



Installing Cisco Unified CallManager Release 5.0(4)

Because the 5.0(x) release of Cisco Unified CallManager has a different installation framework than previous releases of Cisco Unified CallManager, review all installation instructions carefully before you install Cisco Unified CallManager 5.0(4).

This document includes information about installing Cisco Unified CallManager Release 5.0(4) on one server or many servers in a cluster environment.

Contents

This document contains the following topics:

- [Installation Overview](#)
- [Related Documentation](#)
- [Important Considerations](#)
- [Frequently Asked Questions About the Cisco Unified CallManager Installation](#)
- [Browser Requirements](#)
- [Configuring the Hardware](#)
- [Installing Cisco Unified CallManager](#)
- [Gathering Information for an Installation](#)
- [Installing the New Operating System and Application](#)
- [Post-Installation Tasks](#)
- [Examining Log Files](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

Installation Overview

Cisco Unified CallManager 5.0(x) uses a different installation framework than previous releases. The installation process allows you to perform a basic installation, upgrade from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.0(4), and upgrade to a newer service release during the installation.

For a more detailed description of the different installation types, see [Table 1](#).

Table 1 *Installation Options*

Installation Types	Description
Basic Install	This option represents the basic Cisco Unified CallManager 5.0(4) installation, which installs the software from the installation disc and does not use any imported data.
Upgrade During Install	This option allows you to upgrade the software version contained on the installation disc with the latest service release. You can also choose Upgrade During Install followed by a Windows Upgrade and perform both during the installation process.
Windows Upgrade	This option allows you to import database information from a Cisco Unified CallManager 4.x system using a file produced by the Data Migration Assistant (DMA) tool.



Note

This document describes only the first two installation types: Basic Install and Upgrade During Install. For information on performing a Windows Upgrade, refer to *Upgrading Cisco Unified CallManager*.

Related Documentation

Cisco strongly recommends that you review the following documents before you perform the Cisco Unified CallManager installation:

- *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide*
The *Cisco Unified CallManager Administration Guide* provides step-by-step instructions for configuring, maintaining, and administering the Cisco Unified CallManager voice over IP network.
The *Cisco Unified CallManager System Guide* provides descriptions of the Cisco Unified CallManager system and its components, configuration checklists, and links to associated *Cisco Unified CallManager Administration Guide* procedures.
- *Cisco Unified CallManager Features and Services Guide*
This document describes how to configure features and services for Cisco Unified CallManager, including Cisco Music On Hold, Cisco Unified CallManager Extension Mobility, and so on.
- The *Cisco Unified CallManager Serviceability System Guide* and *Cisco Unified CallManager Serviceability Administration Guide*
These documents provide descriptions of Cisco Unified CallManager serviceability and remote serviceability and step-by-step instructions for configuring alarms, traces, and other reporting.

- *Disaster Recovery System Administration Guide*
This document describes how to configure the backup settings, back up Cisco Unified CallManager data, and restore the data.
- *Data Migration Assistant User Guide*
This document provides procedures for migrating data from earlier versions of Cisco Unified CallManager to Cisco Unified CallManager 5.0(x).
- *Cisco Unified Communications Operating System Administration Guide*
This document provides information on how to access and use the utilities that are available on the platform. This document also includes instructions for installing new locales.
- *Cisco Unified CallManager Security Guide*
This document provides instructions on how to configure and troubleshoot authentication and encryption for Cisco Unified CallManager, Cisco Unified IP Phones, SRST references, and Cisco MGCP gateways.
- *Upgrading Cisco Unified CallManager*
This document provides instructions on how to upgrade from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.0(4).

Table 2 lists URLs for software and additional documentation.

Table 2 Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
<i>Cisco Unified CallManager Compatibility Matrix</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/cmcomp.htm
Cisco Unified CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
<i>Cisco Unified CallManager Security Guide</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/a/index.htm
Cisco Unified CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco Unified CallManager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

Important Considerations

Before you proceed with the Cisco Unified CallManager installation, consider the following requirements and recommendations:

- Be aware that when you install Cisco Unified CallManager 5.0(4) on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.
- Install the Cisco Unified CallManager software on the first node or publisher server first and then on the subsequent nodes.
- Make sure that the subsequent node servers that you are installing can connect to the first node server during the installation.
- Enter the same security password on all servers in the cluster.
- Install the Cisco Unified CallManager software during off-peak hours or a maintenance window to avoid impact from call-processing interruptions.
- Configure the server using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco Unified IP Phones can register with the application when you plug the phones into the network.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete installing Cisco Unified CallManager on every server in the cluster.
- Carefully read the instructions that follow before you proceed with the installation

Frequently Asked Questions About the Cisco Unified CallManager Installation

The following section contains information about commonly asked questions and responses. Review this section carefully before you complete the Cisco Unified CallManager installation.

How long does it take to perform the Cisco Unified CallManager installation?

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes per server, depending on your server type. Before you install Cisco Unified CallManager, consider the size of your cluster.

What Passwords do I Need to Specify?

During the Cisco Unified CallManager installation, you must specify the following user names and passwords:

- Administrator account

You use the Administrator username and password to log in to the following areas:

- Cisco Unified Communications Operating System Administration

- Disaster Recovery System
- Command Line Interface

The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. You can change the Administrator password or add a new Administrator account by using the command line interface. See the *Cisco Unified Communications Operating System Administration Guide* for more information.

- Application User password

You use the Application User password for the following default application user names:

- CCMAAdministrator
- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser

You can change the application user password for each application through Cisco Unified CallManager Administration. See the *Cisco Unified CallManager Administration Guide* for more information.

- Database Access Security Password

The system uses this password to authorize communications between nodes, and this password must be the same on all nodes in the cluster.

The Database Access Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

Which servers does Cisco support for this installation?

To find which servers support Cisco CallManager 5.0 releases, please refer to the Guide to Cisco CallManager Upgrades and Server Migrations at

http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/prod_brochure_list.html

May I install other software besides Cisco Unified CallManager on the server?

For Cisco Unified CallManager 5.0(4), you must do all software installations and upgrades by using the Software Upgrades menu options in Cisco Unified Communications Operating System Administration. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified CallManager with Cisco Unified CallManager 5.0(4).

Browser Requirements

You can access Cisco Unified CallManager Administration, Cisco Unified CallManager Serviceability, and Cisco Unified Communications Administration by using the following browsers:

- Microsoft Internet Explorer version 6.0 or later
- Netscape Navigator version 7.1 or later



Note

Cisco does not support or test other browsers, such as Mozilla Firefox.

Installation Options

After the installation restarts, you will be asked to select one of the options that [Table 3](#) lists.

Table 3 *Installation Options*

Installation Options	Description
Basic Install	This option represents the basic installation and does not use any imported data.
Upgrade During Install	This option allows you to upgrade the preinstall software with the latest service release prior to configuring your system. You can also choose Upgrade During Install followed by a Windows Upgrade and perform both during the installation process. Note You must have the software image available on DVD or on a remote server prior to choosing this option.
Windows Upgrade	This option allows you to import the TAR file that the DMA tool produced while upgrading an existing Cisco Unified CallManager server. Note For more information on performing a Windows Upgrade, see <i>Upgrading Cisco Unified CallManager</i> .

Configuring the Hardware

As a part of software installation, the system installer configures the system BIOS and RAID settings for the new operating system and Cisco Unified CallManager application. See [Table 4](#) for the BIOS settings and [Table 5](#) for the RAID settings that are set up during installation.

Table 4 *BIOS Configuration Settings for HP and IBM Servers*

HP Servers	IBM Servers
OS Selection: Linux (not applicable on newer models)	OS Selection: Not applicable
Boot order: CD, C:, Floppy	Boot order: CD, C:, Floppy
Post F1 prompt: Delayed	Post F1 prompt: Delayed
Hyperthreading: Enabled	Hyperthreading: Enabled

Table 5 RAID Settings

MCS 7825 Servers (HP and IBM)	MCS 7835 Servers (HP and IBM)	MCS 7845 Servers (HP and IBM)
RAID not applicable	Logical drives: 1	Logical drives: 2
RAID not applicable	RAID type: 1(1+0)	RAID type: 1(1+0)
Note For the HP 7825H1 and the IBM 7825I1, SATA RAID is enabled, the RAID type is 1(1+0), with one logical drive.		

**Note**

If the hardware configuration process fails during installation, you can use boot-time utilities found on both the IBM and HP servers to manually configure the RAID and BIOS settings, as shown in [Table 4](#) and [Table 5](#).

Installing Cisco Unified CallManager

The next sections contain the procedures for installing the first and subsequent nodes. Review the following sections carefully before you perform the installation:

- [Gathering Information for an Installation, page 7](#)
- [Installing the New Operating System and Application, page 13](#)
- [Post-Installation Tasks, page 20](#)

Gathering Information for an Installation

Use [Table 6 on page 8](#) to record the information about your Cisco Unified CallManager server. Gather this information for each Cisco Unified CallManager server that you are installing in the cluster. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration. You should make copies of this table and record your entries for each server in a separate table, even if you are planning to use the DMABackupInfo.inf file to configure your system.

**Note**

Because some of the fields are optional, they may not apply to your configuration. For example, you choose not to set up an SMTP host.

**Caution**

You cannot change some of the fields after installation without reinstalling the software, so be sure to enter the values that you want.

The last column in the table shows whether a field can be changed after installation, and if so, whether you can change it through Cisco Unified Communications Operating System Administration or through the Command Line Interface (CLI).

Table 6 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Administrator Password		Yes. CLI >set password admin
Application User Password		Yes CLI: set password
Country		Yes CLI>set web-security
DHCP		Yes CLI> set network dhcp
DNS Primary		Yes CLI> set network dns
DNS Secondary		Yes CLI>set network dns
Domain		Yes CLI>Set Network Domain
Domain Name Service DNS Enable		No
Gateway Address		Yes. Use OS Administration > Settings>IP or CLI > set network gateway
Host Name		No
IP Address		Yes Use OS Administration > Settings>IP or CLI>set network IP
IP Mask		Yes. Use OS Administration > Settings>IP or CLI > set IP
Location		Yes CLI>set web-security
Master Administrator ID		No

Table 6 Configuration Data (Continued)

Configuration Data	Your Entry	Can Entry Be Changed After Installation
NTP Server IP Address Note You can enter up to five NTP servers.		Yes Use OS Administration >Settings>NTP Servers
Organization		Yes CLI>set web-security
Security Password		Yes CLI>set password security
SMTP Location		Yes CLI>set smtp
State		Yes CLI>set web-security
Time Zone		Yes CLI>Set Timezone
Unit		Yes CLI>set web-security

For more detailed descriptions of each installation field, see [Table 7](#).

Table 7 Installation Field Definitions

Field	Description	Usage
Administrator ID	This field specifies the name that you want to assign to this account.	Ensure the name is unique; it can contain lowercase, alphanumeric characters, hyphens, and underscores. It must start with a lowercase alphanumeric character. For this mandatory field, you should record it for use when logging in to the CLI on the platform or into the Cisco Unified Communications Operating System Administration. Note You cannot change this field after installation.
Administrator Password	This field specifies the password that you use for logging into the the CLI on the platform and for logging into Cisco Unified Communications Operating System Administration.	Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore. For this mandatory field, you should record it for use when logging in to the Cisco Unified CallManager.

Table 7 Installation Field Definitions (Continued)

Field	Description	Usage
DHCP	Dynamic Host Configuration Protocol	Choose Yes if you want to use DHCP to automatically configure the network settings on your server. If you choose No, you must enter a hostname, IP Address, IP Mask, and Gateway.
DNS Enabled	A DNS server represents a device that resolves a hostname into an IP address or an IP address into a hostname. Note You cannot change the DNS settings after the installation is complete. To change DNS settings, you must reinstall Cisco Unified CallManager.	If you do not have a DNS server, enter No . When DNS is not enabled, you should only enter IP addresses (not hostnames) for all network devices in your Cisco Unified Communications network. If you have a DNS server, Cisco recommends entering Yes to enable DNS. Disabling DNS limits the system ability to resolve some domain names.
DNS Primary	Cisco Unified CallManager contacts this DNS server first when attempting to resolve host names.	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). Consider this field mandatory if DNS is set to yes .
DNS Secondary	When a primary DNS server fails, Cisco Unified CallManager will attempt to connect to the secondary DNS server.	In this optional field, enter the IP address of the secondary DNS. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).
Domain	This field represents the name of the domain in which this machine is located.	Consider this field mandatory if DNS is set to yes .
First Cisco Unified CallManager Node	This field specifies the first Cisco Unified CallManager node that contains the database. Subsequent nodes connect to the the first node to access database content. The first node also synchronizes with an external NTP server and provides time to the other nodes.	Choose Yes if you are configuring the first Cisco Unified CallManager node in the cluster. If you are configuring subsequent nodes, see Table 7 for information on the different fields.

Table 7 *Installation Field Definitions (Continued)*

Field	Description	Usage
Gateway Address	A gateway represents a network point that acts as an entrance to another network. Outbound packets get sent to the gateway that will forward them to their final destination.	Enter the IP address of the gateway in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0) If you do not have a gateway, you must still fill in this field by setting it to 255.255.255.255. Not having a gateway may limit you to only being able to communicate with devices on your subnet.
Hostname	A host name represents an alias that is assigned to an IP address to identify it.	Enter a host name that is unique to your network. The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens. If DHCP is set to No , consider this field mandatory.
IP Address	This field specifies the IP address of this machine. It will uniquely identify the server on this network. Another machine in this network should not be using this IP address.	Enter the IP address in the form ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). If DHCP is set to No , consider this field mandatory.
IP Mask	This field specifies the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address.	Enter the IP mask in the form ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). A valid mask should have contiguous '1' bits on left side and contiguous '0' bits on the right. For example, a valid mask follows: 255.255.240.0 (11111111.11111111.11110000.00000000) An invalid mask follows: 255.255.240.240 (11111111.11111111.11110000.11110000)
NIC Speed	This field specifies the speed of the server network interface card (NIC), in megabits per second.	The possible speeds are 10 or 100.
NIC Duplex	This field specifies the duplex setting of the server NIC.	The possible settings are half and full.

Table 7 Installation Field Definitions (Continued)


Field	Description	Usage
NTP Server	This field identifies the NTP servers with which you want to synchronize.	Enter the hostname or IP Address of one or more NTP server(s). Note You can add additional NTP servers or make changes to the NTP server list at a later time
NTP Server Enable	When enabled, this server will act as a NTP server and provide time updates to the subsequent nodes in the cluster.	Choose Yes if you want to enable this machine to be an NTP server.
Security Password	Cisco Unified CallManager servers in the cluster use the security password to communicate with one another. You will be asked to enter the same security password for each subsequent node in the cluster.	Enter the security password. Enter the same password in the confirm password field. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.  Caution You must enter the same password for all nodes in the cluster.
Set Hardware Clock	This field specifies the date and local time for the machine. Note If you set the hardware clock manually, the node does not use an external NTP server for time synchronization.	Choose Yes if you want to set the date and local time for the time zone that you chose. Enter the hours based on a 24-hour format. Note If you configure an external NTP server, the hardware clock gets set automatically.
SMTP	This field specifies the name of the SMTP host that is used for outbound e-mail.	Enter the hostname or dotted IP address for the SMTP server. For a host, it can contain alphanumeric characters, hyphens, or periods. For a host name, it must start with an alphanumeric character. You must fill in this field if you plan to use Electronic Notification. If not, you can leave it blank.

Table 7 Installation Field Definitions (Continued)

Field	Description	Usage
Subnet IP Address	By entering a subnet address, you can specify a range of IP Addresses that will be granted access to query this NTP server.	Enter an IP subnet that will be granted access to the NTP server During installation, you can only enter two subnets.
Subnet Mask	This field specifies the subnet mask for the subnet address.	Enter the subnet mask for the IP subnet.
Time zone	This field specifies the local time zone and offset from Greenwich Mean Time (GMT).	Choose Yes if you want to change the time zone. Choose the time zone that most closely matches the location of your machine.

Installing the New Operating System and Application

Use this procedure to begin installing the operating system and Cisco Unified CallManager application:

Procedure

- Step 1** Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the Media Check window displays.



Note If you have a new server with Cisco Unified CallManager preinstalled, you do not need to install from a DVD. Go directly to the [“If You Choose Skip” procedure on page 14](#).

- Step 2** Verify that the checksum that displays on the Media Check matches the checksum for the release on Cisco.com.

When the media check completes, the Media Check Result window displays.

- Step 3** If the Media Check Result displays Pass, choose **OK** to continue the installation.

If the media fails the Media Check, either download another copy from Cisco.com or obtain another disc directly from Cisco Systems.

After you choose OK, the system installer performs various hardware checks to ensure you system is correctly configured for Cisco Unified CallManager 5.0(4), including the following:

- First, the installation process checks for the correct drivers, and you may see the following warning:

Drivers not found, do you want to install manually?

To continue the installation, choose **Yes**.

- The installation next checks to see if you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings. If the installation process makes any changes to your hardware configuration settings, you will get prompted to restart your system.

After the hardware checks complete, the Overwrite Hard Drive window displays.

- Step 4** The **Overwrite Hard Drive** window indicates the current software version on your hard drive, if any, and the version on the DVD. Choose **Yes** to continue with the installation or **No** to cancel.



Caution

If you choose **Yes** on the **Overwrite Hard Drive** window, all existing data on your hard drive gets overwritten and destroyed.

The Platform Installation Wizard window displays.

- Step 5** To configure the platform now, choose **Proceed**. If you want to configure the platform later, choose **Skip**.
- If you want to install and configure the software at this time, choose **Proceed** and skip to the [“If You Choose Proceed”](#) section on page 14.
 - If you want to install the software now and configure it later, choose **Skip** and continue with the [“If You Choose Skip”](#) section on page 14.

If You Choose Skip

Start here if you have a server that has Cisco Unified CallManager preinstalled or if you chose **Skip** on Platform Installation Wizard window.

- Step 6** After the system restarts, the Preexisting Installation Configuration window displays. If you have configuration information on a USB drive or on a diskette, insert it now.



Note

If a popup window states that the system detected new hardware, press any key and then choose **Install** from the next window.



Note

If you have a file that the Data Migration Assistant created, see the *Data Migration Assistant User Guide* for more information.

- Step 7** To continue, choose **OK**.

The Platform Installation Wizard window displays.

- Step 8** To continue with the installation, choose **Proceed**.

The Upgrade During Install window displays. Continue with the [“If You Choose Proceed”](#) section on page 14.

If You Choose Proceed

- Step 9** Choose the type of installation to perform by doing the following steps. See [Table 3](#) for more information on installation options:

- a. In the Upgrade During Install window, choose one of the options:
 - To upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the [“Upgrade During Install”](#) section on page 15.

- To skip this step, choose **No**.
- To return to the previous window, choose **Back**.

b. In the Windows Upgrade window, choose **No**.



Note To perform a Windows Upgrade, that is, to upgrade from a Windows version of Cisco Unified CallManager to Cisco Unified CallManager 5.0(4), see *Upgrading to Cisco Unified CallManager* for more information.

c. In the Basic Install window, choose **Continue** to install the software version on the DVD or configure the preinstalled software. Continue with the “[Basic Installation](#)” section on page 17.

Upgrade During Install

If you choose **Yes** in the Upgrade During Install window, the installation wizard installs the software version on the DVD first and then restarts the system. You then get prompted to enter certain network configuration parameter values and the location of the upgrade file.

Step 10 After the system restarts, the Platform Installation Wizard window displays. To continue the installation, choose **Proceed**.

The Upgrade During Install window displays.



Note If the installer pops up a window that states that it detected new hardware, press any key and then choose **Install** from the next window.

Step 11 Choose **Yes**.

The Install Upgrade Retrieval Mechanism Configuration window displays.

Step 12 Choose the upgrade retrieval mechanism to use to retrieve the upgrade file:

- **SFTP**—Retrieves the upgrade file from a remote server by using the Secure File Transfer Protocol (SFTP). Skip to the “[Upgrade From a Remote Server](#)” section on page 16.
- **FTP**—Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the “[Upgrade From a Remote Server](#)” section on page 16.
- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the “[Upgrade From a Local Disc](#)” section on page 15.

Upgrade From a Local Disc

Before you can upgrade from a local drive, you must download the appropriate patch file from Cisco.com and copy the file to a CD or DVD. Because of the size of the patch files, you will need to copy it to a DVD in most cases.

The patch-file name has the following format:

```
cisco-ipt-k9-patchX.X.X.X-X.tar.gz
```

Where X.X.X.X-X represents the release and build number



Note Do not untar or unzip the patch file before you install it because the system will not recognize it as a valid file.

- Step 13** When the Local Patch Configuration window displays, enter the patch directory and patch name, if required, and choose **OK**.



Note You only need to enter the patch directory when the patch is not stored in the root directory of the CD or DVD.

The Install Upgrade Patch Selection Validation window displays.

- Step 14** The window displays the patch file that is available on the CD or DVD. To update the system with this patch, choose **Continue**.

Upgrade From a Remote Server

If you chose to upgrade through an FTP or SFTP connection to a remote server, you must first configure the network settings.

The Auto Negotiation Configuration window displays.

- Step 15** The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) using automatic negotiation. You can change this setting after installation.
- To enable automatic negotiation, choose **Yes**. The DHCP Configuration window displays.



Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays.

- Step 16** If you chose to disable automatic negotiation, manually choose the appropriate NIC Speed and Duplex settings now and choose **OK** to continue.

The DHCP Configuration window displays.

- Step 17** For network configuration, you can choose to either set up static network IP addresses for the node and gateway or to use Dynamic Host Configuration Protocol (DHCP).
- If you have a DHCP server configured in your network and want to use DHCP, choose **Yes**. The system restarts and checks for network connectivity. Skip to the [“Retrieving the Remote Patch” section on page 16](#).
 - If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

- Step 18** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See [Table 7](#) for field descriptions.

The DNS Client Configuration window displays.

- Step 19** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See [Table 7](#) for field descriptions.

After the system configures the network and checks for connectivity, the Remote Patch Configuration window displays.

Retrieving the Remote Patch

- Step 20** Enter the location and login information for the remote file server. See [Table 7](#) for field descriptions. After restarting the network, the system connects to the remote server and retrieves a list of available upgrade patches.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter `/patches`. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

The Install Upgrade Patch Selection window displays.

- Step 21** Choose the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system running the upgraded software version.

After the system restarts, the Preexisting Configuration Information window displays.

Using Preexisting Configuration Information

- Step 22** If you have preexisting configuration information that is stored on a floppy disc or a USB key, insert the disc or the USB key now and choose **Continue**. The installation wizard will read the configuration information during the installation process.

The Platform Installation Wizard window displays.

- Step 23** To continue with the Platform Installation Wizard, choose **Proceed**.

The Product Installation Configuration window displays.

- Step 24** To configure the platform now, choose **Proceed**.

- Step 25** In the Upgrade During Install window, choose **No**.

- Step 26** In the Windows Upgrade window, choose **No**.

- Step 27** In the Basic Install window, choose **Continue**. Continue with the [“Basic Installation” section on page 17](#).

Basic Installation

- Step 28** When the Timezone Configuration displays, choose the appropriate time zone for the server, and then choose **OK**.

The Auto Negotiation Configuration window displays.

- Step 29** The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes**. The DHCP Configuration window displays.



Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays.

- Step 30** If you chose to disable automatic negotiation, manually choose the appropriate NIC Speed and Duplex settings now and choose **OK** to continue.

The DHCP Configuration window displays.

- Step 31** For network configuration, you can choose to either set up static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP).

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The network restarts and the Administrator Login Configuration window displays.
- If you want to configure static IP address for the node, choose **No**. The Static Network Configuration window displays.

Step 32 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See [Table 7](#) for field descriptions.

The DNS Client Configuration window displays.

Step 33 To enable DNS, choose **Yes**, enter your DNS client information and choose **OK**. See [Table 7](#) for field descriptions.

The network restarts using the new configuration information, and the Administrator Login Configuration window displays.

Step 34 Enter your Administrator login and password from [Table 6](#).



Note The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. You will need the Administrator login to log in to Cisco Unified Communications Operating System Administration, the command line interface, and the Disaster Recovery System.

The Certificate Signing Request Information window displays.

Step 35 Enter your certificate signing request information from [Table 6](#) and choose **OK**.

The First Node Configuration window displays.

Step 36 You can configure this server as either the first node in a Cisco Unified CallManager cluster or as a subsequent node.

- To configure this server as the first Cisco Unified CallManager node, choose **Yes** and continue with the [“Configure the First Node”](#) section on page 18.
- To configure this server as a subsequent node in the cluster, choose **No** and continue with the [“Configure a Subsequent Node”](#) section on page 19.

Configure the First Node

If you chose to configure the server as the first node in the cluster, the Network Time Protocol Client Configuration window displays. Cisco recommends that you use an external NTP server to ensure accurate system time on the first node. The external NTP server must be stratum 9 or higher (meaning stratum 1-9). Subsequent nodes in the cluster will get their time from the first node.

Step 37 Choose whether you want to configure an external NTP server or manually configure the system time.

- To set up an external NTP server, choose **Yes** and enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers, and Cisco recommends that you use at least three. Choose **Proceed** to continue with the installation.

The system contacts an NTP server and automatically sets the time on the hardware clock.



Note If the Test button displays, you can choose **Test** to check whether the NTP servers are accessible.

- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The Database Access Security Configuration window displays.

Step 38 Enter the Database Access Security password from [Table 6](#).

**Note**

The Database Access Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. The system uses this password to authorize communications between nodes, and this password must be the same on all nodes in the cluster.

The SMTP Host Configuration window displays.

- Step 39** If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

**Note**

You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the platform GUI or the command line interface.

The Platform Configuration Confirmation window displays.

- Step 40** To continue with the installation, choose **OK**. Or to modify the platform configuration, choose **Back**. When you choose **OK**, the Application User Password Configuration window displays.

- Step 41** Enter the Application User Password from [Table 6](#) and confirm the password by entering it again.

- Step 42** Choose **OK**.

The Cryptographic Export Warning window displays, and the systems installs and configures the software.

- Step 43** When the installation process completes, you get prompted to log in by using the Administrator account and password.

- Step 44** Complete the post-upgrade tasks that are listed in the [“Post-Installation Tasks”](#) section on page 20.

Configure a Subsequent Node

To configure a subsequent node in the cluster, follow these steps.

**Caution**

You must configure a subsequent node on the first node before you install it. From Cisco Unified CallManager Administration on the first node, choose **System>Server**. For more information, see the *Cisco Unified CallManager Administration Guide*.

The First Node Access Configuration window displays.

- Step 45** Enter the First Node Access Configuration information from [Table 6](#).

The SMTP Host Configuration window displays.

- Step 46** If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

**Note**

You must configure an SMTP server to use certain platform features. However, you can also configure an SMTP server later by using the platform GUI or the command line interface.

The Platform Configuration Confirmation window displays.

- Step 47** To start installing the software, choose **OK**, or if you want to change the configuration, choose **Back**.

- Step 48** When the installation process completes, you get prompted to log in by using the Administrator account and password.
- Step 49** Complete the post-upgrade tasks that are listed in the “[Post-Installation Tasks](#)” section on page 20.

Post-Installation Tasks

After installing Cisco Unified CallManager on your server, you must set some configuration parameters for Cisco Unified CallManager and perform other post-installation tasks before you can begin using it. Perform these tasks for the server that you install and complete the tasks before other servers in the cluster are installed.

For post-installation tasks that you must complete after the installation, see [Table 8](#).

Table 8 *Post-Installation Tasks*


Post-Installation Tasks	Important Notes
Log in as the Cisco Unified CallManager Application User and change the Application User passwords.	See the “ Changing the Default Cisco Unified CallManager Application User Passwords ” section on page 21.
<p>Activate Cisco Unified CallManager feature services that you want to run.</p> <p>Before you activate feature services, you must perform required preactivation tasks; for example, before you can activate a service on a server, you must add the server to Cisco Unified CallManager Administration (System > Cisco Unified CallManager).</p> <p>For other service activation requirements, refer to the <i>Cisco Unified CallManager Serviceability Administration Guide</i>.</p> <p> Caution You must activate Cisco Unified CallManager services in Cisco Unified CallManager Serviceability.</p>	<p>Refer to the following documents:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Serviceability Administration Guide</i> • <i>Cisco Unified CallManager Serviceability System Guide</i> <p>See the “Accessing Cisco Unified CallManager Serviceability” section on page 21.</p>
<p>Configure the backup settings.</p> <p>Remember to back up your Cisco Unified CallManager data daily.</p>	Refer to <i>Disaster Recovery System Administration Guide</i> .
The locale English_United_States, installs automatically on the server; however, you can add new locales to the server, if required.	Refer to <i>Cisco Unified Communications Operating System Administration Guide</i> .

Table 8 Post-Installation Tasks (Continued)

Post-Installation Tasks	Important Notes
Cisco recommends that you implement authentication and encryption in your Cisco IP Telephony network.	Refer to <i>Cisco Unified CallManager Security Guide</i>
If necessary, you can add subsequent Cisco Unified CallManager nodes to the cluster.	<p>You must add subsequent Cisco Unified CallManager nodes to the cluster by performing the following tasks:</p> <ol style="list-style-type: none"> 1. Define all subsequent nodes in the cluster by adding the hostname or IP address of the subsequent Cisco Unified CallManager nodes to Cisco Unified CallManager Administration. For more information, refer to <i>Cisco Unified CallManager Administration Guide</i>. 2. Install the new application and configure subsequent Cisco Unified CallManager nodes in the cluster. See Installing Cisco Unified CallManager, page 7 <p>Remember to enter the same security password on all nodes.</p>

Changing the Default Cisco Unified CallManager Application User Passwords

Cisco Unified CallManager installation sets all Application User passwords to the same Application User password that you entered during installation. Cisco recommends that you log in to Cisco Unified CallManager Administration and change these passwords. Refer to *Cisco Unified CallManager System Guide* for the procedure for changing a password.

Accessing Cisco Unified CallManager Serviceability

To access Cisco Unified CallManager Administration or Cisco Unified CallManager Serviceability, you will need to use a web browser from a PC with network access to the Cisco Unified CallManager server.

Even though all Cisco Unified CallManager services are installed on each server in the cluster, you must manually activate the services that you want to run on each server in the cluster through Cisco Unified CallManager Serviceability. For service recommendations and more information, refer to *Cisco Unified CallManager Serviceability Administration Guide* and *Cisco Unified CallManager Serviceability System Guide*.

To activate services through Cisco Unified CallManager Serviceability, follow this procedure:

Procedure

Step 1 Open a web browser on a computer with network access to the Cisco Unified CallManager server.

Step 2 Enter the following url:

http://ccm_server:8080/ccmadmin

where *ccm_server* specifies the IP address or hostname of the Cisco Unified CallManager server.

- Step 3** Enter the Cisco Unified CallManager Application user name and password.
 - Step 4** From the Navigation menu, choose **Cisco Unified CallManager Serviceability** and click **Go**.
 - Step 5** From the menu bar, click **Tools > Service Activation**.
 - Step 6** Choose a server from the drop-down menu.
 - Step 7** Check the Service Names check boxes for the services to activate.
 - Step 8** Click **Save**.
-

Configuring the Database

After installing Cisco Unified CallManager, you use Cisco Unified CallManager Administration to begin configuring the database. The Cisco Unified CallManager database contains information and parameters that relate to the system as a whole, to connected devices, and to individual users. The following list describes a few tasks that you must perform in Cisco Unified CallManager Administration or Cisco Unified CallManager Serviceability:

1. In Cisco Unified CallManager Serviceability, activate the services that you want to run on each server in the cluster.
2. Configure system-level settings, such as Cisco Unified CallManager Groups.
3. Design and configure your dialing plan.
4. Configure media resources for conferences, Music On Hold, and so on.
5. Configure systemwide features, Cisco Unified IP Phone services, Cisco Unified CallManager Extension Mobility, Cisco Unified CallManager Attendant Console, and Cisco Unified CallManager Assistant.
6. Install and configure the gateways.
7. Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.
8. Configure the users.
9. Configure and install the phones; then, associate users with the phones.

For more information about configuring the Cisco Unified CallManager database, refer to the *Cisco Unified CallManager Administration Guide*, the *Cisco Unified CallManager System Guide*, or online help in the Cisco Unified CallManager application.

Examining Log Files

If you encounter problems with the installation, you can obtain and examine the install log files by entering the following commands in Command Line Interface.

To obtain a list of install log files from the command line, enter

```
CLI>file list install
```

To view the log file from the command line, enter

```
CLI>file view install log_file
```

where *log_file* is the log file name.

You can also view logs by using the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT). For more information on using and installing the Cisco Unified CallManager RTMT, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have.pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

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

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

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

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)