** `R4(config)# interface atm0/0`	Species the ATM interface and enters interface configuration mode. **Note** Only the ATM commands and keywords required for this task are described in this task. For more information on the other Frame Relay commands and keywords, refer to the Cisco IOS Asynchronous Transfer Mode Command Reference.
Step 8	**no ip address** **Example:** `R4(config-if)# no ip address`	The main ATM interface does not require an IP address in this configuration. The IP address is assigned to the multipoint subinterface in Step 9.
Step 9	**pvc** *vpi* / *vci* **qsaal** **Example:** `R4(config-if)# pvc 0 5 qsaal`	Configures a PVC for QSAAL1 signaling.
Step 10	**pvc** *vpi* / *vci* **ilmi** **Example:** `R4(config-if)# pvc 0 16 ilmi`	Configures a PVC for ILMI signaling.
Step 11	**no atm ilmi-keepalive** **Example:** `R4(config-if)# no atm ilmi-keepalive`	Disables ATM ILMI keep alives.
Step 12	**exit** **Example:** `R4(config-if)# exit`	Returns to global configuration mode.
Step 13	**interface atm** *slot* / *port* .*subinterface-number***multipoint**	Creates the ATM multipoint virtual subinterface and enters subinterface configuration mode.

	Command or Action	Purpose
	Example: `R4(config-if)# interface atm0/0.50 multipoint`	
Step 14	**ip address** *ip-address mask* **Example:** `R4(config-subif)# ip address 10.10.10.2 255.255.255.0`	Specifies the IP address for the subinterface.
Step 15	**ip helper-address** *ip-address* **Example:** `R4(config-subif)# ip helper-address 172.16.29.252`	Specifies the IP address of the TFTP server. This IP address is used to replace the 255.255.255.255 IP destination broadcast address that R2 will use when it attempts to establish a connection to the TFTP server.
Step 16	**pvc** *vpi* / *vci* **Example:** `R4(config-subif)# pvc 6/60`	Configures the PVC. When configuring PVCs, configure the lowest available VPI and VCI numbers first and enters ATM VC configuration mode. **Note**VCIs 0 to 31 on all VPIs are reserved.
Step 17	**protocol ip** *ip-address* **broadcast** **Example:** `R4(config-if-atm-vc)# protocol ip 10.10.10.1 broadcast`	Specifies the IP address of the device at the other end of this PVC. In this example the device is R2. • For this example, this address is the IP address that will be assigned by the BOOTP server on R4 to R2 during the AutoInstall process.

Step 18	**end**
	Example:
	`R4(config-if-atm-vc)# end`
		Returns to privileged EXEC mode.

Configuring IP Routing R4

In order for R4 to be able to forward IP traffic between network 172.16.29.0 and R2 after the AutoInstall process is complete, R4 needs to have IP routing configured.

Note The configuration file for R2 provided in the Creating the Configuration File for R2 Example section includes the IP routing commands required to establish IP routing connectivity for R2 using RIP Version 2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router rip**
4. **version** *version*
5. **network** *ip-network*
6. Repeat Step 5 for the other IP networks.
7. **no auto-summary**
8. **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	**router rip** **Example:** `Router(config)# router rip`	Enables RIP routing on R4. **Note** Only the RIP commands and keywords required for this task are described in this task. For more information on the other RIP commands and keywords, refer to the Cisco IOS Routing Protocols Command Reference.
Step 4	**version** *version* **Example:** `Router(config-router)# version 2`	Specifies the version of RIP that the router will use.
Step 5	**network** *ip-network* **Example:** `Router(config-router)# network 172.16.0.0`	Specifies the IP networks for which RIP will provide routing services.
Step 6	Repeat Step 5 for the other IP networks. **Example:** `Router(config-router)# network 10.0.0.0`	--
Step 7	**no auto-summary**	Disables the default RIP V2 behavior of summarizing IP subnets in the routing advertisements.

	Command or Action	Purpose
	Example: `Router(config-router)# no auto-summary`	

Step 8	**end**
	Example:
	`Router(config-router)# end`
		Returns to privileged EXEC mode.

Configuring the LS1010 Switch

This task describes how to configure an LS1010 switch to route the PVCs between R6 and R4. R6 is connected to ATM 3/1/1 on the LS1010 switch. R4 is connected to ATM 3/1/2 on the LS1010 switch.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *module* / *slot* / *port*
4. **pvc** *vpi vci* **interface atm** *interface-number vpi vci*
5. **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 atm** *module* / *slot* / *port* **Example:** `Router(config)# interface ATM3/1/2`	Species the ATM interface and enters interface configuration mode. **Note** Only the LS1010 ATM commands and keywords required for this task are described in this task. For more information on the other ATM commands and keywords available on the LS1010, refer to the Lightstream 1010 ATM Switch Documents .
Step 4	**pvc** *vpi vci* **interface atm** *interface-number vpi vci*	Configures a static PVC route. • In this example, a route for the PVC from R6 (5/50) to R4 (6/60) is configured.

	Command or Action	Purpose
	Example: `Router(config-if)# pvc 6 60 interface ATM3/1/1 5 50`	

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Verifying AutoInstall with Frame Relay to ATM Service Internetworking

Perform this task to verify the AutoInstall with Frame Relay to ATM Service Internetworking configuration by setting up the topology shown in the Example Topology for AutoInstall over Frame Relay/ATM Interworking Connections figure, in the Using AutoInstall with Frame Relay to ATM Service Internetworking Example section.

The following prerequisites must be met before you can perform this task:

- You must have a TFTP server on the network with the IP address that you specified on R4 with the **iphelper-address***ip-address* command.
- You must have a configuration file for R2 named r2-confg on the TFTP server.
- You must have a network configuration named network-confg file with the **iphostr210.10.10.1** command in it on the TFTP server.
- You must have configured R6, R4 and the LS1010 ATM switch (or a functional equivalent of the ATM switch) following the instructions provided in the previous tasks in this section.
- R2 must not have a configuration file in NVRAM.

SUMMARY STEPS

1. Connect a console terminal to R2.
2. Power cycle, or power on R2.
3. When the prompt to enter the initial configuration dialog appears, answer no.
4. When the prompt to terminate AutoInstall appears answer no.
5. The AutoInstall process can take several minutes to complete. Do not press any keys on R2’s terminal session until AutoInstall has completed.
6. Copy the running configuration to the startup configuration with the **copyrunning-configstartup-config**command.

DETAILED STEPS

Step 1 Connect a console terminal to R2.
Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:

- 9600 baud
- 8 data bits, no parity, 1 stop bit

- No flow control

Step 2 Power cycle, or power on R2.

Step 3 When the prompt to enter the initial configuration dialog appears, answer no.

Example:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 4 When the prompt to terminate AutoInstall appears answer no.

Example:

```
Would you like to terminate autoinstall? [yes]: no
```

AutoInstall will start.

Example:

```
Please Wait. Autoinstall being attempted over Serial0 !!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Step 5 The AutoInstall process can take several minutes to complete. Do not press any keys on R2's terminal session until AutoInstall has completed.
This display output is from a successful Auto Installation process.

Note You can ignore the "%PARSER-4-BADCFG: Unexpected end of configuration file" error message. This problem does not adversely affect the AutoInstall process.

Note The last two lines with the %SYS-5-CONFIG_I messages indicate the network-confg and r2-confg files have been received successfully.

Example:

```
Press RETURN to get started!
*Mar  1 00:00:11.155: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
*Mar  1 00:00:11.159: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar  1 00:00:11.527: %LINK-3-UPDOWN: Interface Serial1, changed state to down
*Mar  1 00:00:12.271: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,changed state to up
*Mar  1 00:00:29.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to
down
*Mar  1 00:00:32.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
*Mar  1 00:00:40.355: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to
down
*Mar  1 00:00:45.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
*Mar  1 00:01:58.499: %IP-5-WEBINST_KILL: Terminating DNS process
*Mar  1 00:02:00.035: %LINK-5-CHANGED: Interface Ethernet0, changed state to administratively down
*Mar  1 00:02:00.039: %LINK-5-CHANGED: Interface Serial1, changed state to administratively down
*Mar  1 00:02:01.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to
down
*Mar  1 00:02:50.635: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(13a), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Tue 26-Apr-05 12:52 by ssearch
*Mar  1 00:02:50.643: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing
 a cold start
*Mar  1 00:03:54.759: %PARSER-4-BADCFG: Unexpected end of configuration file.
*Mar  1 00:03:54.763: %SYS-5-CONFIG_I: Configured from tftp://172.16.29.252/network-confg by
console
*Mar  1 00:04:12.747: %SYS-5-CONFIG_I: Configured from tftp://172.16.29.252/r2-confg by console
```

If you have logging enabled on your TFTP server the log should contain messages similar to the following text:

Example:

```
Sent network-config to (10.10.10.1), 76 bytes
Sent r2-confg to (10.10.10.1),687 bytes
```

Step 6 Copy the running configuration to the startup configuration with the **copyrunning-configstartup-config**command.

- Troubleshooting, page 69

Troubleshooting

If after approximately five minutes you do not see the %SYS-5-CONFIG_I messages and R2 has a factory default prompt of Router>, the AutoInstall process failed.

SUMMARY STEPS

1. Look for error messages on the TFTP server indicating that the files were not found. A very common mistake is that the .txt extension was added to the r2-confg file (r2-confg.txt) by your text editor. Your operating system might be hiding the extension for known file types when you browse the TFTP root directory. Disable the **Hidefileextensionsforknownfiletypes** option.
2. Test the connectivity in your network by configuring R2 with the configuration file that you created. You can copy the configuration for R2 to R2 by pasting it into the console terminal session.
3. If the IP connectivity appears to be working and the TFTP server is configured correctly, verify that you entered the **iphelper-address***ip-address* command on R4 correctly.

DETAILED STEPS

Step 1 Look for error messages on the TFTP server indicating that the files were not found. A very common mistake is that the .txt extension was added to the r2-confg file (r2-confg.txt) by your text editor. Your operating system might be hiding the extension for known file types when you browse the TFTP root directory. Disable the **Hidefileextensionsforknownfiletypes** option.

TipYou can stop most text editors from adding the filename extension by saving the file with double quotes (“filename“) around the filename. For example, saving the file as “r2-confg” should force the text editor to only use r2-confg.

Step 2 Test the connectivity in your network by configuring R2 with the configuration file that you created. You can copy the configuration for R2 to R2 by pasting it into the console terminal session.
After you have copied the configuration to R2, try to ping 10.10.10.2. If this fails, you have a problem between R2 and R4. Verify the cabling, the status of the interfaces, and the configurations on the routers.

If R2 can ping 10.10.10.2, try pinging the TFTP server (172.16.29.252) from R2. If this fails, you have a configuration problem somewhere between R4 and the TFTP server. Verify the cabling, the status of the interfaces, and the configurations on the routers. Verify the IP address and IP default gateway on the TFTP server.

TipThe IP default gateway on the TFTP server should be 172.16.29.97 (the local Ethernet interface on R4).

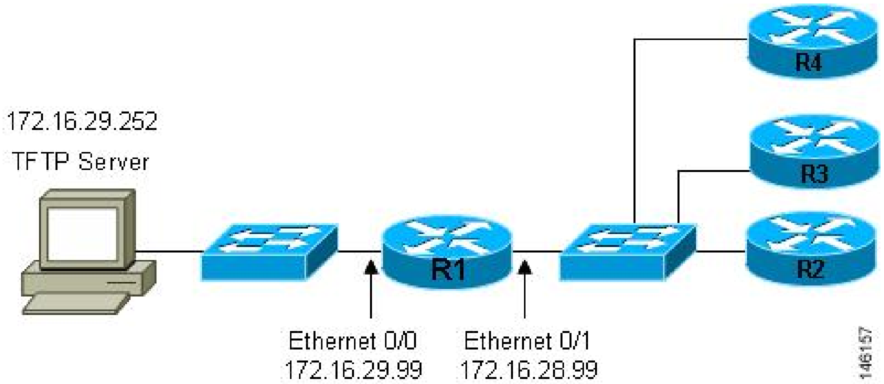
If R2 can ping the TFTP server (172.16.29.252), you probably have a problem with the TFTP server itself. A common mistake with TFTP servers is that they are configured to receive files but not to send them. Another common mistake on UNIX-based TFTP servers is that the files do not have the correct permissions. On a UNIX TFTP server the files should have permissions set to rw-rw-rw.

Step 3 If the IP connectivity appears to be working and the TFTP server is configured correctly, verify that you entered the **iphelper-address***ip-address* command on R4 correctly.

Using AutoInstall to Set Up Devices Connected to LANs Example

This task uses the network in the figure below. This task will show how to use AutoInstall to setup routers R2, R3, and R4. Router R1 is the DHCP server that will be used to assign the IP address for Fast Ethernet 0/0 on the new routers during the AutoInstall process.

Figure 9: Network Topology for Assigning AutoInstall Configuration Files For Specific Devices



Every DHCP client has a unique DHCP client identifier. The DHCP client identifier is used by DHCP servers to keep track of IP address leases and for configuring IP address reservations. You need to know the DHCP client identifier for each of the networking devices that you want to configure with AutoInstall so that you can configure the DHCP IP address reservations which will ensure that each device is provided with the correct IP address, and subsequently its unique configuration file. You can determine the DHCP client identifier manually or automatically.

To use AutoInstall to setup routers R2, R3, and R4, perform following tasks:

- Determining the Value for the DHCP Client Identifier Manually, page 70
- Determining the Value for the DHCP Client Identifier Automatically, page 74

Determining the Value for the DHCP Client Identifier Manually

If you want to determine the value for the client identifiers automatically, you do not need to perform this task. Proceed to the Determining the Value for the DHCP Client Identifier Automatically Example section.

Tip If you are using AutoInstall to configure networking devices that are running a Cisco IOS release other than 12.4(1) or newer the DHCP client identifier might use a different format. In this case use the process explained in the Determining the Vlaue for the DHCP Client Identifier Automatically Example section. .

You must know the MAC address of the Ethernet interface that will be used to connect the router to the LAN during the AutoInstall process to determine the client identifier manually. To determine the client identifier manually requires connecting a terminal to the router, and powering it on, so that you can enter the **showinterface***interface-type interface-number* command.

The client-identifier looks like this:

0063.6973.636f.2d30.3030.362e.3533.6237.2e38.6537.312d.4661.332f.30

The format is nullcisco-0006.53b7.8e71-fa3/0 where 0006.53b7.8e71 is the MAC address and fa3/0 is the short interface name for the interface that the IP address request is made.

The values for the short-if-name field can be obtained from an SNMP workstation with the Cisco MIBs installed. The following is an example of how to map ifIndex to an interface on Cisco IOS:

```
snmpwalk -c public ponch ifName
IF-MIB::ifName.1 = STRING: AT2/0
IF-MIB::ifName.2 = STRING: Et0/0
IF-MIB::ifName.3 = STRING: Se0/0
IF-MIB::ifName.4 = STRING: BR0/0
```

Use the **showinterface***interface-type interface-number* command to display the information and statistics for a Fast Ethernet interface.

```
R6> show interface fastethernet 3/0
FastEthernet3/0 is up, line protocol is up
  Hardware is AmdFE, address is 0006.53b7.8e71 (bia 0006.53b7.8e71)
.
.
.
R6>
```

The MAC address for Fast Ethernet 3/0 on R6 is 0006.53b7.8e71. The format of the client identifier for this interface is nullcisco-0006.53b7.8e71-fa3/0.

Note The short interface name for Fast Ethernet interfaces is fa.

The table below shows the values for converting characters to their hexadecimal equivalents. The last row in the second table below shows the client identifier for Fast Ethernet 3/0 on R6 (nullcisco-0006.53b7.8e71-fa3/0).

Table 3: Hexadecimal to Character Conversion Chart

Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char
00	NUL	1a	SUB	34	4	4e	N	68	h
01	SOH	1b	ESC	35	5	4f	O	69	I
02	STX	1c	FS	36	6	50	P	6a	j
03	ETX	1d	GS	37	7	51	Q	6b	k

Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char
04	EOT	1e	RS	38	8	52	R	6c	l
05	ENQ	1f	US	39	9	53	S	6d	m
06	ACK	20		3a	:	54	T	6e	n
07	BEL	21	!	3b	;	55	U	6f	o
08	BS	22	"	3c	<	56	V	70	p
09	TAB	23	#	3d	=	57	W	71	q
0A	LF	24	$	3e	>	58	X	72	r
0B	VT	25	%	3f	?	59	Y	73	s
0C	FF	26	&	40	@	5a	Z	74	t
0D	CR	27	‘	41	A	5b	[	75	u
0E	SO	28	(	42	B	5c	\	76	v
0F	SI	29	)	43	C	5d	]	77	w
10	DLE	2a	*	44	D	5e	^	78	x
11	DC1	2b	+	45	E	5f	_	79	y
12	DC2	2c	,	46	F	60	`	7a	z
13	DC3	2d	-	47	G	61	a	7b	{
14	DC4	2e	.	48	H	62	b	7c	|
15	NAK	2f	/	49	I	63	c	7D	}
16	SYN	30	0	4a	J	64	d	7e	~
17	ETB	31	1	4b	K	65	e	7f	D
18	CAN	32	2	4c	L	66	f		
19	EM	33	3	4d	M	67	g		

Table 4: Conversion of nullcisco-0006.53b7.8e71-fa3/0 To A Client Identifier

00	c	i	s	c	o	-	0	0	0	6	.	5	3	b	7	.	8	e	7	1	-	f	a	3	/	0
00	63	69	73	63	6f	2d	30	30	30	36	2e	35	33	62	37	2e	38	65	37	31	2d	66	61	33	2f	30

R4

Use the **showinterface***interface-type interface-number* command to display the information and statistics for Ethernet 0 on R4.

```
R4> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb0e (bia 00e0.1eb8.eb0e)
```

The MAC address for Ethernet 0 on R4 is 00e0.1eb8.eb0e. The format of the client identifier for this interface is nullcisco-00e0.1eb8.eb0e-et0.

Note The short interface name for Ethernet interfaces is et.

Using the values for converting characters to their hexadecimal equivalents in the first table above, the client identifier for Ethernet 0 on R4 is shown in the last row of the table below.

Table 5: Conversion of null.cisco-00e0.1eb8.eb0e-et0 To A Client Identifier for R4

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	0	e	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	30	65	2d	45	74	30

R3

Use the **showinterface***interface-type interface-number* command to display the information and statistics for Ethernet 0 on R3.

```
R3> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb73 (bia 00e0.1eb8.eb73)
```

The MAC address for Ethernet 0 on R3 is 00e0.1eb8.eb73. The format of the client identifier for this interface is: nullcisco-00e0.1eb8.eb73-et0.

Using the values for converting characters to their hexadecimal equivalents in the first table above, the client identifier for Ethernet 0 on R3 is shown in the last row of the table below.

Table 6: Conversion of null.cisco-00e0.1eb8.eb73-et0 To A Client Identifier for R3

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	7	3	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	37	33	2d	45	74	30

R2

Use the **showinterface***interface-type interface-number* command to display the information and statistics for Ethernet 0 on R2.

```
R2> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb09 (bia 00e0.1eb8.eb09)
```

The MAC address for Ethernet 0 on R2 is 00e0.1eb8.eb09. The format of the client identifier for this interface is nullcisco-00e0.1eb8.eb09-et0.

Using the values for converting characters to their hexadecimal equivalents in the first table above, the client identifier for Ethernet 0 on R2 is shown in the last row of the table below

Table 7: Conversion of null.cisco-00e0.1eb8.eb09-et0 To A Client Identifier for R2

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	0	9	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	30	39	2d	45	74	30

You have now determined the values for the client identifiers on each router. The final step is to add a period after each group of four characters working from the left to the right as shown below:

- R4-0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30
- R3-0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
- R2-0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30

- What to Do Next, page 74

What to Do Next

Save the values in a text file and proceed to the Creating a Private DHCP Pool for Each of the Routers Example section.

Determining the Value for the DHCP Client Identifier Automatically

If you determined the value for the client identifiers manually, you do not need to perform this task. Proceed to the Creating a Private DHCP Pool for Each of the Routers Example section.

This task will create a DHCP server on R1 that will provide only one IP address. This IP address will used by each new router in sequence while you determine the value of the router's client identifier. By limiting the IP address scope to a single IP address you avoid any possible confusion about which router you are working on. If somebody powers up another router that attempts to start the AutoInstall process, it will not be able to obtain an IP address.

Tip Do not place the network-confg or router configuration files (r4-confg, r3-confg, or r2-confg) in the root directory of the TFTP server yet. You do not want any of the routers to load these files until you have ensured that each router will obtain the correct IP address from the DHCP server so that the router will load the correct configuration file.

This task is broken down into subtasks. See the Determining the Value for the DHCP Client Identifier Manually section for more information.

Configuration Examples for Using AutoInstall to Remotely Configure Cisco Networking Devices

- Using AutoInstall with Frame Relay to ATM Service Internetworking Example, page 56
- Using AutoInstall to Set Up Devices Connected to LANs Example, page 78
- Using AutoInstall to Set Up Devices Connected to WANs Example, page 86

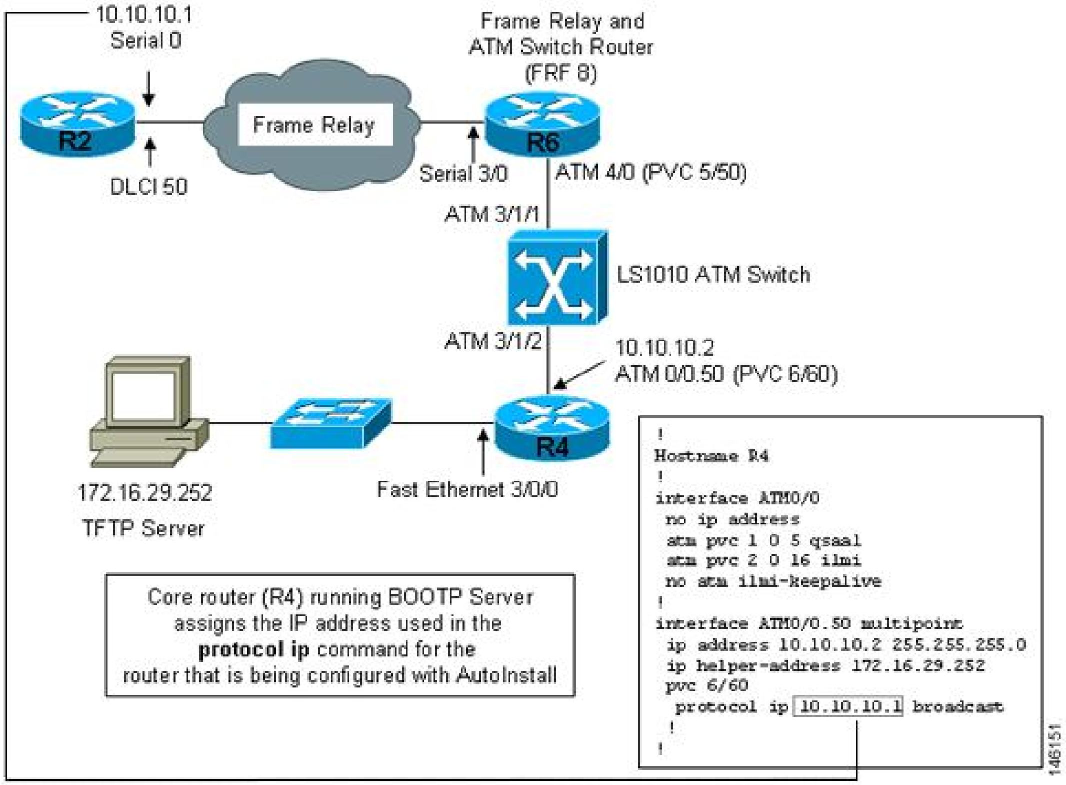
Using AutoInstall with Frame Relay to ATM Service Internetworking Example

Refer to the figure below for the sample network used in this task. Perform this task to configure routers R6, R4, and the LS1010 ATM switch so that AutoInstall can be used with Frame Relay to ATM Service Internetworking (FRF8) to set up router R2.

Note

The IP address that will be assigned to Serial 0 on R2 (10.10.10.1/24) during and after the AutoInstall process and the IP address that is assigned to ATM 0/0.50 on R4 (10.10.10.2/24) are on the same subnet (10.10.10.0/24). Using IP addresses on the same subnet is required because the interfaces on R6 and the LS10101 switch are switching the IP packets between R2 and R4 at Layer 2.

Figure 10: Example Topology for AutoInstall over Frame Relay/ATM Interworking Connections



```
!
Hostname R4
!
interface ATM0/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 no atm ilmi-keepalive
!
interface ATM0/0.50 multipoint
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 172.16.29.252
 pvc 6/60
  protocol ip 10.10.10.1 broadcast
  !
!
```

- Configuring R6 for Frame Relay to ATM Service Internetworking, page 57
- Verifying Frame Relay to ATM Service Internetworking on R6, page 61
- Configuring R4 for Frame Relay to ATM Service Internetworking, page 61
- Configuring IP Routing R4, page 64
- Configuring the LS1010 Switch, page 66
- Verifying AutoInstall with Frame Relay to ATM Service Internetworking, page 67
- Configuring R6 for Frame Relay to ATM Service Internetworking Example, page 76

- Configuring R4 for Frame Relay to ATM Service Internetworking Example, page 76
- Configuring R4 for Frame Relay to ATM Service Internetworking Example, page 76
- Configuring the LS1010 Switch Example, page 77
- Creating the Configuration File for R2 Example, page 77

Configuring R6 for Frame Relay to ATM Service Internetworking Example

The following example shows how to configure R6 for Frame Relay to ATM Service Internetworking (FRF8).

```
!
hostname R6
!
interface Serial3/0
 no ip address
 encapsulation frame-relay IETF
 frame-relay interface-dlci 50 switched
 frame-relay lmi-type ansi
 frame-relay intf-type dce
!
interface ATM4/0
 pvc 0 5 qsaal
 pvc 0 16 ilmi
 no atm ilmi-keepalive
 pvc 5/50
  encapsulation aal5mux fr-atm-srv
!
connect r2 serial3/0 50 atm4/0 5/50 service-interworking
!
```

Configuring R4 for Frame Relay to ATM Service Internetworking Example

The following example configures R4 as the core router for AutoInstall using Frame Relay to ATM Service Internetworking (FRF8).

```
!
hostname R4
!
interface FastEthernet3/0/0
 ip address 172.16.29.97 255.255.255.0
!
interface ATM0/0
 no ip address
 pvc 0 5 qsaal
 pvc 0 16 ilmi
 no atm ilmi-keepalive
!
interface ATM0/0.50 multipoint
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 172.16.29.252
 pvc 6/60
  protocol ip 10.10.10.1 broadcast
 !
!
```

Configuring R4 for Frame Relay to ATM Service Internetworking Example

The following example shows how to configure IP routing on R4.

```
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
!
```

Configuring the LS1010 Switch Example

The following example shows how to configure the LS1010 ATM switch to route the PVCs between R6 and R4.

```
!
atm address 47.0091.8100.0000.0010.11b9.6101.0010.11b9.6101.00
atm router pnni
 no aesa embedded-number left-justified
 node 1 level 56 lowest
  redistribute atm-static
!
interface ATM2/0/0
 no ip address
 no ip directed-broadcast
 atm maxvp-number 0
!
interface ATM3/1/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
!
interface ATM3/1/1
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
!
interface ATM3/1/2
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 pvc 6 60 interface ATM3/1/1 5 50
!
interface ATM3/1/3
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
!
```

Creating the Configuration File for R2 Example

SUMMARY STEPS

1. Create the following configuration file for R2.
2. Store the configuration file on the TFTP server with the name r2-confg.

DETAILED STEPS

Step 1 Create the following configuration file for R2.

Example:

```
!
hostname R2
!
!
```

```
enable secret 7gD2A0
!
interface Ethernet0
 no ip address
 shutdown
!
interface Serial0
 ip address 10.10.10.1 255.255.255.0
 encapsulation frame-relay IETF
 frame-relay map ip 10.10.10.2 50 broadcast
 frame-relay interface-dlci 50
 frame-relay lmi-type ansi
!
interface Serial1
 no ip address
 shutdown
!
!
router rip
 version 2
 network 10.0.0.0
 no auto-summary
!
ip http server
ip classless
!
line vty 0 4
 password 87F3c0m
 login
!
end
```

Step 2 Store the configuration file on the TFTP server with the name r2-confg.

Example:

```
Router# copy running-config tftp:
Address or name of remote host []? 192.0.2.1
Destination filename [running-config]? r2-config
!!!
1030 bytes copied in 9.612 secs (107 bytes/sec)
Router#
```

Using AutoInstall to Set Up Devices Connected to LANs Example

Determining the Value for the DHCP Client Identifier Automatically Example

Configuring IP on the Interfaces on R1 Example

The following example shows how to configure the **iphelper-address***ip-address* command on Ethernet0/1.

```
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
 ip address 172.16.28.99 255.255.255.0
 ip helper-address 172.16.29.252
!
```

Configuring a DHCP Pool on R1 Example

The following example shows how to configure the commands to set up a temporary DHCP server on R1.

Note There should be only one DHCP server in operation on R1. This server should be the only DHCP server that is accessible by the routers that you will be using AutoInstall to set up.

```
!
ip dhcp pool get-client-id
   network 172.16.28.0 255.255.255.0
!
```

Excluding All But One of the IP Addresses from the DHCP Pool on R1 Example

The following example shows how to configure the **ipdhcpexcluded-address** command to exclude every IP address except 172.16.28.1 from the DHCP pool.

Note You need to ensure that there is only one IP address available from the DHCP server at any time.

```
!
ip dhcp excluded-address 172.16.28.2 172.16.28.255
!
```

Verifying the Configuration on R1 Example

The following example shows how to verify the configuration on R1.

Verify that the configuration file for R1 has a DHCP server pool configured to provide a single IP address (172.16.28.1) to a DHCP client.

Verify that the configuration file has the IP addresses for the Ethernet interfaces and the **iphelper-address***ip-address* command.

```
!
ip dhcp excluded-address 172.16.28.2 172.16.28.255
!
ip dhcp pool get-client-id
   network 172.16.28.0 255.255.255.0
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
 ip address 172.16.28.99 255.255.255.0
 ip helper-address 172.16.29.252
!
```

Enabling debug ip dhcp server events on R1 Example

The following example shows how to enable the **debugipdhcpserverevents** command on R1.

Use the display output from the **debugipdhcpserverevents** command on the terminal connected to R1 to identify the value of the client identifier for each router.

```
R1# debug ip dhcp server events
```

Identifying the Value for the Client Identifier on Each of the Routers Example

The following example shows how to identify the value for the client identifier on each of the routers.

The following step is repeated for each of the routers. You should have only one of the routers powered-on at any time. When you have identified the value of the client identifier field for the router, turn the router off and proceed to the next router.

R4

Connect R4 to the Ethernet network and power it on. The following message is displayed on the terminal connected to R1 when R4 is assigned the IP address 172.16.28.1.

```
DHCPD: assigned IP address 172.16.28.1 to client 0063.6973.636f.2d30.3065.302e.
3165.6238.2e65.6230.652d.4574.30.
```

Copy the client identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30 to a text file and save it. Keep the text file open for the next two routers.

Turn off R4

Release the IP address binding for R4 from the DHCP pool on R1 using the **clearipdhcpbinding*** command on R1.

```
R1# clear ip dhcp binding *
R1#
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

R3

Connect R3 to the Ethernet network and power it on. The following message is displayed on the terminal connected to R1 when R3 is assigned the IP address 172.16.28.1.

```
DHCPD: assigned IP address 172.16.28.1 to client 0063.6973.636f.2d30.3065.302e.
3165.6238.2e65.6237.332d.4574.30.
```

Copy the client identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30 to the text file and save it. Keep the text file open for the final router.

Turn off R3.

Release the IP address binding for R3 from the DHCP pool on R1 using the **clearipdhcpbinding*** command on R1.

```
R1# clear ip dhcp binding *
R1#
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

R2

Connect R2 to the Ethernet network and power it on. The following message is displayed on the terminal connected to R1 when R2 is assigned the IP address 172.16.28.1.

```
DHCPD: assigned IP address 172.16.28.1 to client 0063.6973.636f.2d30.3065.302e.
3165.6238.2e65.6230.392d.4574.30.
```

Copy the client identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30 to the text file and save it.

Turn off R2

Release the IP address binding for R2 from the DHCP pool on R1 using the **clearipdhcpbinding*** command on R1.

```
R1# clear ip dhcp binding *
R1#
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

Client Identifiers for R4, R3, and R2

You have determined the values for the client identifiers on each router.

- R4-0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30
- R3-0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
- R2-0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30

Removing the DHCP Pool on R1 for Network 172.16.28.0 24 Example

The following example shows how to remove the temporary DHCP pool on the router that is no longer required.

```
R1(config)# no ip dhcp pool get-client-id
```

Removing the Excluded Address Range From R1 Example

The following example shows how to remove the command for excluding all of the IP addresses except 172.16.28.1 from the DHCP pool on the router.

```
R1(config)# no ip dhcp excluded-address 172.16.28.2 172.16.28.255
```

Creating a Private DHCP Pool for Each of The Routers Example

The following example shows how to create private DHCP address pools for each router to ensure that each router is assigned the IP address that maps to its host name in the network-configuration file.

```
!
ip dhcp pool r4
   host 172.16.28.100 255.255.255.0
   client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30
!
ip dhcp pool r3
   host 172.16.28.101 255.255.255.0
   client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
!
ip dhcp pool r2
   host 172.16.28.102 255.255.255.0
   client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30
```

Creating Configuration Files for Each Router Example

The following example shows how to create the configuration files for each router and place them in the root directory of the TFTP server.

Tip You must include the commands for configuring passwords for remote Telnet access and access to privileged EXEC mode if you are going to access the routers remotely to save their configuration files to NVRAM.

r2-confg

```
!
hostname R2
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 172.16.28.102 255.255.255.0
!
interface Serial0
 ip address 192.168.100.1 255.255.255.252
 no shutdown
!
interface Serial1
 ip address 192.168.100.5 255.255.255.252
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Ethernet0
!
line vty 0 4
 password 5Rf1k9
 login
!
end
```

r3-confg

```
!
hostname R3
!
enable secret 7gD2A0
!
```

```
interface Ethernet0
 ip address 172.16.28.101 255.255.255.0
!
interface Serial0
 ip address 192.168.100.9 255.255.255.252
 no shutdown
!
interface Serial1
 ip address 192.168.100.13 255.255.255.252
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Ethernet0
!
line vty 0 4
 password 5Rf1k9
 login
!
end
```

r4-confg

```
!
hostname R3
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 172.16.28.101 255.255.255.0
!
interface Serial0
 ip address 192.168.100.9 255.255.255.252
 no shutdown
!
interface Serial1
 ip address 192.168.100.13 255.255.255.252
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Ethernet0
!
line vty 0 4
 password 5Rf1k9
 login
!
end
```

Creating the network-confg file Example

The following example shows how to create the network-configuration file with the **iphost***hostnameip-address* commands that map the IP addresses that you will be assigning with the DHCP server to the hostname.

```
ip host r4 172.16.28.100
ip host r3 172.16.28.101
ip host r2 172.16.28.102
```

Setting Up the Routers with AutoInstall Example

The following example shows how to set up three routers (R4, R3, and R2) using AutoInstall.

Connect a terminal to the routers if you want to monitor the progress of AutoInstall. Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:

- 9600 baud
- 8 data bits, no parity, 1 stop bit
- No flow control

You should have the following files in the root directory of the TFTP server.

- network-confg
- r4-confg
- r3-confg
- r2-confg

The TFTP server must be running.

Power on each router.

Timesaver You can set up all three routers concurrently.

R4

The following is an excerpt of the messages that are displayed on R4's console terminal during the AutoInstall process:

```
Loading network-confg from 172.16.29.252 (via Ethernet0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.100 to r4
Loading r4-confg from 172.16.29.252 (via Ethernet0): !
[OK - 687 bytes]
```

R3

The following is an excerpt of the messages that are displayed on R3's console terminal during the AutoInstall process:

```
Loading network-confg from 172.16.29.252 (via Ethernet0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.101 to r3
Loading r3-confg from 172.16.29.252 (via Ethernet0): !
[OK - 687 bytes]
```

R2

The following is an excerpt of the messages that are displayed on R2's console terminal during the AutoInstall process:

```
Loading network-confg from 172.16.29.252 (via Ethernet0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.102 to r2
Loading r2-confg from 172.16.29.252 (via Ethernet0): !
[OK - 687 bytes]
```

TFTP Server Log

The TFTP server log should contain messages similar to the following text.

```
Sent network-confg to (172.16.28.100), 76 bytes
Sent r4-confg to (172.16.28.100),687 bytes
Sent network-confg to (172.16.28.101), 76 bytes
Sent r3-confg to (172.16.28.101),687 bytes
Sent network-confg to (172.16.28.102), 76 bytes
Sent r2-confg to (172.16.28.102),687 bytes
```

Saving the Configuration Files on the Routers Example

The following example shows how to save the running configurations on each router to the startup configuration to ensure that the routers retain their configurations if they are ever power cycled.

R4

```
R1# telnet 172.16.28.100
Trying 172.16.28.100 ... Open
User Access Verification
Password:
R4> enable
Password:
R4# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4# exit
[Connection to 172.16.28.100 closed by foreign host]
R1#
```

R3

```
R1# telnet 172.16.28.101
Trying 172.16.28.101 ... Open
User Access Verification
Password:
R3> enable
Password:
R3# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3# exit
[Connection to 172.16.28.101 closed by foreign host]
R1#
```

R2

```
R1# telnet 172.16.28.102
Trying 172.16.28.102 ... Open
User Access Verification
Password:
R2> enable
Password:
R2# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2# exit
[Connection to 172.16.28.102 closed by foreign host]
R1#
```

Removing the Private DHCP Address Pools from R1 Example

The following example shows how to remove the private DHCP address pools from R1.

```
R1(config)# no ip dhcp pool r4
R1(config)# no ip dhcp pool r3
R1(config)# no ip dhcp pool r2
```

This task is the final step for using AutoInstall to set up devices connected to LANs.

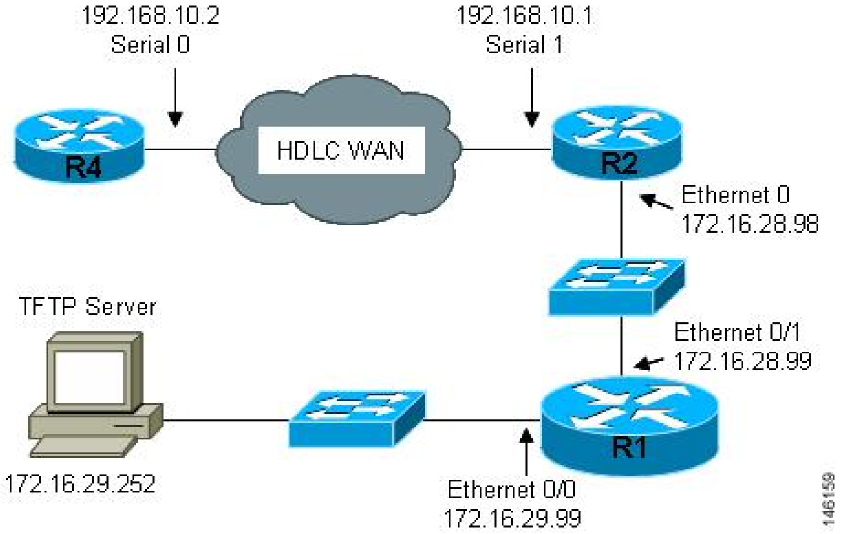
Using AutoInstall to Set Up Devices Connected to WANs Example

- HDLC WAN Connections, page 86
- Frame-Relay WAN Connections, page 89

HDLC WAN Connections

This section uses the network in the figure below. The section shows how to use AutoInstall to setup R4. R2 will use SLARP to provide R4 the IP address (192.168.20.2) required for AutoInstall.

Figure 11: Network Topology Using AutoInstall to Configure Routers Connected to HDLC WANs



- Creating the Configuration for R4 Example, page 86
- Creating the network-confg File Example, page 87
- Configuring R1 and R2 Example, page 87
- Setting Up R4 using AutoInstall Example, page 88
- Save the Configuration File on R4 Example, page 88

Creating the Configuration for R4 Example

The following example shows how to create the configuration file for R4 and save it on the TFTP server as r4-confg:

```
!
hostname R4
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 10.89.45.1 255.255.255.0
 no shutdown
!
interface Serial0
 ip address 192.168.10.2 255.255.255.0
 no fair-queue
!
router rip
 version 2
 network 168.192.0.0
 no auto-summary
!
ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Serial0
!
line vty 0 4
password 6T2daX9
!
end
```

Creating the network-confg File Example

The following example shows how to create the network configuration file for R4 and save it on the TFTP server as network-confg:

```
ip host r4 192.168.10.2
```

Configuring R1 and R2 Example

The following example shows how to configure R1 and R2 using the following configurations:

R1

```
!
hostname R1
!
enable secret 7gD2A0
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
 ip address 172.16.28.99 255.255.255.0
!
interface Serial2
 ip helper-address 172.16.29.252
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
ip classless
ip http server
!
```

```
line vty 0 4
 password 67F2SaB
!
end
```

R2

```
!
hostname R2
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 172.16.28.98 255.255.255.0
!
interface Serial1
 ip address 192.168.10.1 255.255.255.0
 clockrate 64000
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.10.0
 no auto-summary
!
ip http server
ip classless
!
line vty 0 4
 password u58Hg1
!
end
```

Setting Up R4 using AutoInstall Example

The following example shows how to set up R4 using AutoInstall.

Connect R4 to the HDLC WAN network.

Power R4 on.

The AutoInstall process should be complete in approximately 5 minutes.

TFTP Server Log

The TFTP server log should contain messages similar to the following text:

```
Sent network-confg to (192.168.10.2), 76 bytes
Sent r4-confg to (192.168.10.2),687 bytes
```

Save the Configuration File on R4 Example

The following example shows how to save the running configurations on R4 to the startup configuration to ensure that R4 retains its configuration if it is ever power cycled.

```
R1# telnet 192.168.10.2
Trying 192.168.10.2 ... Open
User Access Verification
Password:
R4> enable
Password:
R4# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4# exit
```

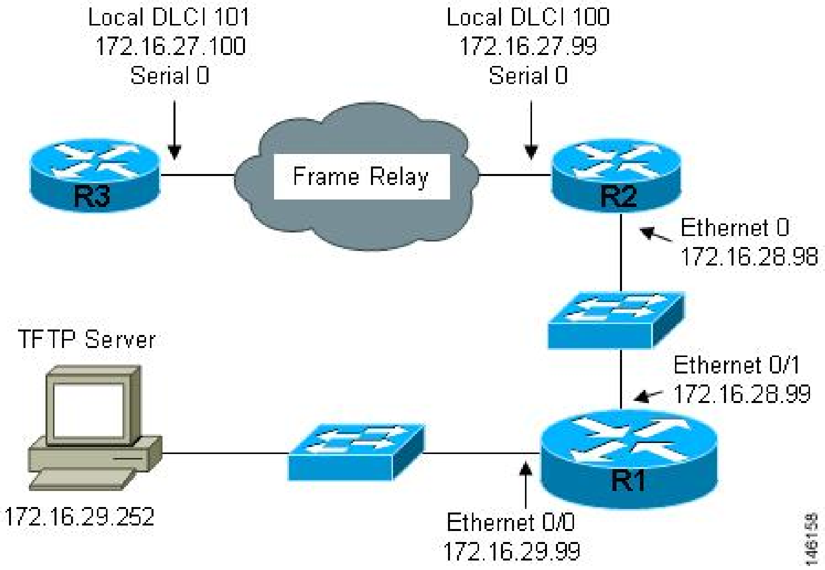
```
[Connection to 192.168.10.2 closed by foreign host]
R1#
```

Frame-Relay WAN Connections

This section uses the network in the figure below. The section shows how to use AutoInstall to setup R4. R2 will use BOOTP to provide R4 the IP address (172.16.27.100) required for AutoInstall.

R2 uses 172.16.27.100 as the IP address to provide to R3 using BOOTP because this is the IP address in the **frame-relay map ip 172.16.27.100 100 broadcast** command on serial 0 that points to serial 0 on R3.

Figure 12: Network Topology for Using AutoInstall to Configure Routers Connected to Frame Relay WANs



- Creating the Configuration for R3 Example, page 89
- Creating the network-confg File Example, page 90
- Configuring R1 and R2 Example, page 90
- Setting Up R3 using AutoInstall Example, page 91
- Saving the Configuration File on R3 Example, page 91

Creating the Configuration for R3 Example

The following example shows how to create the configuration file for R4 and save it on the TFTP server as r3-confg:

```
!
hostname R3
!
enable secret 8Hg5Zc20
!
interface Ethernet0
 no ip address
 shutdown
!
interface Serial0
 ip address 172.16.27.100 255.255.255.0
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay map ip 172.16.27.99 101 broadcast
 frame-relay interface-dlci 101
!
interface Serial1
 no ip address
 shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
line vty 0 4
 password 67Td3a
 login
!
end
```

Creating the network-confg File Example

The following example shows how to create the network configuration file for R3 and save in on the TFTP server as network-confg:

```
ip host r3 172.16.27.100
```

Configuring R1 and R2 Example

The following example shows how to configure R1 and R2 using the following configurations:

R1

```
!
hostname R1
!
enable secret 86vC7Z
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
 ip address 172.16.28.99 255.255.255.0
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
line vty 0 4
 password 6Gu8z0s
!
!
end
```

R2

```
!
hostname R2
!
enable secret 67Hfc5z2
!
interface Ethernet0
 ip address 172.16.28.98 255.255.255.0
 ip helper-address 172.16.29.252
!
interface Serial0
```

```
 ip address 172.16.27.99 255.255.255.0
 ip helper-address 172.16.29.252
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay map ip 172.16.27.100 100 broadcast
 frame-relay interface-dlci 100
!
interface Serial1
 no ip address
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
line vty 0 4
 password 9Jb6Z3g
!
end
```

Setting Up R3 using AutoInstall Example

The following example shows how to set up R3 using AutoInstall.

Connect R3 to the Frame Relay network.

Power R3 on.

The AutoInstall process should be complete in approximately 5 minutes.

TFTP Server Log

The TFTP server log should contain messages similar to the following text:

```
Sent network-confg to (172.16.27.100), 76 bytes
Sent r3-confg to (172.16.27.100),687 bytes
```

Saving the Configuration File on R3 Example

The following example shows how to save the running configurations on R3 to the startup configuration to ensure that R3 retains its configuration if it is ever power cycled.

```
R1# telnet 172.16.27.100
Trying 172.16.27.100 ... Open
User Access Verification
Password:
R3> enable
Password:
R3# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4# exit
[Connection to 192.168.10.2 closed by foreign host]
R1#
```

Additional References

The following sections provide references related to using AutoInstall to remotely configure Cisco networking devices.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuration Fundamentals commands	*Cisco IOS Configuration Fundamentals Command Reference*
Frame Relay-to-ATM Service Interworking (FRF. 8)	• Frame Relay-ATM Interworking Supported Standards module in the *Cisco IOS Wide-Area Networking Configuration Guide* • Configuring Frame Relay-ATM Interworking module in the *Cisco IOS Wide-Area Networking Configuration Guide*
Overview of Cisco IOS setup mode and AutoInstall for configuring Cisco networking devices	Overview: Basic Configuration of a Cisco Networking Device module in the *Cisco IOS Configuration Fundamentals Configuration Guide*
Using setup mode to configure a Cisco networking device	Using Setup Mode to Configure a Cisco Networking Device module in the *Cisco IOS Configuration Fundamentals Configuration Guide*

MIBs

MIB	MIBs Link
IF-MIB	The IFNAME object in the IF-MIB can be used to identify the values for the short interface names used in the DHCP Client Identifier for Cisco IOS devices when they are configured as DHCP clients. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and	http://www.cisco.com/cisco/web/support/index.html

Description	Link
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.	

Feature Information for Using AutoInstall to Remotely Configure a Cisco Networking Device

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8: Feature Information for Usinf AutoInstall to Remotely Set Up a Cisco Networking Device

Feature Name	Releases	Feature Configuration Information
AutoInstall over Frame Relay-ATM Interworking Connections	12.2(4)T	The AutoInstall over Frame Relay-ATM Interworking Connections feature extends the functionality of the existing Cisco IOS AutoInstall feature. While AutoInstall over Frame Relay encapsulated serial interfaces has long been supported, this feature provides the same functionality when the central (existing) router has an ATM interface instead of a Frame Relay interface. No new or modified commands are introduced with this feature. All commands used with this feature are documented in the *Cisco IOS Configuration Fundamentals Command Reference*.

Feature Name	Releases	Feature Configuration Information
AutoInstall Using DHCP for LAN Interfaces	12.1(5)T 12.2(33)SRC	The AutoInstall Using DHCP for LAN Interfaces feature enhances the benefits of AutoInstall by replacing the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces (specifically Ethernet, Token Ring, and FDDI interfaces).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Configuring Operating Characteristics for Terminals

Configuring the operating characteristics for terminals enables you to customize the settings for displays, formatting, and usability of the terminals on your network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Operating Characteristics for Terminals

- You should have at least a basic familiarity with the Cisco IOS environment and the command-line interface.
- You should have at least a minimal configuration running on your system. You can create a basic configuration file using the **setup** command (see Using Setup Mode to Configure a Cisco Networking Device for details).

Restrictions for Configuring Operating Characteristics for Terminals

- Many of the Cisco IOS commands described in this document are available and function only in certain configuration modes on the router.
- Some of the Cisco IOS configuration commands are only available on certain router platforms, and the command syntax may vary on different platforms.

Information About Configuring Operating Characteristics for Terminals

Definition of the Escape Character and Other Key Sequences

You can define or modify the default keys used to execute functions for system escape, terminal activation, disconnect, and terminal pause. Generally, the keys used are actually combinations of keys, such as pressing the Control (Ctrl) key and another key (or keys) at the same time (such as Ctrl-^). Sequences of keys, such as pressing the Control key and another key, then pressing yet another key, are also sometimes used (for example Ctrl-^, x). However, in each case these keys are referred to as characters, because each key or combination of keys is represented by a single ASCII character. For a complete list of available ASCII characters and their decimal and keyboard equivalents, see the “ASCII Character Set” appendix of the Cisco IOS Configuration Fundamentals command Reference.

Specification of an International Character Display

The classic U.S. ASCII character set is limited to 7 bits (128 characters), which adequately represents most displays in the U.S. Most defaults on the modem router work best on a 7-bit path. However, international character sets and special symbol display can require an 8-bit wide path and other handling.

You can use a 7-bit character set (such as ASCII), or you can enable a full 8-bit international character set (such as ISO 8859). This allows special graphical and international characters for use in banners and prompts, and adds special characters such as software flow control. Character settings can be configured globally, per line, or locally at the user level. Use the following criteria for determining which configuration mode to use when you set this international character display:

- If a large number of connected terminals support nondefault ASCII bit settings, use the global configuration commands.
- If only a few of the connected terminals support nondefault ASCII bit settings, use line configuration commands or the EXEC local terminal setting commands.

Note Setting the EXEC character width to an 8-bit character set can cause failures. If a user on a terminal that is sending parity enters the **help** command, an "unrecognized command" message appears because the system is reading all eight bits, although the eighth bit is not needed for **help**.

If you are using the **autoselect** function, the activation character should be set to the default Return, and the EXEC character bit should be set to 7. If you change these defaults, the application does not recognize the activation request.

Data Transparency for File Transfers

Data transparency enables the Cisco IOS software to pass data on a terminal connection without the data being interpreted as a control character.

During terminal operations, some characters are reserved for special functions. For example, the key combination Ctrl-Shift-6, X (^^x) suspends a session. When transferring files over a terminal connection (using the Xmodem or Kermit protocols, for example), you must suspend the recognition of these special characters to allow a file transfer. This process is called *data transparency* .

You can set a line to act as a transparent pipe so that programs such as Kermit, Xmodem, and CrossTalk can download a file across a terminal line. To temporarily configure a line to act as a transparent pipe for file transfers, use the **terminaldownload** command in EXEC mode. The **terminaldownload** command is equivalent to using all the following commands:

- **terminal telnet transparent**
- **terminal no escape-character**
- **terminal no hold-character**
- **terminal no padding 0**
- **terminal no padding 128**
- **terminal parity none**
- **terminal databits**

Terminal Screen Length and Width

By default, the Cisco IOS software provides a screen display of 24 lines by 80 characters. You can change these values if they do not meet the requirements of your terminal. The screen values you set are passed during rsh and rlogin sessions.

The screen values set can be learned by some host systems that use this type of information in terminal negotiation. To disable pausing between screens of output, set the screen length to 0.

The screen length specified can be learned by remote hosts. For example, the rlogin protocol uses the screen length to set terminal parameters on a remote UNIX host. The width specified also can be learned by remote hosts.

Creation of Character and Packet Dispatch Sequences

The Cisco IOS software supports dispatch sequences and TCP state machines that send data packets only when they receive a defined character or sequence of characters. You can configure dispatch characters that allow packets to be buffered, then sent upon receipt of a character. You can configure a state machine that allows packets to be buffered, then sent upon receipt of a sequence of characters. This feature enables packet transmission when the user presses a function key, which is typically defined as a sequence of characters, such as Esc I C.

TCP state machines can control TCP processes with a set of predefined character sequences. The current state of the device determines what happens next, given an expected character sequence. The state-machine commands configure the server to search for and recognize a particular sequence of characters, then cycle through a set of states. The user defines these states--up to eight states can be defined. (Think of each state as a task that the server performs based on the assigned configuration commands and the type of character sequences received.)

The Cisco IOS software supports user-specified state machines for determining whether data from an asynchronous port should be sent to the network. This functionality extends the concept of the dispatch character and allows the equivalent of multicharacter dispatch strings.

Up to eight states can be configured for the state machine. Data packets are buffered until the appropriate character or sequence triggers the transmission. Delay and timer metrics allow for more efficient use of system resources. Characters defined in the TCP state machine take precedence over those defined for a dispatch character.

LPD Protocol Support on a Printer

The Cisco IOS software supports a subset of the Berkeley UNIX Line Printer Daemon (LPD) protocol used to send print jobs between UNIX systems. This subset of the LPD protocol permits the following:

- Improved status information
- Cancellation of print jobs
- Confirmation of printing and automatic retry for common print failures
- Use of standard UNIX software

The Cisco implementation of LPD permits you to configure a printer to allow several types of data to be sent as print jobs (for example, PostScript or raw text).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Managing Connections Menus and System Banners

Management of connections to other hosts, banner messages for router users, and creation of menus for specific user tasks consists of many optional features that provide better support for users on your network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Managing Connections Menus and System Banners

- You should have at least a basic familiarity with the Cisco IOS environment and the command-line interface.
- You should have at least a minimal configuration running on your system. You can create a basic configuration file using the **setup** command (see Using Setup Mode to Configure a Cisco Networking Device for details).

Restrictions for Managing Connections Menus and System Banners

- Many of the Cisco IOS commands described in this document are available and function only in certain configuration modes on the router.
- Some of the Cisco IOS configuration commands are only available on certain router platforms, and the command syntax may vary on different platforms.

Information About Managing Connections Menus and System Banners

Escape fromTerminal Sessions and Switch to Other Connections

After you have started a connection, you can escape out of the current terminal session by using the escape key sequence (Ctrl-Shift-6 then X by default). You can type the command character as you hold down the Ctrl key or with the Ctrl key released; you can type either uppercase or lowercase letters.

Note In screen output examples that show two caret (^^) symbols together, the first caret represents the Control key (Ctrl) and the second caret represents the key sequence Shift-6. The double-caret combination (^^) means hold down the Ctrl key while you press the Shift and the 6 key.

By default, the escape key sequence is Ctrl-Shift-6, X. However, the escape key sequence can be changed using the **escape-character** line configuration command. To determine the current setting for the escape character, use the **showterminal** privileged or user EXEC command.

You can have several concurrent sessions open and switch back and forth between them.

The number of sessions that can be open at one time is defined by the **session-limitVDPN** configuration mode command.

Banner Tokens

Banners can be customized with the use of banner tokens. Tokens are keywords in the form $(*token*) that, when used in a banner message, display the currently configured value of the token argument (for example, the router hostname, domain name, or IP address). Using these tokens, you can design your own banners that will display current Cisco IOS configuration variables. Only Cisco IOS supported tokens may be used. There is no facility for you to define your own tokens.

The table below lists the tokens supported by the different **banner** commands.

Table 9: Tokens Allowed by Banner Type

Token	Description	motd banner	login banner	exec banner	incoming banner	slip-ppp banner
$(hostname)	Router Hostname	Yes	Yes	Yes	Yes	Yes
$(domain)	Router Domain Name	Yes	Yes	Yes	Yes	Yes
$(peer-ip)	IP Address of the Peer Machine	No	No	No	No	Yes
$(gate-ip)	IP Address of the Gateway Machine	No	No	No	No	Yes
$(encap)	Encapsulation Type (SLIP or PPP)	No	No	No	No	Yes
$(encap-alt)	Encapsulation Type Displayed as SL/IP instead of SLIP	No	No	No	No	Yes
$(mtu)	Maximum Transmission Unit Size	No	No	No	No	Yes
$(line)	vty or tty (async) Line Number	Yes	Yes	Yes	Yes	No
$(line-desc)	User-specified description of the Line	Yes	Yes	Yes	Yes	No

Exit a Session Started from a Router

The protocol used to initiate a session determines how you exit that session.To exit from SLIP and PPP connections, you must hang up the dial-in connection, usually with a command that your dial-in software supports.

To exit a local area transport (LAT), Telnet, rlogin, TN3270, or X.3 packet assembler/disassembler (PAD) session begun from the router to a remote device, press the escape key sequence (Ctrl-Shift-6 then X

[Ctrl^X] by default for some systems, Ctrl-Z by default for other systems) and enter the **disconnect**command at the EXEC prompt. You can also log out of the remote system.

You can use either the **exit** or **logout** command in EXEC mode to terminate an active terminal session.

To exit a Telnet session *to* a router, see the “Log Out of a Router” section.

Log Out of a Router

The method you use to logout from or disconnect from a router depends on where you are located in relation to the router, and the port on the router to which you log in.

If your terminal or computer running a terminal-emulation application is remotely connected to the console port of the router, you disconnect by issuing the command or key sequence used by your terminal-emulation package. For example, if you are on a Macintosh computer running the application TCP/Connect from InterCon Corporation, you would press Ctrl-] at the user or privileged EXEC prompt to disconnect.

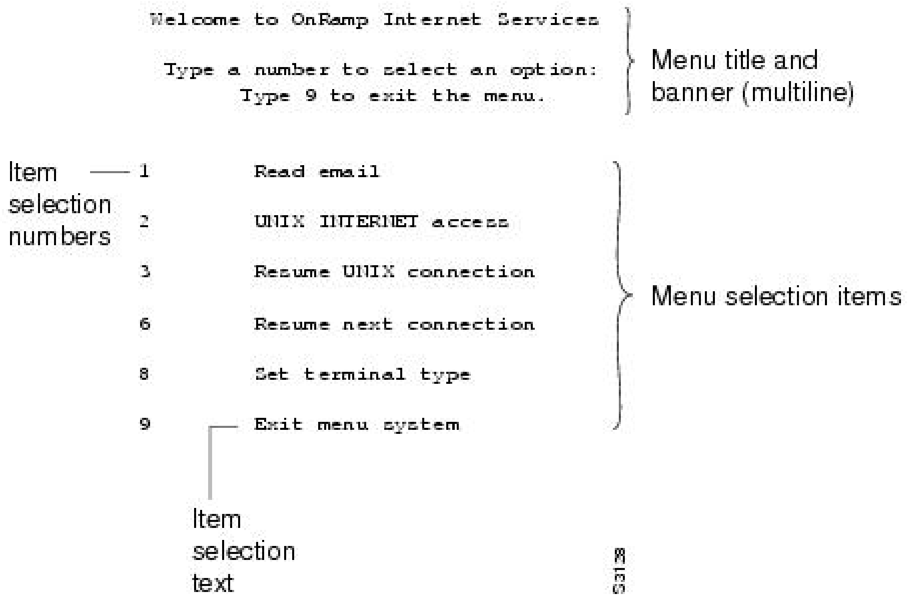
If you are on a remote terminal and connect to a vty through a synchronous interface on the router, you can issue one of the following commands in user EXEC or privileged EXEC mode to log out:

- **exit**
- **logout**

Create Menus

A menu is a displayed list of actions from which a user can select without needing to know anything about the underlying command-level details. A menu system (also known as a user menu) effectively controls the functions a user can access. The figure below illustrates the parts that make up a typical menu.

Figure 13: Typical Menu Example



```
 Welcome to OnRamp Internet Services

  Type a number to select an option:
       Type 9 to exit the menu.


1        Read email

2        UNIX INTERNET access

3        Resume UNIX connection

6        Resume next connection

8        Set terminal type

9        Exit menu system
```

Any user that can enter configuration mode can create menus. Remember the following guidelines when you create menus:

- Each menu item represents a single user command.
- The menu system default is a standard "dumb" terminal that displays text only in a 24-line-by-80-column format.
- A menu can have no more than 18 menu items. Menus containing more than 9 menu items are automatically configured as single-spaced menus; menus containing 9 or fewer menu items are automatically configured as double-spaced menus, but can be configured as single-spaced menus using the **menu single-space**global configuration command. (For more information about menu display configuration options, see the Specifying Menu Display Configuration Options modulelater in this chapter.)
- Item keys can be numbers, letters, or strings. If you use strings, you must configure the **menu line-mode** global configuration command.
- When you construct a menu, always specify how a user exits a menu and where the user goes. If you do not provide an exit from a menu--such as with the **menu-exit** command (described in the section Specifying the Underlying Command for the Menu Item module later in this chapter), the user will be trapped.

The **exec-timeout** line configuration command can be used to close and clean up an idle menu; the **session-timeout** command can be used to clean up a menu with an open connection.

Enable or Disable the Display of Banners

You can control display of the MOTD and line-activation (EXEC) banners. By default, these banners are displayed on all lines. To enable or disable the display of such banners, use the following commands in line configuration mode, as needed:

- **no exec-banner** --Suppresses the display of MOTD and EXEC banners.
- **exec-banner** --Reinstates the display of the EXEC or MOTD banners.
- **no motd-banner** --Suppresses the display of MOTD banners.
- **motd-banner** --Reinstates the display of the MOTD banners.

These commands determine whether the router will display the EXEC banner and the MOTD banner when an EXEC session is created. These banners are defined with the **bannermotd** and **bannerexec** global configuration commands. By default, the MOTD banner and the EXEC banner are enabled on all lines.

Disable the EXEC and MOTD banners using the **noexec-banner** command.

The MOTD banners can also be disabled by the **nomotd-banner** line configuration command, which disables MOTD banners on a line. If the **noexec-banner** command is configured on a line, the MOTD banner will be disabled regardless of whether the **motd-banner**command is enabled or disabled. The table below summarizes the effects of the combination of the **exec-banner** command and the **motd-banner** command.

Table 10: Banners Displayed by exec-banner and motd-banner Command Combinations

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner EXEC banner	None
no motd-banner	EXEC banner	None

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the **noexec-banner** command or **nomotd-banner** command is configured. The table below summarizes the effects of the combination of the **exec-banner** command and the **motd-banner** command for reverse Telnet connections.

Table 11: Banners Displayed Based on exec-banner and motd-banner Command Combinations for Reverse Telnet Sessions to Async Lines

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner Incoming banner	Incoming banner
no motd-banner	Incoming banner	Incoming banner

How to Manage Connections Configure Messages and Banners and Create User Menus

- Managing Connections, page 104
- Configuring Terminal Messages, page 111
- Enabling Terminal Banners, page 113
- Creating a Menu Task List, page 117

Managing Connections

To configure connection-management activities that apply to all supported connection protocols, perform the tasks described in the following sections. All tasks are optional.

- Displaying Current Terminal Settings, page 104
- Escaping Terminal Sessions and Switching to Other Connections, page 105
- Assigning a Logical Name to a Connection, page 106
- Changing a Login Username, page 106
- Accessing a System with TACACS Security, page 107
- Locking Access to a Terminal, page 108
- Sending Messages to Other Terminals, page 109
- Clearing TCP Connections, page 110
- Disconnecting a Line, page 110

Displaying Current Terminal Settings

To display the current settings for the terminal line connection, complete the task in this section:

SUMMARY STEPS

1. **show terminal**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show terminal** **Example:** `Router# show terminal`	Displays current settings for the terminal.

Example

The following example shows sample output of the**showterminal**l command:

```
AccessServer1> show terminal
Line 2, Location: "", Type: "VT220"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: PSI Enabled, Ready, Active, No Exit Banner
Capabilities: none
Modem state: Ready
Group codes:    0
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                        none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: 00:01:07
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are lat pad v120 mop telnet rlogin nasi.  Preferred is lat.
No output characters are padded
No special data dispatching characters
```

Escaping Terminal Sessions and Switching to Other Connections

To switch between sessions by escaping one session and resuming a previously opened session, perform the following steps:

SUMMARY STEPS

1. Escape out of the current session by pressing the escape key sequence (Ctrl-Shift-6 then X [Ctrl^, X] by default) and return to the EXEC prompt.
2. Enter the **where** privileged EXEC command to list the open sessions. All open sessions associated with the current terminal line are displayed.
3. Enter the **resume** privileged EXEC command and the session number to make the connection.

DETAILED STEPS

Step 1 Escape out of the current session by pressing the escape key sequence (Ctrl-Shift-6 then X [Ctrl^, X] by default) and return to the EXEC prompt.

Step 2 Enter the **where** privileged EXEC command to list the open sessions. All open sessions associated with the current terminal line are displayed.

Step 3 Enter the **resume** privileged EXEC command and the session number to make the connection.

You also can resume the previous session by pressing the Return key.

The Ctrl^, X key combination and the **where** and **resume** privileged EXEC commands are available with all supported connection protocols (for example, Telnet).

Assigning a Logical Name to a Connection

To assign a logical name to a connection, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **name-connection**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**name-connection** **Example:** `Router# name-connection`	Assigns a logical name to a connection: • The logical name can be useful for keeping track of multiple connections. • You are prompted for the connection number and name to assign. The **where**privilegedEXEC command displays a list of the assigned logical connection names.

Changing a Login Username

You can change your login username if you must match outgoing access list requirements or other login prompt requirements. A login server must be running and available to use this command. To change a login username, complete the task in this section:

SUMMARY STEPS

1. **login**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**login** **Example:** `Router# login`	Allows you to log in to the system a second time for the purposes of changing your login name. • When you enter this command, the system prompts you for a username and password. Enter the new username and the original password. If the username does not match, but the password does, the Cisco IOS software updates the session with the new username used by the **login** command attempt.

Example

In this example, assume that a user logged in as user1 needs to change the login name to user2:

```
Router> login
Username: user2
Password: <letmein>
Router>
```

In this example, the password letmein is the same password used at the initial login. (The angle brackets in the example indicate that the password is not displayed on the screen when entered.) At the second Router> prompt, the user is now logged in as user2.

- Troubleshooting Tips, page 107

Troubleshooting Tips

If no username and password prompts appear, the network administrator did not specify that a username and password be required at login time. If both the username and password are entered correctly, the session becomes associated with the specified username.

Accessing a System with TACACS Security

To access a system with TACACS security, enter your login name or specify a TACACS server by using the *user@tacacs-server* syntax when the “Username:” prompt appears, complete the tasks in this section:

SUMMARY STEPS

1. **login**
2. Username: *user@tacacs-server*
3. Password: *password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**login** **Example:** `Router> login`	Allows you to log in to the system a second time for the purposes of changing your login name.
Step 2	Username: *user@tacacs-server*	Specifies the new username and authenticates the name with the server specified with the *tacacs-server* argument.

	Command or Action	Purpose
	Example: `Username: myname@company1`	
Step 3	Password: *password* **Example:** `Password: guessme`	Specifies the TACACS password for the username specified in Step 2.

Example

In the following example, user2 specifies the TACACS host host1 to authenticate the password:

```
Router> login

Username: user2@host1

Translating “HOST1”...domain server (131.108.1.111) [OK]

Password: <letmein2>
```

- Troubleshooting Tips, page 108

Troubleshooting Tips

Only the specified host (tacacs-server) is accessed for user authentication information.

If you do not specify a host, the router tries each of the TACACS servers in the list until it receives a response. If you specify a host that does not respond, no other TACACS server will be queried. The router either will deny access or it will function, according to the action specified by the **tacacs-serverlast-resort** global configuration command, if it is configured. If you specified a TACACS server host with the *user@tacacs-server* argument, the TACACS server specified is used for all subsequent authentication or notification queries, with the possible exception of Serial Line Internet Protocol (SLIP) address queries.

For more information on configuring TACACS, refer to the **tacacs-serverhost** global configuration command in the “TACACS, Extended TACACS, and TACACS+ Commands” chapter of the Cisco IOS Security Command Reference .

For an example of changing a login name, see the “Example: Changing a Login Username and Password ” section.

Locking Access to a Terminal

To lock access to your terminal session while keeping your connection open by setting a temporary password, complete the tasks in this section.

Note For this temporary locking feature to work, the line must first be configured to allow locking (using the **lockable** line-configuration mode command).

SUMMARY STEPS

1. Issue the **lock** command in user or privileged EXEC mode.
2. Enter a password, which can be any arbitrary string. The system will prompt you to confirm the password. The screen then is cleared, and the message “Locked” is displayed.
3. To regain access to your session, reenter the password.

DETAILED STEPS

Step 1 Issue the **lock** command in user or privileged EXEC mode.
When you issue this command, the system will prompt you for a password.

Step 2 Enter a password, which can be any arbitrary string. The system will prompt you to confirm the password. The screen then is cleared, and the message “Locked” is displayed.

Step 3 To regain access to your session, reenter the password.

Example

The following is an example of the prompts displayed after the **lock** command is entered. Note that the entered password does not appear on screen.

```
Router# lock

Password:
Again:
                        Locked
Password:
Router#
```

The Cisco IOS software honors session timeouts on locked lines. You must clear the line to remove this feature.

Sending Messages to Other Terminals

To send messages to one or all terminals, for example to inform users of an impending shutdown, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **send** {*line-number* | *****}

DETAILED STEPS

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

Step 2	**send** {*line-number* | *****}
	Example:
	`Router# send *`
		Sends a message to other terminals. Using the * sends messages to all terminals:
		• The system prompts for the message, which can be up to 500 characters long. Press Ctrl-Z to end the message. Press Ctrl-C to abort the command.

Clearing TCP Connections

To clear a TCP connection, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. Router# **clear tcp**{**line***line-number* | **local***host-name port* **remote***host-name port* |**tcb** *tcb-address* }

DETAILED STEPS

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

Step 2	Router# **clear tcp**{**line***line-number* | **local***host-name port* **remote***host-name port* |**tcb** *tcb-address* }
	Example:
	`Router# clear tcp line 2`
		Clears a TCP connection:
		• The **clear tcp** command is particularly useful for clearing non-functioning TCP connections.
		• **line** *line-number* --Terminates the TCP connection on the specified tty line. All TCP sessions initiated from that tty line are also terminated.
		• **local** *host-name port* **remote** *host-name port* --Terminates the specific TCP connection identified by the hostname/port pair of the local and remote router.

Disconnecting a Line

To disconnect a line, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **disconnect** [*connection*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**disconnect** [*connection*] **Example:** `Router# disconnect`	Disconnects a line. **Note** Avoid disconnecting a line to end a session. Instead, log out of the host to allow the router to clear the connection. You should disconnect a line only if you cannot log out of an active session (for example, if the line is stuck or frozen). If your terminal or computer running a terminal-emulation application is connected physically to the console port of the router, you can also disconnect from the router by physically disconnecting the cable from the console port of the router.

Configuring Terminal Messages

To configure messages that can be displayed to terminal users that connect to the system, perform any of the tasks found in the following sections. All tasks are optional.

- Enabling an Idle Terminal Message, page 111
- Configuring a “Line in Use” Message, page 112
- Configuring a “Host Failed” Message, page 113

Enabling an Idle Terminal Message

To enable the idle terminal message, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure line**
3. **vacant-message** [*d message d*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure line** **Example:** `Router# configure line`	Enters line configuration mode.

	Command or Action	Purpose

Step 3	**vacant-message** [*d message d*]
	Example:
	`Router(config-line)# vacant-message &tty# is now available`
	Example:
	`<blank line>`
	Example:
	`Press RETURN to get started.&`
		Configures the system to display an idle terminal message. The argument *d* indicates any delimiting character.
		Note You can configure the system to display a message when a console or terminal is not in use. Also called a *vacant message* , this message is different from the banner message displayed when a user logs in to the system.

- Troubleshooting Tips, page 112

Troubleshooting Tips

Commands requiring a delimiting character (the *d* argument) are used throughout this chapter. Any character can be used as the delimiting character, but we recommend the use of the quote sign ("), because this character is unlikely to be needed within the message itself. Other commonly used delimiting characters include the percent sign (%) or the forward slash (/), but because these characters have meanings within certain Cisco IOS commands, they are not recommended. For example, to set the vacant message to This terminal is idle you would enter the command **vacant-message"Thisterminalisidle"**.

Configuring a “Line in Use” Message

To configure the system to display a “line in use” message when an incoming connection is attempted and all rotary group or other lines are in use, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure line**
3. **refuse-message** *d message d*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure line**	Enters line configuration mode.

	Command or Action	Purpose
	Example: `Router# configure line`	
Step 3	**refuse-message** *d message d* **Example:** `Router(config-line)# refuse-message & line in use &`	Configures the system to display a “line in use” message. The argument *d* indicates any delimiting character. **Note** If you do not define such a message, the user receives a system-generated error message when all lines are in use. You also can use this message to provide the user with further instructions.

Configuring a “Host Failed” Message

To configure the system to display a “host failed” message when a Telnet connection with a specific host fails, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure line**
3. **busy-message** *hostname d message d*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure line** **Example:** `Router# configure line`	Enters line configuration mode.
Step 3	**busy-message** *hostname d message d* **Example:** `Router(config-line)# busy-message network1 & host failed &`	Configures the system to display a “host failed” message. The argument *d* indicates any delimiting character.

Enabling Terminal Banners

Banners are informational messages that can be displayed to users. To enable terminal banners, perform any of the tasks in the following sections. All tasks are optional.

- Configuring a Message-of-the-Day Banner, page 114

- Configuring a Login Banner, page 114
- Configuring an EXEC Banner, page 115
- Configuring a Banner Sent on Incoming Connections, page 116
- Configuring a SLIP-PPP Banner Message, page 116

Configuring a Message-of-the-Day Banner

You can configure a message-of-the-day (MOTD) banner to be displayed on all connected terminals. This banner is displayed at login and is useful for sending messages (such as impending system shutdowns) that affect all network users. To configure the MOTD banner, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner motd** *d message d*

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	**banner motd** *d message d* **Example:** `Router(config)# banner motd &system will be unavailable from 15:00 to 19:00 today&`	Configures the system to display a message-of-the-day banner. The argument *d* indicates any delimiting character.

Configuring a Login Banner

You can configure a login banner to be displayed on all connected terminals after the MOTD banner appears and before the login prompts. To configure a login banner, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner login** *d message d*

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	**banner login** *d message d* **Example:** `Router(config)# banner login &Access for authorized users only. Please enter your username and password.&`	Configures the system to display a banner before the username and password login prompts. The argument *d* indicates any delimiting character. **Note** The login banner cannot be disabled on a per-line basis. To globally disable the login banner, you must delete the login banner with the **no banner login** command.

Configuring an EXEC Banner

You can configure a banner to be displayed whenever an EXEC process is initiated. For example, this banner will be displayed to a user using Telnet to access the system after entering a username and password, but before the user EXEC mode prompt is displayed. To configure an EXEC banner, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner exec** *d message d*

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.

	Command or Action	Purpose
Step 3	**banner exec** *d message d* **Example:** `Router(config)# banner exec &Session activated on line $(line), $(line-desc). Enter commands at the prompt.&`	Configures the system to display a banner whenever an EXEC process is initiated. The argument *d* indicates any delimiting character. **Note** You can include tokens in the form $(token) in the message text. Tokens will be replaced with the corresponding configuration variable.

Configuring a Banner Sent on Incoming Connections

To configure a banner that is sent on incoming connections, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner incoming** *d message d*

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	**banner incoming** *d message d* **Example:** `Router(config)# banner incoming &You have entered $(hostname).$(domain) on line $(line) ($(line-desc))&`	Configures the system to display a banner when there is an incoming connection to a terminal line from a host on the network. The argument *d* indicates any delimiting character. **Note** You can include tokens in the form $(token) in the message text. Tokens will be replaced with the corresponding configuration variable. **Note** You can configure a banner to be displayed on terminals connected to reverse Telnet lines to provide instructions to users of these types of connections. Reverse Telnet connections are described in more detail in the Configuring and Managing External Modems chapter of the Cisco IOS Dial Technologies Configuration Guide, Release 12.4.

Configuring a SLIP-PPP Banner Message

To configure a SLIP-PPP banner message, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner slip-ppp** *d message d*

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	**banner slip-ppp** *d message d* **Example:** `Router(config)# banner slip-ppp &Entering encapsulation mode. Async interface address is unnumbered (Ethernet0) Your IP address is 10.000.0.0 MTU is 1500 bytes &`	Configures a SLIP-PPP banner to display a customized message. The argument *d* indicates any delimiting character. **Note** Default banner messages have been known to cause connectivity problems in some non-Cisco SLIP and PPP dialup software. You can customize the SLIP-PPP banner message to make Cisco SLIP and PPP compatible with non-Cisco dialup software. **Note** You can include tokens in the form $(token) in the message text. Tokens will be replaced with the corresponding configuration variable.

Creating a Menu Task List

- Specifying the Menu Title, page 118
- Clearing the Screen, page 119
- SpecifyingtheMenuPrompt, page 120
- Specifying the Menu Item Text, page 120
- Specifying the Underlying Command for the Menu Item, page 121
- Specifying Connection Resumption, page 123
- Using the resume next Command, page 124
- Specifying the Default Command for the Menu, page 124
- Creating a Submenu, page 125
- Creating Hidden Menu Entries, page 128
- Specifying Menu Display Configuration Options, page 128
- Configuring the Menu to Operate in Line Mode, page 129
- Displaying Single-Spaced Menus, page 129
- Displaying an Informational Status Line, page 130
- Specifying per-Item Menu Options, page 131
- Invoking the Menu, page 132

- Deleting the Menu from the Configuration, page 132

Specifying the Menu Title

To specify an identifying title for the menu, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **title** *d title d*

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	**menu** *menu-name* **title** *d title d* **Example:** `Router(config)# menu Access1 title &Welcome to Access1 Internet Services&`	Specifies the title for the menu. The argument d indicates any delimiting character.

Example

The following example specifies the title that is displayed when the OnRamp menu is selected. The following four main elements create the title:

- The**menutitle** command
- Delimiter characters that open and close the title text
- Escape characters to clear the screen (optional)
- Title text

The following example shows the command used to create the title for the menu shown in the Typical Menu Example figure in the Create Menu section:

```
Router(config)# menu OnRamp title %^[[H^[[J
Enter TEXT message.  End with the character '%'.
               Welcome to OnRamp Internet Services

       Type a number to select an option;
              Type 9 to exit the menu.
%
Router(config)#
```

You can position the title of the menu horizontally by preceding the title text with blank characters. You can also add lines of space above and below the title by pressing Enter.

In this example, the title text consists of the following elements:

- One-line title
- Space
- Two-line menu instruction banner

Title text must be enclosed within text delimiter characters--the percent sign character (%) in this example. Title text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), or tilde (~). You can use any character that is not likely to be used within the text of the title as delimiter characters. Ctrl-C is reserved for special use and should not be used in the text of the title.

This title text example also includes an escape character sequence to clear the screen before displaying the menu. In this case the string ^[[H^[[J is an escape string used by many VT100-compatible terminals to clear the screen. To enter it, you must enter Ctrl-V before each escape character (^[).

Clearing the Screen

To clear the screen before displaying the menu, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **clear-screen**

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	**menu** *menu-name* **clear-screen** **Example:** `Router(config)# menu Access1 clear-screen`	Specifies screen clearing before displaying menus and submenus. **Note** This option uses a terminal-independent mechanism based on termcap entries defined in the router and the terminal type configured for the user terminal. The **menu clear-screen** command allows the same menu to be used on multiple types of terminals instead of terminal-specific strings being embedded within menu titles. If the termcap entry does not contain a clear string, the menu system inserts 24 new lines, causing all existing text to scroll off the top of the terminal screen.

Example

The following example clears the screen before displacing the OnRamp menu or a submenu:

```
Router(config)# menu OnRamp clear-screen
```

SpecifyingtheMenuPrompt

To specify a menu prompt, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **prompt** *d prompt d*

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	**menu** *menu-name* **prompt** *d prompt d*
	Example:
	`Router(config)# menu Access1 prompt /`
	Example:
	`Enter TEXT message.  End with the character '/'.`
	Example:
	`Select an item. /`
		Specifies the prompt for the menu. The argument *d* indicates any delimiting character.:
		• A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.

Specifying the Menu Item Text

Each displayed menu entry consists of the selection key (number, letter, or string) and the text describing the action to be performed. You can specify descriptive text for a maximum number of 18 menu items. Because each menu entry represents a single user interface command, you must specify the menu item text one entry at a time. To specify the menu item text, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **text** *menu-item menu-text*

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	**menu** *menu-name* **text** *menu-item menu-text* **Example:** `Router(config)# menu Access1 text 1 Read email`	Specifies the text for the menu item.

Example

The following example specifies the text that is displayed for the three entries in the OnRamp menu:

```
Router(config)# menu OnRamp text 1 Read email
Router(config)# menu OnRamp text 2 UNIX Internet Access
Router(config)# menu OnRamp text 9 Exit menu system
```

You can provide access to context-sensitive help by creating a “help server” host and using a menu entry to make a connection to that host.

- Troubleshooting Tips, page 121

Troubleshooting Tips

Menu selection keys need not be contiguous. You can provide consistency across menus by assigning a particular number, letter, or string to a special function--such as Help or Exit--regardless of the number of menu entries in a given menu. For example, menu entry H could be reserved for help across all menus.

When more than nine menu items are defined in a menu, the **menuline-mode** and **menusingle-space** global configuration commands are activated automatically. The commands can be configured explicitly for menus of nine items or fewer. For more information on these commands, see the section “Specifying Menu Display Configuration Options ” later in this chapter.

Specifying the Underlying Command for the Menu Item

Each displayed menu entry issues a user interface command when the user enters its key. Each menu entry can have only a single command associated with it. To specify the underlying menu item command, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **command** *menu-item command*

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	**menu** *menu-name* **command** *menu-item command* **Example:** `Router(config)# menu OnRamp command 1 rlogin mailsys`	Specifies the command to be performed when the menu item is selected.

Example

The following example specifies the commands that are associated with the three entries in the OnRamp menu:

```
Router(config)# menu OnRamp command 1 rlogin mailsys
Router(config)# menu OnRamp command 2 rlogin unix.cisco.com
Router(config)# menu OnRamp command 9 menu-exit
```

- Troubleshooting Tips, page 122

Troubleshooting Tips

The **menu-exit** command is available only from within menus. This command provides a way to return to a higher-level menu or to exit the menu system.

When a menu item allows you to make a connection, the menu item should also contain entries that can be used to resume connections; otherwise, when you try to escape from a connection and return to the menu, there is no way to resume the session. It will sit idle until you log out.

You can build the **resumeconnection** user EXEC command into a menu entry so that the user can resume a connection, or you can configure the line using the **escape-charnone** command to prevent users from escaping their sessions.

Specifying Connection Resumption

To specify connection resumption as part of the menu item command, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **command** *menu-item* **resume** [*connection*] **/connect** [*connect string*]

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	**menu** *menu-name* **command** *menu-item* **resume** [*connection*] **/connect** [*connect string*] **Example:** `Router(config)#  menu newmenu command 1 resume mailsys / connect rlogin mailsys`	Specifies that the**resume** command will be performed when the menu item is selected: • Embedding the **resume** command within the **menu** command permits a user to resume the named connection or make another connection using the specified name, if there is no active connection by that name. As an option, you can also supply the connect string needed to connect initially. When you do not supply this connect string, the command uses the specified connection name. • You can use the **resume** command in the following menu entries: ◦ Embedded in a menu entry ◦ As a separate, specific menu entry ◦ As a “rotary” menu entry that steps through several connections

Examples

In the following example, the **resume** command is embedded in the **menu** command so that selecting the menu item either starts the specified connection session (if one is not already open) or resumes the session (if one is already open):

```
Router(config)# menu newmenu text 1 Read email
Router(config)# menu newmenu command 1 resume mailsys /connect rlogin mailsys
```

In the following example, the **resume** command is used in a separate menu entry (entry 3) to resume a specific connection:

```
Router(config)# menu newmenu text 3 Resume UNIX Internet Access
Router(config)# menu newmenu command 3 resume unix.cisco.com
```

Using the resume next Command

You use the **resume/next** command to resume the next open connection in the user list of connections. This command allows you to create a single menu entry that advances through all of the user connections. To specify **resume/next** connection resumption as part of the menu item command, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **command** *menu-item* **resume/next**

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	**menu** *menu-name* **command** *menu-item* **resume/next** **Example:** `Router(config)# menu newmenu command 6 resume/next`	Specifies **resume/next** connection resumption.

Example

The following example shows a menu entry (entry 6) created to advance through all of the user connections:

```
Router(config)# menu newmenu text 6 Resume next connection
Router(config)# menu newmenu command 6 resume/next
```

Specifying the Default Command for the Menu

When a user presses Enter without specifying an item, the router performs the command for the default item. To specify the default item, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **default** *menu-item*

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	**menu** *menu-name* **default** *menu-item*
	Example:
	`Router(config)# menu Access1 9 text Exit the menu`
	Example:
	`menu Access1 9 command menu-exit`
	Example:
	`menu Access1 default 9`
		Specifies the command to be performed when the menu user does not select a menu item.

Creating a Submenu

To create submenus that are opened by selecting a higher-level menu entry, use the **menu** command to invoke a menu in a line menu entry. To specify a submenu item command, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **text** *menu-item menu-text*
4. **menu** *menu-name* **command** *menu-item* **menu** *menu-name2*
5. Router(config)#**menu***menu-name***title** *delimiter menu-titledelimiter*
6. **menu** *menu-name* **text** *menu-item menu-text*
7. **menu** *menu-name* **command** *menu-item command*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. - Enter your password if prompted.

	Command or Action	Purpose
	Example: `Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**menu** *menu-name* **text** *menu-item menu-text* **Example:** `Router(config)# menu Access1 text 1 IBM Information Systems`	Specifies the menu item that invokes the submenu.
Step 4	**menu** *menu-name* **command** *menu-item* **menu** *menu-name2* **Example:** `Router(config)# menu Access1 command 1 tn3270 vms.cisco.com`	Specifies the command to be used when the menu item is selected.

Step 5	Router(config)#**menu***menu-name***title** *delimiter menu-titledelimiter*
	Example:
	`Router(config)# menu Access1 title /^[[H^[[J`
	Example:
	`Enter TEXT message.  End with the character '/'.`
	Example:
	`Welcome to Access1 Internet Services`
	Example:
	`Type a number to select an option;`
	Example:
	`Type 9 to exit the menu.`
	Example:
	`/`
		Specifies the title for the submenu.

Step 6	**menu** *menu-name* **text** *menu-item menu-text* **Example:** `Router(config)# menu Access1 text 2 UNIX Internet Access`	Specifies the submenu item.

	Command or Action	Purpose
Step 7	**menu** *menu-name* **command** *menu-item command* **Example:** `Router(config)# menu Access1 command 2 rlogin unix.cisco.com`	Specifies the command to be used when the submenu item is selected. Repeat this command as needed.

Examples

The following example specifies that the menu item (entry 8) activates the submenu in the OnRamp menu:

```
Router(config)# menu OnRamp text 8 Set terminal type
```

The following example specifies the command that is performed when the menu item (entry 8) is selected in the OnRamp menu:

```
Router(config)# menu OnRamp command 8 menu Terminals
```

The following example specifies the title for the Terminals submenu:

```
Router(config)# menu Terminals title /
                     Supported Terminal Types

        Type a number to select an option;
       Type 9 to return to the previous menu.
```

The following example specifies the submenu items for the Terminals submenu:

```
Router(config)# menu Terminals text 1 DEC VT420 or similar
Router(config)# menu Terminals text 2 Heath H-19
Router(config)# menu Terminals text 3 IBM 3051 or equivalent
Router(config)# menu Terminals text 4 Macintosh with gterm emulator
Router(config)# menu Terminals text 9 Return to previous menu
```

The following example specifies the commands associated with the items in the Terminals submenu:

```
Router(config)# menu Terminals command 1 term terminal-type vt420
Router(config)# menu Terminals command 2 term terminal-type h19
Router(config)# menu Terminals command 3 term terminal-type ibm3051
Router(config)# menu Terminals command 4 term terminal-type gterm
Router(config)# menu Terminals command 9 menu-exit
```

When you select entry 8 on the main menu, the following Terminals submenu appears:

```
      Supported Terminal Types
  Type a number to select an option;
Type 9 to return to the previous menu.
1     DEC VT420 or similar
2     Heath H-19
3     IBM 3051 or equivalent
4     Macintosh with gterm emulator
9     Return to previous menu
```

Note If you nest too many levels of menus, the system displays an error message on the terminal and returns to the previous menu level.

Creating Hidden Menu Entries

A hidden menu entry is a menu item that contains a selection key but no associated text describing the action to be performed. Include this type of menu entry to aid system administrators that provide help to users. The normal procedure is to specify a menu command but omit specifying any text for the item. To create a hidden menu item, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **command** *menu-item command*

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	**menu** *menu-name* **command** *menu-item command* **Example:** `Router(config)# menu OnRamp command 7 show whoami Terminals submenu of OnRamp Internet Access menu`	Specifies the command to be used when the hidden menu entry is selected.

The following example shows the command associated with the submenu entry in the OnRamp menu:

```
Router(config)# menu OnRamp command 7 show whoami
```

If additional text is appended to the**showwhoami** command, that text is displayed as part of the data about the line. For example, the hidden menu entry created by the command:

```
Router(config)# menu OnRamp command 7 show whoami Terminals submenu of OnRamp Internet
Access menu
```

Displays information similar to the following:

```
Comm Server "cs101", Line 0 at 0 bps. Location "Second floor, West"
Additional data: Terminals submenu of OnRamp Internet Access menu
To prevent the information from being lost if the menu display clears the screen, this
command always displays a --More-- prompt before returning.
```

Specifying Menu Display Configuration Options

In addition to the **menuclear-screen** global configuration command (described in the “Specifying the Menu Title ” section), the following three **menu** commands define menu functions:

- **menu line-mode**
- **menu single-space**
- **menu status-line**

Configuring the Menu to Operate in Line Mode

To configure the menu to operate in line mode, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **line-mode**

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	**menu** *menu-name* **line-mode** **Example:** `Router(config)# menu OnRamp line-mode`	Configures the menu to use line mode for entering menu items: • The line-mode option is invoked automatically when more than nine menu items are defined, but it can also be configured explicitly for menus of nine items or fewer. • In a menu of nine or fewer items, you ordinarily select a menu item by entering the item number or a letter. In line mode, you select a menu entry by entering the item key and pressing Enter. The line mode allows you to backspace over the selection and enter another before pressing Enter to issue the command. This function allows you to change the selection before you invoke the command. • In order to use strings as selection keys, you must enable the **menu line-mode** command.

Displaying Single-Spaced Menus

To use the **single-space** option to display single-spaced menus, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **single-space**

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	**menu** *menu-name* **single-space** **Example:** `Router(config)# menu Access1 single-space`	Configures the specified menu to display single-spaced: • If there are nine or fewer menu items, the Cisco IOS software ordinarily displays the menu items double-spaced. In a menu of more than nine items, the **single-space** option is activated automatically to fit the menu into a normal 24-line terminal screen. However, the single-space option also can be configured explicitly for menus of nine or fewer items.

Displaying an Informational Status Line

To display the informational status line, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **status-line**

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**	Enters global configuration mode.

	Command or Action	Purpose
	Example: `Router# configure terminal`	
Step 3	**menu** *menu-name* **status-line** **Example:** `Router(config)# menu OnRamp status-line`	Configures the specified menu to display a status line: • The **status-line** keyword displays a line of status information about the current user at the top of the terminal screen before the menu title is displayed. This status line includes the router host name, the user line number, and the current terminal type and keymap type (if any).

Specifying per-Item Menu Options

To configure per-item menu options, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **menu** *menu-name* **options** *menu-item* **pause**
4. **menu** *menu-name* **options** *menu-item* **login**

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	**menu** *menu-name* **options** *menu-item* **pause** **Example:** `Router(config)# menu Access1 options 3 pause`	Configures the system to pause after the specified menu item is selected by the user. Enter this command once for each menu item that pauses.
Step 4	**menu** *menu-name* **options** *menu-item* **login** **Example:** `Router(config)# menu Access1 options 3 login`	Configures the specified menu item to require a login before executing the command. Enter this command once for each menu item that requires a login.

Invoking the Menu

To invoke (access) a menu, use the following command in user EXEC or privileged EXEC mode:

SUMMARY STEPS

1. **enable**
2. **menu** *menu-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**menu** *menu-name* **Example:** `Router# menu OnRamp`	Invokes a preconfigured user menu: • You can define menus containing privileged EXEC commands, but users must have privileged access when they start up the menu. • To ensure that a menu is automatically invoked on a line, make sure the menu does not have any exit paths that leave users in an interface they cannot operate, then configure that line with the **autocommandmenu***menu-name* line configuration command. (The **autocommandmenu** *menu-name* command configures the line to automatically execute the**menu***menu-name* command when a user initiates a connection over that line.) • Menus also can be invoked on a per-user basis by defining an **autocommand** command for that local username.

Example

In the following example, the OnRamp menu is invoked:

```
Router# menu OnRamp
      Welcome to OnRamp Internet Services

       Type a number to select an option;
            Type 9 to exit the menu.
1     Read email
2     UNIX Internet access
3     Resume UNIX connection
6     Resume next connection
9     Exit menu system
```

Deleting the Menu from the Configuration

To delete the menu from the configuration, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no menu** *menu-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	**no menu** *menu-name* **Example:** `Router(config)# no menu OnRamp`	Deletes the menu by specifying the menu name. **Note**In order to use the menu again, you must reconfigure the entire menu.

The following example deletes the OnRamp menu from the configuration:

```
Router(config)#
no menu OnRamp
```

Configuration Examples for Connection Management System Banners and User Menus

Example Changing a Login Username and Password

The following example shows how login usernames and passwords can be changed. In this example, a user currently logged in under the username user1 attempts to change that login name to user2. After entering the **login** command, the user enters the new username, but enters an incorrect password. Because the password does not match the original password, the system rejects the attempt to change the username.

```
Router> login
Username: user2
Password:
% Access denied
Still logged in as "user1"
```

Next, the user attempts the login change again, with the username user2, but enters the correct (original) password. This time the password matches the current login information, the login username is changed to user2, and the user is allowed access to the user login information.

```
Router> login
Username: user2
Password:
Router>
```

Example Sending Messages to Other Terminals

The following example shows the process of sending a message to all terminal connections on the router:

```
Router# send *
Enter message, end with CTRL/Z; abort with CTRL/C:
this is a message^Z
Send message? [confirm]
Router#
***
***
*** Message from tty50 to all terminals:
***
this is a message
Router#
```

Example Clearing a TCP IP Connection

The following example clears a TCP connection using its tty line number. The **showtcp** EXEC command displays the line number (tty2) that is used in the **cleartcpprivileged**EXEC command mode.

```
Router# show tcp

    tty2, virtual tty from host router20.cisco.com
    Connection state is ESTAB, I/O status: 1, unread input bytes: 0
    Local host: 171.69.233.7, Local port: 23
    Foreign host: 171.69.61.75, Foreign port: 1058

    Enqueued packets for retransmit: 0, input: 0, saved: 0

    Event Timers (current time is 0x36144):
    Timer          Starts    Wakeups            Next
    Retrans             4          0             0x0
    TimeWait            0          0             0x0
    AckHold             7          4             0x0
    SendWnd             0          0             0x0
    KeepAlive           0          0             0x0
    GiveUp              0          0             0x0
    PmtuAger            0          0             0x0

    iss: 4151109680  snduna: 4151109752  sndnxt: 4151109752     sndwnd:  24576
    irs: 1249472001  rcvnxt: 1249472032  rcvwnd:       4258  delrcvwnd:     30

    SRTT: 710 ms, RTTO: 4442 ms, RTV: 1511 ms, KRTT: 0 ms
    minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 300 ms

Router# clear tcp line 2
    [confirm]
     [OK]
```

The following example clears a TCP connection by specifying its local router hostname and port and its remote router hostname and port. The **showtcpbrief** privileged EXEC command displays the local (Local Address) and remote (Foreign Address) hostnames and ports to use in the **cleartcp**privilegedEXEC command.

```
Router# show tcp brief
```

```
    TCB       Local Address           Foreign Address        (state)
    60A34E9C  router1.cisco.com.23      router20.cisco.1055  ESTAB

Router# clear tcp local router1 23 remote router20 1055
    [confirm]
     [OK]
```

The following example clears a TCP connection using its TCB address. The **showtcpbrief** EXEC command displays the TCB address to use in the **cleartcp** EXEC command.

```
Router# show tcp brief
    TCB       Local Address           Foreign Address        (state)
    60B75E48  router1.cisco.com.23      router20.cisco.1054  ESTAB

Router# clear tcp tcb 60B75E48
    [confirm]
     [OK]
```

Example Configuring Banners

The following example shows how to use the **banner** global configuration commands to notify your users that the server will be reloaded with new software. The **noexec-banner** line configuration command is used to disable EXEC banners and message-of-the-day banners on the vty lines.

```
!
line vty 0 4
 no exec-banner
!
banner exec /
 This is Cisco Systems training group router.

 Unauthorized access prohibited.
 /
!
banner incoming /
 You are connected to a Hayes-compatible modem.

 Enter the appropriate AT commands.
 Remember to reset anything you have changed before disconnecting.
 /
!
banner motd /
 The router will go down at 6pm today for a software upgrade
 /
```

When someone connects to the router, the MOTD banner appears before the login prompt. After the user logs in to the router, the router will display the EXEC banner or incoming banner, depending on the type of connection. For a reverse Telnet login, the router will display the incoming banner. For all other connections, the router will display the EXEC banner.

Example Configuring a SLIP-PPP Banner with Banner Tokens

The following example configures the SLIP-PPP banner using several tokens and the percent sign (%) as the delimiting character:

```
Router(config)# banner slip-ppp %


Enter TEXT message.  End with the character '%'.
Starting $(encap) connection from $(gate-ip) to $(peer-ip) using a maximum packet size of
$(mtu) bytes... %
```

When a user enters the **slip** command, that user will see the following banner. Notice that the **$(***token***)** syntax is replaced by the corresponding configuration variable.

```
Starting SLIP connection from 192.168.69.96 to 172.16.80.8 using a maximum packet size of
1500 bytes...
```

Example Configuring a Menu

The following example allows menu users to use Telnet to access one of three different machines. The user also can display the output of the **showuser** EXEC command and exit the menu. One hidden menu item (configured as menu new command here show version) allows system administrators to display the current software version.

```
menu new title ^C


              Telnet Menu


^C
menu new prompt ^C

Please enter your selection: ^C
menu new text 1 telnet system1
menu new command 1 telnet system1
menu new options 1 pause
menu new text 2 telnet system2
menu new command 2 telnet system2
menu new options 2 pause
menu new text b telnet system3
menu new command b telnet system3
menu new options b pause
menu new text me show user
menu new command me show user
menu new options me pause
menu new command here show version
menu new text Exit Exit
menu new command Exit menu-exit
menu new clear-screen
menu new status-line
menu new default me
menu new line-mode
!
```

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Using the Cisco IOS Web Browser User Interface

The Cisco IOS software includes a Web browser user interface (UI) from which you can issue Cisco IOS commands. The Cisco IOS Web browser UI is accessed from the router home page, and can be customized for your business environment. For example, you can view pages in different languages and save them in Flash memory for easy retrieval.

For a complete description of the Cisco Web browser UI configuration commands in this chapter, refer to the “Cisco IOS Web Browser User Interface Commands”chapter of the *Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the *Cisco IOS Command Reference Master Index* or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco IOS Web Browser User Interface

- You must have Cisco IOS Release 12.2 or a later release installed and running on your network
- To use the Cisco IOS Web browser UI, your computer must have a World Wide Web browser application.

- Most Cisco routers and access servers automatically generate a password protected home page when the HTTP server is enabled on the device. To access the home page, your computer must be on the same network as the router.

Restrictions for Cisco IOS Web Browser User Interface

- The Web browser UI is automatically enabled on the Cisco 1003, Cisco 1004, or Cisco 1005 routers to allow you to use ClickStart to configure your router. For all other Cisco devices, you must enable the Cisco Web browser UI.
- You can issue most Cisco IOS commands using a Web browser by connecting to the home page generated by the Cisco IOS software for your system.
- The Cisco Web browser UI works with most web browsers. Your Web browser must be able to read and submit forms.

Information About Cisco IOS Web Browser User Interface

Customizing the Cisco Web Browser UI

You can customize the HTML pages used by the Cisco Web browser UI to display Cisco IOS command output and Cisco IOS platform-specific variables (for example, a router host name or router address). You can display this information using HTML formatted Server Side Includes (SSIs) that you insert into your custom HTML pages.

Understanding SSIs

SSIs are HTML formatted commands or variables that you insert into HTML pages when you customize Cisco IOS platform configuration pages for a Web browser. These SSI commands and SSI variables display Cisco IOS command output and Cisco IOS platform-specific variables.

Note The majority of the customization features in this section are for the ClickStart EZsetup feature for the Cisco 1000 series, Cisco 1003/1004 series, and Cisco 1005 series routers only.

The Cisco IOS software supports two HTML SSI commands defined for customizing HTML pages: the SSI EXEC command and the SSI ECHO command. The HTML format of the SSI EXEC command is **<!--#execcmd="***xxx***"-->**, and the HTML format of the SSI ECHO command is **<!--#echovar="***yyy***"-->**. (See the section "Customizing HTML Pages Using SSIs" later in this chapter for a description of how to use these commands).

In addition to the two SSI commands, the Cisco IOS software supports several SSI variables defined for customizing HTML pages. SSI variables are used with the SSI ECHO command. One SSI variable is defined for all Cisco IOS platforms (SERVER_NAME), and other SSI variables are specifically defined for ISDN, Frame Relay, and asynchronous serial platforms. The format and a description of all the available SSI variables are provided in the table below. (See the section Customizing HTML Pages Using SSIs later in this chapter for a description of how to use these SSI variables with the SSI ECHO command).

The SSI EXEC command is supported on all platforms. The SSI ECHO command, used with SSI variables, is supported on all platforms listed in the table below.

Table 12: Description of SSI Variables

HTML Format of SSI Variable	Description of Variable Displayed on Browser Page	Cisco IOS Platforms This SSI Is Supported On
SERVER_NAME	Host name of the HTTP server.	All Cisco IOS platforms
EZSETUP_PASSWORD	Enable password (currently left blank).	Cisco 1000 series
EZSETUP_PASSWORD_VERIFY	Repeat of the enable password to verify accuracy (currently left blank).	Cisco 1000 series
EZSETUP_ETHERNET0_ADDRESS	IP address of the Ethernet interface 0.	Cisco 1000 series
EZSETUP_ETHERNET0_MASK	IP mask of the Ethernet interface 0.	Cisco 1000 series
EZSETUP_DNS_ADDRESS	Domain Name System (DNS) address used by the router.	Cisco 1000 series
EZSETUP_STANDARD_DEBUG_Y	Standard debug variable. Returns CHECKED if set to TRUE; otherwise, it is blank.	Cisco 1000 series
EZSETUP_STANDARD_DEBUG_N	Standard debug variable. Returns CHECKED if set to FALSE; otherwise, it is blank.	Cisco 1000 series
EZSETUP_ISDN_SWITCHTYPE	ISDN switch type.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_REMOTE_NAME	Name of remote ISDN system.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_REMOTE_NUMBER	Phone number of remote ISDN system.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_CHAP_PASSWORD	CHAP password of remote ISDN system.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPID1	ISDN SPID 1.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPID2	ISDN SPID 2.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPEED_56	Speed of ISDN interface. Returns CHECKED if set to 56K; otherwise, it is blank.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPEED_64	Speed of ISDN interface. Returns CHECKED if set to 64K; otherwise, it is blank.	Cisco 1003 and Cisco 1004
EZSETUP_FR_ADDRESS	Frame Relay IP address.	Cisco 1005

HTML Format of SSI Variable	Description of Variable Displayed on Browser Page	Cisco IOS Platforms This SSI Is Supported On
EZSETUP_FR_MASK	Frame Relay IP mask.	Cisco 1005
EZSETUP_FR_DLCI	Frame Relay DLCI.	Cisco 1005
EZSETUP_ASYNC_REMOTE_NAME	Name of remote system.	Cisco 1005
EZSETUP_ASYNC_REMOTE_NUMBER	Phone number of remote system.	Cisco 1005
EZSETUP_ASYNC_CHAP_PASSWORD	CHAP password for remote system.	Cisco 1005
EZSETUP_ASYNC_LINE_PASSWORD	Async line password.	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED	Speed of async modem (either 14.4K or 28.8K).	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED_144K	Returns CHECKED if async modem speed is 14.4K; otherwise it is blank.	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED_288K	Returns CHECKED if async modem speed is 28.8K; otherwise it is blank.	Cisco 1005

When you have designed a set of HTML pages that include SSIs, you can copy these pages to a Cisco IOS platform's Flash memory. When you retrieve these pages from Flash memory and display them using a Web browser, any SSI command that was designed into these pages will display either Cisco IOS command output or a current variable or identifier defined in the table below. For example, the SSI ECHO command with the variable SERVER_NAME will display the current host name of the HTTP server you are using, and the SSI ECHO command with the variable EZSETUP_ISDN_SWITCHTYPE will display the current ISDN switch type you are using.

Using SSIs, you can customize set of HTML pages to appear in languages other than English and copy these pages to Flash memory on multiple Cisco IOS platforms. When you retrieve these pages from the Flash memory of a Cisco IOS platform, current variables and identifiers associated with the platform you are currently using are displayed. SSIs save you from needing to duplicate these international pages (considered relatively large images that contain 8-bit or multibyte characters) and store them in the source code for each platform you are using.

- Customizing HTML Pages Using SSIs, page 140
- Copying HTML Pages to Flash Memory, page 141
- Displaying HTML Files Containing SSIs, page 141

Customizing HTML Pages Using SSIs

When you are customizing an HTML page for a Web browser, type **<!--#execcmd=“***xxx***”-->** in your HTML file where you want Cisco IOS command output to appear on the browser page. Replace the *xxx variable* with any Cisco IOS EXEC mode command.

When you are customizing an HTML page for a Web browser, type **<!--#echovar=“***yyy***”-->** in your HTML file where you want a value or identifier associated with a particular Cisco IOS platform (for example, an

ISDN or Frame Relay platform) to appear on the browser page. Replace the *yyy* variable with an SSI variable described in the Description of SSI Variables table in the Understanding SSIs module.

Copying HTML Pages to Flash Memory

Once you have customized HTML pages using SSIs, copy your HTML pages to a Cisco IOS platform's Flash memory. To do this, save your pages using a filename appended with ".shtml" (for example, *filename* .shtml) and copy your file to Flash memory using a**copy** EXEC command (for example, the **copytftpflash** command). (Refer to the Cisco IOS command references for a **copy** command compatible with your platform.)

Displaying HTML Files Containing SSIs

When the Cisco Web browser UI is enabled, you can retrieve your HTML page from Flash memory and display it on the Cisco Web browser by typing **http://***router*/**flash/***filename*in the URL window. Replace *router* with the host name or IP address of the current Cisco IOS platform you are using, and replace *filename* with the name of the file you created with ".shtml" appended, for example, http://myrouter/flash/ssi_file.shtml.

Methods of User Authentication

The **iphttpauthentication**command specifies the authentication method to be used for login when a client connects to the HTTP server. Use of the **iphttpauthenticationaaa** command option is recommended. The**enable**, **local**, and **tacacs** methods should be specified using the **aaaauthenticationlogin** command.

If you do not use this command, the default authentication method is used. The default method of authentication for the HTTP server is to use the configured "enable" password. The "enable" password is configured with the **enablepassword** global configuration command. If the enable password is used as the HTTP server login authentication method, the client connects to the HTTP server with a default privilege level of 15.

Note When the "enable" password is used as the HTTP server login authentication method, any username entered will be ignored; the server will only verify the "enable" password. This may make it easier for an attacker to access the router. Because a username and password pair is more secure than using only a password for authentication, using only "enable" password for authentication is strongly discouraged. Instead, use of the **local** or **tacacs** authentication options, configured as part of a global Authentication, Authorization, and Accounting (AAA) framework, is recommended. To configure HTTP access as part of a AAA policy, use the **iphttpauthenticationaaa** command option. The "local", "tacacs", or "enable" authentication methods should then be configured using the **aaaauthenticationlogin** command.

For information about adding users into the local username database, refer to the Cisco IOS Security Configuration Guide.

Methods for Entering Commands

Entering Commands Using Hypertext Links

To enter a command using hypertext links, scroll through the commands listed at the bottom of the screen and click the one you want to execute. If the link is a complete command, it is executed. If the command has more parameters, another list of command hypertext links is displayed. Scroll through this second list and click the one you want to execute.

If the command is a request for information, like a **show** EXEC command, the information is displayed in the Web browser window.

If the command requires a variable, a form in which you can enter the variable is displayed.

Entering Commands Using the Command Field

Entering the command in the command field is just like entering it at a terminal console. Enter the command using the syntax documented in the Cisco IOS command reference. If you are uncertain of the options available for a particular command, type a question mark (**?**).

For example, entering **show?**in the command field displays the parameters for the **show**EXEC command. The Cisco Web browser UI displays the parameters as hypertext links. To select a parameter, you can either click on one of the links or you can enter the parameter in the command field.

Entering Commands Using the URL Window

You can issue a command using the URL window for the Web browser. To issue a command using the URL window, use the following syntax:

http:// *router-name* / [**level**/*level*/]*command-mode*/*command*

The table below lists the URL arguments you must use when requesting a web page.

Table 13: Web Browser URL Argument Descriptions

Argument	Description
router-name	Name of the router being configured.
level/ *level*	(Optional) The privilege level you are requesting at which you are requesting access.
mode	The mode the command will be executed in, such as EXEC, configuration, or interface.
command	The command you want to execute. Replace spaces in the command syntax with forward slashes. If you do not specify a command in the URL, your browser will display a web page listing all of the commands available for the specified command mode.

For example, to execute a **showrunning-configuration** EXEC command on a router named example, you would enter the following in the URL window:

```
http://example/exec/show/running-configuration
```

After issuing this command, the Cisco Web browser UI will display the running configuration for the router.

The difference between entering a command in the Command field and entering a command in the URL window is that in the URL window, forward slashes should be used instead of spaces in the command syntax.

Specifying the Method for User Authentication

To specify how HTTP server users are authenticated, use the following command in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http authentication** {**aaa**|**enable** | **local** | **tacacs**}

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	**ip http authentication** {**aaa**|**enable** | **local** | **tacacs**}
	Example:
	`Router(config)# ip http authentication tacacs`
		Specifies how the HTTP server users are authenticated.

Example

The following example specifies that the method configured for AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method.

```
Router(config)# ip http authentication aaa
Router(config)# aaa authentication login default local
```

Default Privilege Level

The default privilege level when accessing a router home page is privilege level 15 (global access). If privilege levels have been configured on the router and you have been assigned a privilege level other than 15, you must specify the privilege level to access the router home page.

When you specify a privilege level, the Cisco Web Browser UI will display and accept only those commands that have been defined for your user level. (For more information about privilege levels, see the Configuring Passwords and Privileges chapter in the Cisco IOS Security Configuration Guide.)

How to Configure and Use the Cisco IOS Web Browser User Interface

Enabling the Cisco IOS Web Browser UI

To enable the Cisco Web browser UI, you must enable the HTTP server on your router:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**

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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the HTTP server (web server) on the system.

Configuring Access to the Cisco IOS Web Browser UI

To control access to the Cisco Web browser UI, you can specify the authentication method for the HTTP server, apply an access list to the HTTP server, and assign a port number for the HTTP server, as described in the following sections.

- Applying an Access List to the HTTP Server, page 145
- Changing the HTTP Server Port Number, page 146

Specifying the Method for User Authentication

To specify how HTTP server users are authenticated, use the following command in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http authentication** {**aaa**|**enable** | **local** | **tacacs**}

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	**ip http authentication** {**aaa**|**enable** | **local** | **tacacs**}
	Example:
	`Router(config)# ip http authentication tacacs`
		Specifies how the HTTP server users are authenticated.

Example

The following example specifies that the method configured for AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method.

```
Router(config)# ip http authentication aaa
Router(config)# aaa authentication login default local
```

Applying an Access List to the HTTP Server

To control which hosts can access the HTTP server used by the Cisco Web browser UI, you can apply an access list:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http access-class** {*access-list-number* |*access-list-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	**ip http access-class** {*access-list-number* |*access-list-name* }
	Example:
	`Router(config)# ip http access-class 20`
		Applies an access list to the HTTP server used by the Cisco IOS ClickStart software or the Cisco Web browser user interface.

Example

In the following example the access list identified as “20” is defined and assigned to the HTTP server:

```
Router(config)# ip access-list standard 20

Router(config-std-nacl)# permit 209.165.202.0 0.0.0.255

Router(config-std-nacl)# permit 209.165.0.0 0.0.255.255

Router(config-std-nacl)# permit 209.0.0.0 0.255.255.255

! (Note: all other access implicitly denied)
Router(config-std-nacl)# exit

Router(config)# ip http access-class 20
```

Changing the HTTP Server Port Number

By default, the HTTP server uses port 80 on the router. To assign the Cisco Web browser UI to a different port, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http port** *number*

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	**ip http port** *number* **Example:** `Router(config)# ip http port 32`	Assigns a port number to be used by the Cisco IOS Web browser interface.

Accessing and Using the Cisco IOS Web Browser UI

This section describes the tasks used to access the Cisco IOS Web browser UI and issue commands:

- Accessing the Router Home Page, page 147
- Changing the Default Privilege Level, page 148

Accessing the Router Home Page

To access a router home page, perform the following steps:

SUMMARY STEPS

1. Enter **http://***router-name***/** in the URL field of your Web browser and press **Return** . (For example, to access a Cisco router named cacophony, type **http://cacophony/**.) The browser then prompts you for the password.
2. Enter the password. The required password is dependent on the user authentication method configured for the HTTP server (using the **ip http authentication** global configuration command).

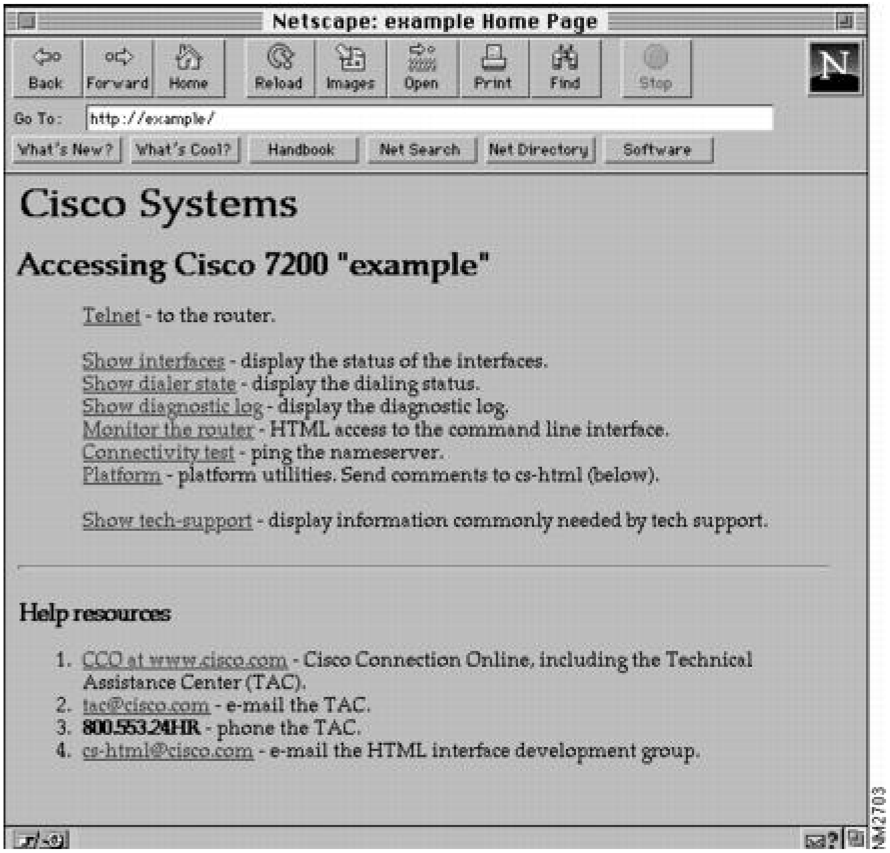
DETAILED STEPS

Step 1 Enter **http://***router-name***/** in the URL field of your Web browser and press **Return** . (For example, to access a Cisco router named cacophony, type **http://cacophony/**.) The browser then prompts you for the password.

Step 2 Enter the password. The required password is dependent on the user authentication method configured for the HTTP server (using the **ip http authentication** global configuration command).

After entering the password, the browser will display the router home page. An example of a router home page is shown below.

Figure 14: Example of a Home Page for a Cisco 7200 Series Router



Cisco Systems

Accessing Cisco 7200 "example"

Telnet - to the router.

Show interfaces - display the status of the interfaces.
Show dialer state - display the dialing status.
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface.
Connectivity test - ping the nameserver.
Platform - platform utilities. Send comments to cs-html (below).

Show tech-support - display information commonly needed by tech support.

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. **800.553.24HR** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

Changing the Default Privilege Level

To access a router Web page for a preassigned privilege level other than the default of 15, perform the following steps:

SUMMARY STEPS

1. E nter **http://***router-name***/level/***level***/exec** in the URL field of your Web browser and press **Return**. For example, to request access to EXEC mode at user privilege level of 12 on a Cisco router named cacophony, type **http://cacophony/level/12/exec**. The browser will then prompt you for your username and password.
2. Enter your username and password and press **Return**. The required password is dependent on the user authentication method configured for the HTTP server. The Web browser will display a Web page specific to your user privilege level.

DETAILED STEPS

Step 1 E nter **http://***router-name***/level/***level***/exec** in the URL field of your Web browser and press **Return**. For example, to request access to EXEC mode at user privilege level of 12 on a Cisco router named cacophony, type **http://cacophony/level/12/exec**. The browser will then prompt you for your username and password.

Step 2 Enter your username and password and press **Return**. The required password is dependent on the user authentication method configured for the HTTP server. The Web browser will display a Web page specific to your user privilege level.

Configuration Examples for the Cisco IOS Web Browser User Interface

- Example SSI EXEC Command, page 149
- Example SSI ECHO Command, page 150

Example SSI EXEC Command

The following example shows how the HTML SSI EXEC command can be used to execute a command. In this example, the Cisco IOS **showusers** EXEC command is executed.

The contents of the HTML file in Flash memory are as follows:

```
<HTML>
<HEAD>
<TITLE> SSI EXEC Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI EXEC command
<HR>
<PRE>
<!--#exec cmd=“show users”-->
</PRE>
<BR>
</BODY>
</HTML>
```

The contents that the Web browser receives when the HTML file is retrieved from Flash memory are as follows:

```
<HTML>
<HEAD>
<TITLE> SSI EXEC Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI EXEC command
<HR>
USERS:<BR>
<PRE>
Line    User  Host(s) Idle  Location
0 con 0       idle      12
2 vty 0       idle       0  router.cisco.com
</PRE>
```

```
<BR>
</BODY>
</HTML>
```

The Web browser shows the following text:

```
This is an example of the SSI EXEC command
------------------------------------------
USERS:
Line    User  Host(s) Idle  Location
0 con 0       idle      12
2 vty 0       idle       0  router.cisco.com
```

Example SSI ECHO Command

The following is an example of the HTML SSI ECHO command used with the SSI variable *SERVER_NAME* to display the Cisco IOS platform host name "rain."

The contents of the HTML file in Flash memory is as follows:

```
<HTML>
<HEAD>
<TITLE>SSI Echo Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI echo command
<HR>
The name of this server is:<BR>
<!--#echo var="SERVER_NAME"-->
<BR>
</BODY>
</HTML>
```

The contents that the Web browser receives when the HTML file is retrieved from Flash memory are as follows:

```
<HTML>
<HEAD>
<TITLE>SSI Echo Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI echo command
<HR>
The name of this server is:<BR>
rain
<BR>
</BODY>
</HTML>
```

The Web Browser shows the following text:

```
This is an example of the SSI echo command
------------------------------------------
The name of this server is:
rain
```

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Unique Device Identifier Retrieval

The Unique Device Identifier Retrieval feature provides the ability to retrieve and display the Unique Device Identifier (UDI) information from any Cisco product that has electronically stored such identity information.

History for Unique Device Identifier Retrieval Feature

Release	Modification
12.3(4)T	This feature was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXE5	This feature was integrated into Cisco IOS Release 12.2(18)SXE5.

Software images for Cisco 12000 series Internet routers have been deferred to Cisco IOS Release 12.0(27)S1.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Prerequisites for Unique Device Identifier Retrieval

In order to use UDI retrieval, the Cisco product in use must be UDI-enabled. A UDI-enabled Cisco product supports five required Entity MIB objects. The five Entity MIB v2 (RFC-2737) objects are as follows:

- entPhysicalName
- entPhysicalDescr
- entPhysicalModelName
- entPhysicalHardwareRev
- entPhysicalSerialNum

Although the **showinventory** command may be available, using that command on devices that are not UDI-enabled will likely produce no output.

Information About Unique Device Identifier Retrieval

Unique Device Identifier Overview

Each identifiable product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a superentity like a stack. Most Cisco entities that are orderable products will leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

Benefits of the Unique Device Identifier Retrieval Feature

- Identifies individual Cisco products in your networks.
- Reduces operating expenses for asset management through simple, cross-platform, consistent identification of Cisco products.
- Identifies PIDs for replaceable products.

- Facilitates discovery of products subject to recall or revision.
- Automates Cisco product inventory (capital and asset management).
- Provides a mechanism to determine the entitlement level of a Cisco product for repair and replacement service.

How to Retrieve the Unique Device Identifier

Retrieving the Unique Device Identifier

Perform this task to retrieve and display identification information for a Cisco product.

SUMMARY STEPS

1. **enable**
2. **show inventory** [**raw**] [*entity*

DETAILED STEPS

Step 1 **enable**

Enters privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show inventory** [**raw**] [*entity*

Enter the**showinventory** command to retrieve and display information about all of the Cisco products installed in the networking device that are assigned a PID, VID, and SN. If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

Example:

```
Router# show inventory
NAME: “Chassis”, DESCR: “12008/GRP chassis”
PID: GSR8/40           ,  VID: V01,  SN: 63915640
NAME: “slot 0”, DESCR: “GRP”
PID: GRP-B             ,  VID: V01,  SN: CAB021300R5
NAME: “slot 1”, DESCR: “4 port ATM OC3 multimode”
PID: 4OC3/ATM-MM-SC    ,  VID: V01,  SN: CAB04036GT1
NAME: “slot 3”, DESCR: “4 port 0C3 POS multimode”
PID: LC-4OC3/POS-MM    ,  VID: V01,  SN: CAB014900GU
NAME: “slot 5”, DESCR: “1 port Gigabit Ethernet”
PID: GE-GBIC-SC-B      ,  VID: V01,  SN: CAB034251NX
NAME: “slot 7”, DESCR: “GRP”
PID: GRP-B             ,  VID: V01,  SN: CAB0428AN4O
NAME: “slot 16”, DESCR: “GSR 12008 Clock Scheduler Card”
PID: GSR8-CSC/ALRM     ,  VID: V01,  SN: CAB0429AUYH
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0428ALOS
NAME: “sfslot 2”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0429AU0M
NAME: “sfslot 3”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0429ARD7
```

```
NAME: “PSslot 1”, DESCR: “GSR 12008 AC Power Supply”
PID: FWR-GSR8-AC-B     ,  VID: V01,  SN: CAB041999CW
```

Enter the**showinventory**command with an *entity* argument value to display the UDI information for a specific type of Cisco entity installed in the networking device. In this example, a list of Cisco entities that match the sfslot argument string is displayed.

Example:

```
Router# show inventory sfslot
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0428ALOS
NAME: “sfslot 2”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0429AU0M
NAME: “sfslot 3”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0429ARD7
```

You can request even more specific UDI information using the**showinventory**command with an *entity* argument value that is enclosed in quotation marks. In this example, only the details for the entity that exactly matches the sfslot 1 argument string are displayed.

Example:

```
Router# show inventory “sfslot 1”
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0428ALOS
```

For diagnostic purposes, the**showinventory**command can be used with the **raw** keyword to display every RFC 2737 entity including those without a PID, UDI, or other physical identification.

NoteThe **raw** keyword option is primarily intended for troubleshooting problems with the **showinventory** command itself.

Example:

```
Router# show inventory raw
NAME: “Chassis”, DESCR: “12008/GRP chassis”
PID:                   ,  VID: V01,  SN: 63915640
NAME: “slot 0”, DESCR: “GRP”
PID:                   ,  VID: V01,  SN: CAB021300R5
NAME: “slot 1”, DESCR: “4 port ATM OC3 multimode”
PID: 4OC3/ATM-MM-SC    ,  VID: V01,  SN: CAB04036GT1
NAME: “slot 3”, DESCR: “4 port 0C3 POS multimode”
PID: LC-4OC3/POS-MM    ,  VID: V01,  SN: CAB014900GU
```

Enter the**showinventory**command with the **raw** keyword and an *entity* argument value to display the UDI information for the Cisco entities that are installed in the networking device and that match the argument string, even if they do not contain an assigned PID.

Example:

```
Router# show inventory raw slot
NAME: “slot 0”, DESCR: “GRP”
PID:                  ,  VID: V01,  SN: CAB021300R5
NAME: “slot 1”, DESCR: “4 port ATM OC3 multimode”
PID: 4OC3/ATM-MM-SC    ,  VID: V01,  SN: CAB04036GT1
NAME: “slot 3”, DESCR: “4 port 0C3 POS multimode”
PID: LC-4OC3/POS-MM    ,  VID: V01,  SN: CAB014900GU
```

- Troubleshooting Tips, page 157

Troubleshooting Tips

If any of the Cisco products do not have an assigned PID, the output may display incorrect PIDs and the VID and SN elements may be missing, as in the following example.

```
NAME: "Four Port High-Speed Serial", DESCR: "Four Port High-Speed Serial"
PID: Four Port High-Speed Serial, VID: 1.1, SN: 17202570
NAME: "Serial1/0", DESCR: "M4T"
PID: M4T               , VID:    , SN:
```

In the sample output, the PID is exactly the same as the product description. The UDI is designed for use with new Cisco products that have a PID assigned. UDI information on older Cisco products is not always reliable.

Configuration Examples for Unique Device Identifier Retrieval

There are no configuration examples for the UDI Retrieval feature. For sample display output from the show inventory command, see the “Retrieving the Unique Device Identifier” section.

Additional References

This section provides references related to the UDI Retrieval feature.

Related Documents

Related Topic	Document Title
Information about managing configuration files	• *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.0 • *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2 • *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, Release 12.3
Commands for showing interface statistics	• *Cisco IOS Interface Command Reference*, Release 12.0 • *Cisco IOS Interface Command Reference*, Release 12.2 • *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.3T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
CISCO-ENTITY-ASSET-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2737	*Entity MIB (Version 2)*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

ACL Authentication of Incoming rsh and rcp Requests

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the ACL Authentication of Incoming RSH and RCP Requests feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

Feature Overview

To enable the Cisco IOS software to receive incoming remote shell (rsh) protocol and remote copy (rcp) protocol requests, customers must configure an authentication database to control access to the router. This configuration is accomplished by using the **iprcmdremote-host**command.

Currently, when using this command, customers must specify the local user, the remote host, and the remote user in the database authentication configuration. For users who can execute commands to the router from multiple hosts, multiple database authentication configuration entries must be used, one for each host, as shown below.

```
ip rcmd remote-host local-user1 remote-host1 remote-user1
ip rcmd remote-host local-user1 remote-host2 remote-user1
ip rcmd remote-host local-user1 remote-host3 remote-user1
ip rcmd remote-host local-user1 remote-host4 remote-user1
```

This feature allows customers to specify an access list for a given user. The access list identifies the hosts to which the user has access. A new argument, *access-list* , has been added that can be used with this command to specify the access list, as shown below.

```
ip rcmd remote-host local-user1 access-list remote-user1
```

To allow a user access to the hosts identified in the access list, first define the access list. If the access list is not already defined, access to the host will be denied. For information about defining an access list, refer to the *Cisco IOS Security Configuration Guide* , Release 12.2.

For more information about using the modified **iprcmdremote-host** command, see the “Command Reference” section later in this document.

- Related Documents, page 160

Related Documents

- *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide* , Release 12.2
- *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

- Cisco 805
- Cisco 806
- Cisco 828
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1750
- Cisco 1751
- Cisco 2420
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 2500 series
- Cisco 2600 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco uBR7200 series
- Cisco Voice Gateway 200
- URM (Universal Route Module)

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register .

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.