This chapter covers the following topics:

- The requirements to perform Cisco Unified CallManager server installation

- Cisco Unified CallManager installation process

- Cisco Unified CallManager postinstallation procedures

- Cisco Unified CallManager upgrade process

Cisco Unified CallManager Installation and Upgrades

When Cisco first announced that the Cisco CallManager platform would use Microsoft Windows 2000 as a foundation operating system and Microsoft SQL 2000 as a database store, concern arose that the Cisco administrator would require a thorough understanding of these applications to successfully operate a Cisco IP telephony network. Although an understanding of these components can be useful for monitoring and troubleshooting purposes, it is not necessary for Cisco CallManager installation and setup. Cisco has done a fantastic job of "wizard-izing" and scripting the complete installation of both Windows 2000 and SQL 2000, hiding any complexity behind a friendly **Next** button.

The upgrade process of Cisco CallManager is not quite as friendly as a clean install; however, if you keep the potential pitfalls in mind, a Cisco CallManager upgrade can go quite smoothly. This chapter discusses both the clean install and upgrade process of Cisco CallManager.

Cisco Unified CallManager 4.x Clean Installation Process

A clean installation of Cisco CallManager has always been an extremely simple process. As you perform the Cisco CallManager installation, the automated setup process prompts you for the information that is necessary to build Windows 2000, Microsoft SQL Server 2000, and Cisco CallManager with a base configuration. The entire operating system installation process, excluding preinstallation tasks, takes approximately 25 to 45 minutes per server, depending on your server type. Installing Cisco CallManager, excluding pre- and postinstallation tasks, takes 45 to 90 minutes per server, depending on your server type.

Installation Disks

All Cisco MCSs and customer-provided servers that meet approved Cisco configuration standards ship with a blank hard drive. When you purchase a Cisco IP telephony application, you use the appropriate disks to install or upgrade the operating system and application:

■ **Disk 1: Cisco IP Telephony Server Operating System Hardware Detection Disk**— Checks the server and displays an error message if it detects an unsupported server. After you boot the server using the Hardware Detection CD-ROM, the automated installation process prompts for the correct CD-ROMs to use based on the type of hardware platform detected.

■ **Disk 2: Cisco IP Telephony Server Operating System Installation and Recovery Disk**—Installs the operating system. Use only one of the server-specific Cisco IP Telephony Server Operating System Installation and Recovery disks that come in your software kit. Depending on your platform, the Operating System disc could be CD-ROM or DVD-based. After the operating system installation, a prompt instructs you to insert the appropriate Cisco CallManager software disk into the drive.

■ **Disk 3: Cisco CallManager 4.1 Software Disk**— This disk installs the Cisco CallManager application on the server.

You might also receive a Cisco IP Telephony Server Operating System Upgrade Disk. Use this disk to upgrade the operating system on existing (not new) servers in the cluster. You do not need to use this disk if you are performing a new operating system installation.

Installation Configuration Data

As mentioned previously, the installation process for Cisco CallManager is automated by a step-by-step wizard. You will initially boot off the Hardware Detection CD-ROM, which will walk you through a wizard prompting you for the basic configuration data to get the server running. The process erases all data on the server hard disk. During the installation, you are prompted for the following items:

■ **New installation or server replacement**—Choose this option if you are installing the Cisco IP telephony application for the first time, overwriting an existing installation, or replacing a server. To replace the server, you must store the data to a network directory or tape device before the operating system installation. Choosing this setting erases all existing drives.

■ **Cisco product key**—Cisco supplies a product key when you purchase a Cisco IP telephony product. The product key is based on a file encryption system that allows you to install only the components that you have purchased. It also prevents you from installing other supplied software for general use. The product key consists of alphabetical characters only.

■ **Username and organization name**—The system will prompt you for a username and an organization name to register the software product that you are installing. Do not leave the field blank. You can enter letters, numbers, hyphens (-), and underscores (_).

■ **Computer name**—The system will prompt you to assign a unique computer name, using 15 characters or fewer, to each Cisco CallManager server. The computer name can contain alphabetic and numeric characters, hyphens, and underscores, but it must begin with a letter of the alphabet. Follow your local naming conventions, if possible. If you want to change the computer name after the application installation, you must completely reinstall the operating system and the application.

■ **Workgroup**—The system will also prompt you for a workgroup name. A workgroup consists of a collection of computers that share the same workgroup name. Computers in the same workgroup can more easily communicate with each other across the network. Ensure that this entry, which must also be 15 characters or fewer, follows the same naming conventions as the computer name.

■ **Domain suffix**—When prompted, you must enter the Domain Name System (DNS) suffix in the format "mydomain.com" or "mycompany.mydomain.com." If you are not using DNS, use a fictitious domain suffix, such as fictitioussite.com.

■ **TCP/IP properties**—You must assign an IP address, subnet mask, and default gateway when installing a Cisco CallManager server. Changing the Cisco CallManager IP address after you install the software can be a tedious process, so be sure to plan accordingly.

CAUTION   It is strongly recommended that you choose static IP information, which ensures that the Cisco CallManager server obtains a fixed IP address. With this selection, Cisco IP Phones can register with Cisco CallManager when the telephones are plugged into the network. Using Dynamic Host Configuration Protocol (DHCP) can cause problems, including failure of the telephony system.

■ **DNS**—You can identify a primary DNS server for this optional field. By default, the telephones will attempt to connect to Cisco CallManager using DNS. Therefore, you must verify that the DNS server contains a mapping of the IP address and the fully qualified domain name (FQDN) of the Cisco CallManager server. If you do not use DNS, use the server IP address, instead of a server name, to register the telephones with Cisco CallManager.

NOTE   Before you begin installing multiple servers in a cluster, you must have a name resolution method in place, such as DNS, Windows Internet Naming Service (WINS), or local name resolution using a configured LMHOSTS file. If you use DNS, you must verify that the DNS server contains a mapping of the IP address and the hostname of the server that you are installing. This verification must take place before you begin the installation. If you use local name resolution, ensure that the LMHOSTS file is updated on the existing servers in the cluster before you begin the installation on the new subscriber server. You must add the same information to the LMHOSTS file on the new server during installation.

TIP   Although it might seem tedious, Cisco considers the creation of LMHOST file IP address to hostname mappings on each Cisco CallManager server a better practice. Using DNS services introduces another point of failure for the voice network.

- **SNMP community string**—The Windows 2000 Simple Network Management Protocol (SNMP) agent provides security through the use of community names and authentication traps. Cisco sets the community rights to none for security reasons. If you want to use SNMP with this server, you must configure it.

- **Database server**—You must determine whether you will configure this server as a publisher database server or as a subscriber database server through a radio button selection during the Cisco CallManager installation. This selection is permanent. You must reinstall the Cisco CallManager server if you want to reassign the database server type at a later date.

NOTE   You must install a Cisco CallManager publisher server before you can install any subscriber servers. When you are configuring a subscriber database server, ensure that the server that you are installing can connect to the publisher database server during the installation. This connection facilitates the copying of the publisher database to the local drive on the subscriber server. You must supply the name of the publisher database server and a username and password with administrator access rights on that server. The installation will be discontinued if, for any reason, the publisher server cannot be authenticated.

- **New password for the system administrator**—Cisco CallManager Releases 3.0 and later support password protection. A prompt at the end of the installation procedure will ask you to supply a new password for the system administrator.

NOTE   For Cisco CallManager database replication, you must enter the same Administrator account password for the publisher and all of the subscribers in the cluster. The installation wizard will request this password.

Sample Configuration Data Worksheet

Table 3-1 shows the configuration information that you need to install the Cisco CallManager software on your server. You should complete all of the fields in the table, unless otherwise noted. You must gather this information for each Cisco CallManager server that you are installing in the cluster. Make copies of this table, and record your entries for each server in a separate table. Table 3-1 summarizes the data you should have available when you begin the installation.

Table 3-1   *Configuration Data for Cisco MCS*

Configuration	Data
Cisco product key	
Username	
Name of your organization	

Table 3-1   *Configuration Data for Cisco MCS (Continued)*

Configuration	Data
Computer name	
Workgroup	
Microsoft NT domain (optional)	
DNS domain suffix	
Current time zone, date, and time	
DHCP parameters	It is recommended that you program a fixed IP address in TCP/IP properties for the server instead of using DHCP.
TCP/IP properties (required if DHCP is not used): • IP address • Subnet mask • Default gateway	
DNS servers (optional): • Primary • Secondary WINS servers (optional): • Primary • Secondary • LMHOSTS file (optional)	
Database server (choose one): • Publisher • Subscriber If you are configuring a subscriber server, supply the username and password of the publishing database server: • Publisher username • *Publisher password*	
Backup (choose one or both): • Server • Target	
New Windows 2000 administrator password	

Postinstallation Procedures

After you complete the Cisco CallManager software installation, the installation wizard will prompt you to change all passwords used in the Cisco CallManager cluster. These passwords should be the same on all servers you install into the cluster. In addition, many supporting services are running on your server that you might be able to stop. The fewer services you have running on your server, the more server resources you will have available to support the IP telephony network. In addition, running more services on the Cisco CallManager server introduces more security vulnerabilities for the underlying Windows operating system. You should stop all of the following services on both the Publisher and Subscriber servers in your cluster and set them to manual-start status unless they are otherwise needed on the system:

- DHCP client

- Fax service

- FTP Publishing Service

- Smart Card (unless using security tokens)

- Smart Card Helper

- Computer browser

- Distributed File System

- License Logging Service

By default, the installation wizard configures all Subscribers with Internet Information Server (IIS) Services running. This allows you to make changes to the cluster by accessing the web interface on your subscriber servers. Even though you are accessing the web interface on the Subscriber server, the changes are actually being made on the Publisher server (because it has the only writable copy of the database). In addition, allowing the web services to run on all Subscriber servers introduces more security risk as there are now multiple points of access for the Cisco CallManager administration interface. Because of this, it is usually best to save the Subscriber resources by stopping the web services on all servers except the Publisher. You can accomplish this by stopping the following services:

- Microsoft Internet Information Server (IIS) Admin Service

- World Wide Web Publishing Service

You can stop all of these services through the Windows 2000 Services console. To open this console, click **Start > Programs > Administrative Tools > Services**. When the console opens, Windows lists all services in alphabetic order. Right-click on the service you want to disable and choose **Properties**. In the Properties window shown in Figure 3-1, use the drop-down box to select

either a **Manual** startup or to **Disable** the service. These will take effect the next time you reboot the Cisco CallManager server. You can also choose to stop the service without restarting the server from this page.

> **TIP**   Because Cisco CallManager requires these services to be active when upgrading to new Cisco CallManager versions, setting them to a state of Manual is suggested.

Figure 3-1   *Windows 2000 Service Properties*

Activating Cisco Unified CallManager Services

If you are installing Cisco CallManager for the first time, all services that are required to run Cisco CallManager automatically install on the system; however, none of the services are activated at the completion of the installation (except for the Cisco Database Layer Monitor service). Cisco CallManager Serviceability provides a web-based Service Activation tool that is used to activate or deactivate multiple services and to select default services to activate.

It is recommended that you activate only the required components for each server in the cluster. Each component that you activate adds to the server load.

If you are upgrading Cisco CallManager, the services that you have already started on your system will start after the upgrade.

Each service performs specific functions for the IP telephony network. Some services might need to run on a single Cisco CallManager server in a cluster; other services might need to run on all of the Cisco CallManager servers in the cluster.

> **CAUTION**   Be sure to activate at least the Cisco CallManager service before you apply any configuration to your Cisco CallManager server. Failure to do so can lead to unpredictable results, potentially leading to a server reinstall.

The following information briefly describes each available Cisco CallManager service:

■ **Cisco CallManager Service**—Allows the server to participate in telephone registration, call processing, and other Cisco CallManager functions. Cisco CallManager Service is the core service of the Cisco CallManager platform.

■ **Cisco TFTP**—Activates a TFTP server on Cisco CallManager. The TFTP service delivers Cisco IP Phone loads and configuration files to IP Phones, along with streamed media files, such as music on hold (MOH) and ring files.

■ **Cisco Messaging Interface**—Allows Cisco CallManager to interface with a Simplified Message Desk Interface (SMDI)-compliant, external voice-mail system.

■ **Cisco IP Voice Media Streaming Application**—Allows Cisco CallManager to act as a Media Termination Point (MTP), a conference bridge, a music on hold (MOH) server, and an annunciator. The voice network uses these media resources for feature functionality.

■ **Cisco CTIManager**—Allows Cisco CallManager to support computer telephony integration (CTI) services and provides Telephony Application Programming Interface (TAPI) or Java Telephony Application Programming Interface (JTAPI) client support. Cisco CTIManager allows you to use applications such as Cisco IP SoftPhone.

■ **Cisco Telephony Call Dispatcher**—Distributes calls to multiple telephone numbers (hunt groups). Cisco WebAttendant, Attendant Console, and Auto Attendant require Cisco Telephony Call Dispatcher (TCD).

■ **Cisco MOH Audio Translator**—Allows Cisco CallManager to convert MP3 or WAV audio files into voice codec format used for MOH.

■ **Cisco Real-Time Information Server (RIS) Data Collector**—Allows Cisco CallManager to write trace and alarm file information to a database, Microsoft Event Viewer, or alert an SNMP server.

- **Cisco Database Layer Monitor**—Monitors aspects of the Microsoft SQL 2000 database, as well as call detail records (CDRs).

- **Cisco CDR Insert**—Allows Cisco CallManager to write CDRs to the local database and replicates CDR files to the Microsoft SQL publisher at a configured interval.

- **Cisco CTL Provider**—Works with the Cisco Certificate Trust List (CTL) client to change the security mode for the cluster from nonsecure to secure (called mixed mode).

- **Cisco Extended Functions**—Provides support for some Cisco CallManager features, including Cisco Call Back and Quality Report Tool (QRT).

- **Cisco Serviceability Reporter**—Generates the following daily reports: Device Statistics, Server Statistics, Service Statistics, Call Activities, and Alert.

- **Cisco WebDialer**—Provides click-to-dial functionality by using a web page or a desktop application.

- **Cisco IP Manager Assistant**—Allows Cisco CallManager to support the Cisco IP Manager Assistant (IPMA), an application designed to allow a receptionist and manager to support special functionality between their phones.

- **Cisco CallManager Extension Mobility**—Allows Cisco CallManager to support extension mobility functions for roaming users. By using extension mobility features, you can assign users roaming phone profiles that activate when they log in to a phone. Works similarly to the roaming profiles in a Windows-based domain environment.

- **Cisco Certificate Authority Proxy Function**—Working in conjunction with the Cisco Certificate Authority Proxy Function (CAPF) application, the Cisco CAPF service can perform the following tasks, depending on your configuration:

  — Issues locally significant certificates to supported Cisco IP Phone models

  — Requests certificates from third-party certificate authorities on behalf of supported Cisco IP Phone models

  — Upgrades existing certificates on the phones

  — Retrieves phone certificates for troubleshooting

  — Deletes locally significant certificates on the phone

You must activate the Cisco CallManager services from the Service Activation web interface rather than the Windows 2000 Services control panel. To access this interface, perform the following steps:

Step 1 Open Internet Explorer, and go to https://<CallManager_IP_Address>/ ccmadmin. The <CallManager_IP_Address> is the IP address of the Cisco CallManager server that is running IIS web services. Enter the administrative username and password information.

Step 2 From the Application menu, choose **Cisco CallManager Serviceability**. The Cisco CallManager Serviceability interface appears.

Step 3 From the Tools menu, choose **Service Activation**. A window similar to the window shown in Figure 3-2 appears.

Figure 3-2 *Cisco CallManager Service Activation Interface*
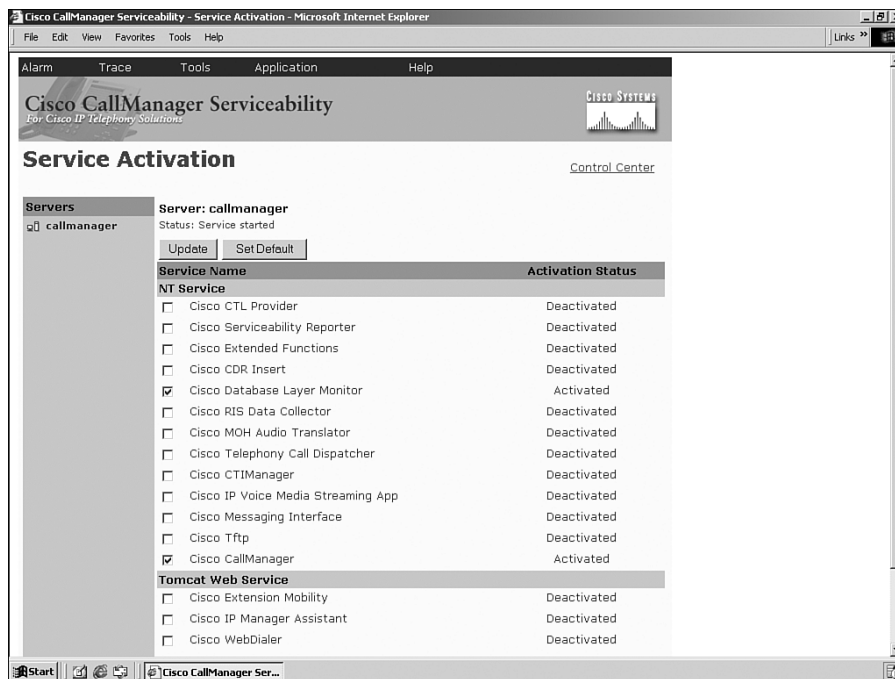
Step 4 Click the server that you want to configure from the Servers column. Next click the services that you want to activate, and click the **Update** button. (You will experience a slight delay.) The Service Activation window will refresh when the process is complete.

> **TIP**   The method shown is just one way to access the Cisco CallManager Serviceability pages. If you are working on the Cisco CallManager itself, you can get there quicker by using the Windows 2000 Start menu (**Start > Programs > Cisco CallManager > Cisco CallManager Serviceability**) or by accessing https://<CallManager-IP-Address>/CCMService.

> **CAUTION**   Remember to activate the Cisco CallManager services from the Service Activation web interface. Activating the services through the Windows 2000 Services console will produce unpredictable and unstable results.

When you click the **Set Default** button in the web interface, the Service Activation tool chooses the services required to run Cisco CallManager based on a single-server configuration. This is the bare minimum to have a working Cisco CallManager–based IP telephony network. Because Cisco highly advises against single-server installations, you will most likely use the **Set Default** button in a lab environment.

Upgrading Prior Cisco Unified CallManager Versions

Cisco supports the upgrade to Cisco CallManager 4.1 from Cisco CallManager Release 3.3(4), 3.3(5), 4.0(1), and 4.0(2a). You must first upgrades earlier versions to one of these releases before you can upgrade to version 4.1.

> **NOTE**   Cisco CallManager 4.1(3) is the most recent version available at the time of this writing. If you are upgrading to a more recent version, refer to the specific upgrade instructions provided in the documentation for the more recent Cisco CallManager version.

If your server runs a version of Cisco CallManager Release 3.2 or earlier, you must first upgrade every server in the cluster to the latest version of Cisco CallManager Release 3.3 before you can upgrade to a version of Cisco CallManager Release 4.1. This is because the database structure and storage system changes from versions prior to release 3.3. (Earlier versions use SQL 7.0 rather than SQL 2000.)

Before you perform any upgrade procedures, it is strongly recommended that you install the latest operating system upgrade and service release, SQL service releases and hotfixes, and Cisco CallManager service release for the versions that currently run in the cluster. Cisco provides the service release and corresponding "readme" documentation on Cisco.com. To obtain these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml (CCO login is required).

> **NOTE**   Cisco releases all service packs, hotfixes, and Windows operating system upgrades through the CCO website. Updates released by Microsoft should *never* be applied to the Cisco CallManager server as they can potentially cause the Cisco CallManager software to become unstable or to crash. Cisco guarantees that they will release any critical operating system patch within 24 hours of the Microsoft announcement. Noncritical patches are rolled up into a monthly update.

Cisco requires that you install Cisco IP Telephony Server Operating System Version 2000.2.6 (available from Cisco CCO) before you upgrade to Cisco CallManager Release 4.1.

> **CAUTION**   Because the foundation operating system components might change, the upgrade procedure will many times require you to back up the database on the Publisher server, reimage Cisco CallManager completely (using the clean installation method discussed earlier in the chapter), and then restore the SQL data from backup. If your version of Cisco CallManager requires this, be absolutely sure to install the newer backup software on the Cisco CallManager you are upgrading before you initially back up the database. Many times, the backup software changes between the 3.x and 4.x versions of Cisco CallManager. Because of this, you will usually find the latest version of the backup software in the /backup folder on the first Cisco CallManager Installation CD-ROM. If you do not install the new backup software before performing the Cisco CallManager upgrade, your backup file (and SQL data) might be unreadable in the new Cisco CallManager version.

Because many of the Cisco CallManager servers are equipped with RAID 1 configurations (mirrored hard disks), a common upgrade strategy is as follows:

Step 1   Remove the mirrored hard disk from the production Cisco CallManager server.

Step 2   Boot a lab server using the mirrored hard disk.

Step 3   Perform the Cisco CallManager software upgrade on the mirrored hard disk.

Step 4   During a scheduled window of downtime, reboot the production server using the upgraded, mirrored drive.

Step 5   The hard drive running the older Cisco CallManager version will become the new, backup mirrored drive.

By using this upgrade process, you can reduce the amount of voice network downtime to the amount of time it takes to reboot the Cisco CallManager server on the upgraded drive.

> **CAUTION**   The upgrade process described will cause a loss of any database changes performed from the time you have removed the mirrored drive until the time you reboot your Cisco CallManager server using the new version. Plan your upgrade windows accordingly.

Summary

This chapter covered the Cisco CallManager installation and upgrade process. When you purchase a Cisco MCS and Cisco CallManager software, you will receive a number of CDs (and even DVDs). Of those, you will only need three discs for the installation: the hardware detection CD, the operating system CD/DVD, and the Cisco CallManager installation CD/DVD. The installation itself is very automated and disk image-based. It requires very little knowledge of the foundation Windows 2000 operating system and SQL 2000 database store. After the installation completes, you should stop any unnecessary services running on your Cisco CallManager and start the Cisco CallManager services required for your network.

The upgrade process for Cisco CallManager varies wildly depending on the version of Cisco CallManager you are using. The process can be as simple as inserting the Cisco CallManager installation disk and following a step-by-step wizard or as complex as a complete reimage of all servers in the cluster. The key is to make sure that you have backed up all data from the SQL server with the newest version of the backup software available from the Cisco CallManager installation CD-ROM or the Cisco website.

Review Questions

You can find the solutions to these questions in Appendix A, "Answers to Review Questions."

1. Cisco CallManager uses which of these operating systems?

    a. Linux

    b. Windows NT

    c. Windows 2000

    d. Windows 2003

2. Why is it recommended that you stop IIS on the subscriber servers? (Choose two.)

   a. enhances server call processing and redundancy

   b. maximizes the number of devices in a cluster

   c. disables the use of remote terminal services

   d. helps prevent unauthorized access to the server

   e. makes more resources available for critical voice services

3. When you first install Cisco CallManager software, which CD-ROM should you use to boot the server to determine the correct CD-ROM to insert next?

   a. Cisco CallManager 4.0 Software Disk

   b. Cisco IP Telephony Server Operating System Hardware Detection Disk

   c. Cisco CallManager Installation, Upgrade, and Recovery Disk

   d. Cisco IP Telephony Server Backup and Restore Disk

   e. Cisco Extended Services and Locales Disk

4. If you are not using DNS, what must you configure to resolve server names for the Cisco CallManager installation process?

   a. DHCP

   b. backup server

   c. LMHOSTS file

   d. DNS reverse lookup

5. Which of the following represent Windows services that you are able to stop on both Publisher and Subscriber servers? (Choose three.)

   a. computer browser

   b. DHCP client

   c. database layer monitor

   d. CTL provider

   e. FTP Publishing Service

6. If you want to set up a Cisco CallManager as a single-server configuration in a lab environment, what button can you click on the Service Activation web page to start the necessary services?

   a. Single Server

   b. Lab

   c. Set Default

   d. Minimal Service

7. You have just completed the installation of a Cisco CallManager server, entered the new passwords for all accounts, and restarted. What is the next step you should take?

    a. Configure the Cisco CallManager server settings to send IP address information to the IP Phones rather than hostname.

    b. Activate the necessary services through the Service Activation web page.

    c. Upgrade the backup software to the latest version.

    d. Apply the latest operating system service pack from the Cisco website.