Upgrading Cisco CallManager

Release 4.0(2)

Corporate 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: 408 526-4100

Text Part Number: 78-16385-01

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

The preface covers these topics:

Purpose of Document

This document provides Cisco CallManager upgrade procedures and requirements for the Cisco Media Convergence Server and the customer-provided server that meets approved Cisco configuration standards.

This document contains information on the following topics:

Tip Use this document in conjunction with the documents that are listed in the "Locating Related Documentation" section on page viii.

Audience

The *Upgrading Cisco CallManager* document provides information for network administrators who are responsible for maintaining the Cisco CallManager system. This guide requires knowledge of telephony and IP networking technology.

Conventions

Consider the following documentation conventions as you review this upgrade document:

Using the Cisco IP Telephony Applications Backup Utility, Version 3.5.52 (or later) replaces the document, *Backing Up and Restoring Cisco CallManager Release 3.3*.

Unless otherwise specified, base server model numbers will be used in this document. For example references to the MCS-7835 apply to servers including the MCS-7835, the MCS-7835-1000, the MCS-7835-1266, the MCS 7835H-2.4, the MCS-7835I-2.4, MCS-7835H-3.0, MCS-7835I-3.0, the customer-provided DL380, and the customer-provided IBM xSeries 342 and 345.

Blue Text—To quickly navigate to a section or URL from your computer, click text that appears in blue.

Note Reader, take note. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Reader, be careful. You may do something that could result in equipment damage or loss of data.

Timesaver Reader, this tip saves you time as you perform the procedure.

(Required)

This convention indicates that you must perform the procedure. Failing to perform the procedure could cause a total system failure or a loss of data and configuration settings.

(Recommended)

This convention indicates that the procedure is strongly recommended, but not required.

Locating Related Documentation

Cisco strongly recommends that you review the following documents before you upgrade:

- *Release Notes for Cisco CallManager Release 4.0*

  Cisco provides a version of this document that matches the version of the upgrade document. Use this document as a companion guide to the upgrade document.

- *Cisco CallManager Compatibility Matrix*

  To ensure continued functionality with interfacing Cisco IP telephony applications after the Cisco CallManager upgrade, refer to the *Cisco CallManager Compatibility Matrix*, which provides information and workarounds for applications that are integrated with Cisco CallManager.

Affected applications may include Cisco Conference Connection, Cisco SoftPhone, Cisco uOne, Cisco 186 Analog Telephony Adaptor, Cisco Personal Assistant, Cisco Customer Response Solutions (CRS), Telephony Application Programming Interface and Java Telephony Application Programming Interface (TAPI/JTAPI) applications, including Cisco-provided and third-party applications, and Cisco Telephony Service Provider (TSP).

If you use Cisco CallManager and related Cisco IP telephony applications in a call-center environment, review this document before you begin any upgrade procedures.

- *Cisco IP Telephony Operating System, SQL Server, Security Updates*

  This document provides information on the latest operating system, SQL Server, and security support updates. Information in this document applies to servers that are running the following Cisco IP telephony applications: Cisco CallManager, Conference Connection, Personal Assistant, and Cisco Customer Response Applications/Solutions, and so on.

- *Using Cisco IP Telephony Applications Backup Utility, Version 3.5.52* (or later)

  This document describes how to install the utility, configure the backup settings, back up Cisco CallManager data, and restore the data/server.

  This document also provides a list of files that the utility backs up. This utility does not back up operating system files, except for Hosts/LMHosts files, if those files exist on the server.

- *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide 4.0(2)* (or later)

  This document describes how to install the BARS utility, configure the backup settings, back up Cisco CallManager data, and restore the data/server.

  This document also provides a list of files that the utility backs up. This utility does not back up operating system files, except for Hosts/LMHosts files, if those files exist on the server.

- The appropriate Cisco IP telephony application documentation

  Locate the release notes, installation/upgrade, and configuration guides for the applications that you have integrated with Cisco CallManager.

Click the URLs in Table 1 to navigate to the appropriate documentation.

Table 1 Quick Reference for URLs

Related Information and Software	URL and Additional Information
Operating system documentation and Virtual Network Computing (VNC) documentation (not readme documentation)	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
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
Cisco CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
Cisco CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm

Table 1 Quick Reference for URLs (continued)

Related Information and Software	URL and Additional Information
Cisco CallManager, SQL Server, and operating system service releases, upgrades, and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml See the "Verifying Services, Patches, and Hotfixes" section on page 5. **Note** The operating system and SQL Server 2000 service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

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/univercd/home/home.htm

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *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

- *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

- 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

Preinstallation Information

This section provides information that you should consider before upgrading a Cisco CallManager server and frequently asked questions (FAQs) regarding the Cisco CallManager 4.0 upgrade.

Important Considerations

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

- Install the Cisco CallManager software on the publisher server first and then on the subscriber server(s).
- Make sure that you are logged in as the administrator on the server before starting the Cisco CallManager installation.
- Install the Cisco CallManager software on one server at a time to ensure that subscriber servers can receive replicate copies of the database from the publisher database server.
- Make sure that the subscriber server that you are installing can connect to the publishing database server during the installation.
- Do not choose cancel after you start the installation. If you choose cancel, you will need to reimage your machine by reinstalling the operating system.
- Security settings for the Cisco CallManager server are set up by the installation and upgrade scripts. Do not make any adjustments to these pre-defined settings or you may experience a significant impact to the functionality of your server.
- When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, use alphanumeric characters only.
- Enter the same administrator password on all servers in the cluster.
- Install the Cisco CallManager software during off-peak hours or a maintenance window to avoid impact from call-processing interruptions.
- Do not configure any server in the cluster as a Domain Controller.
- Place the server in a Workgroup before you install the software.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco 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 use terminal services to install the Cisco CallManager software.

- Do not install any Cisco-verified applications until you complete installing Cisco CallManager on every server in the cluster.
- Cisco provides support for a limited set of applications on the servers where Cisco CallManager is installed. If you are uncertain whether a third-party application is supported, do not install it on the server.
- You must disable third-party, Cisco-verified applications on your servers before starting the Cisco CallManager installation.
- Install a security agent to protect your servers against unauthorized intrusion.
- Do not install Cisco Unity on a server where Cisco CallManager is installed.
- Installing or using Netscape Navigator on the Cisco MCS or the Cisco-approved, customer-provided server causes severe performance problems.
- Carefully read the instructions that follows before you proceed with the installation.

Frequently Asked Questions About Cisco CallManager 4.0 Upgrades

The following frequently asked questions apply for all Cisco CallManager 4.0 upgrades. For information that is specific to the version upgrade, see the following sections:

- Upgrading from Cisco CallManager 3.2 (If You Are Not Replacing Hardware), page 2-1
- Upgrading from Cisco CallManager 3.3 or Cisco CallManager 4.0(1) (If You Are Not Replacing Hardware), page 3-1

Tip If you are replacing hardware during the upgrade, skip to the "Replacing Servers During the Upgrade" section on page 7-1.

From which versions of Cisco CallManager can I upgrade to Cisco CallManager Release 4.0(2)?

To verify which versions of Cisco CallManager are compatible for upgrade, refer to the *Cisco CallManager Compatibility Matrix*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

If your server runs Cisco CallManager Release 2.4 or 3.0, you must upgrade every server in the cluster to the latest version of Cisco CallManager Release 3.2 before you can upgrade to a version of Cisco CallManager Release 4.0. For information on upgrading to Cisco CallManager Release 3.2, refer to the latest version of *Upgrading Cisco CallManager Release 3.2*.

Before you perform any upgrade procedures, Cisco strongly recommends that you install the latest operating system upgrade/service release, SQL service releases/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.

Caution Cisco recommends that you only upgrade to Cisco CallManager 4.0(2) from a version that is compatible for upgrade to 4.0(2). Versions that are not compatible for upgrade to 4.0(2) contain features that are not supported in 4.0(2). If you upgrade from an unsupported version, you cannot access those features that are not supported in 4.0(2), and you will lose the data that is associated with those features.

Which servers and operating system versions does Cisco support for this upgrade?

For Cisco CallManager Release 4.0(2), Cisco supports the servers that are listed in the *Cisco CallManager Compatibility Matrix*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.

Cisco recommends that you install Cisco-provided operating system version 2000.2.6 with the latest service release 2000.2.6.sr1 (or later) before you upgrade to Cisco CallManager Release 4.0(2).

For Cisco CallManager 3.2 Upgrades to 4.0(2)

You must perform a Same Server Recovery by using the operating system disks that ship with this version of Cisco CallManager to install operating system version 2000.2.4 before you upgrade to 2000.2.6sr1. "Upgrading from Cisco CallManager 3.2 (If You Are Not Replacing Hardware)" section on page 2-1.

You must use the Cisco CallManager 4.0(2) software kit to upgrade the Cisco CallManager software to version 4.0(2).

For Cisco CallManager 3.3 Upgrades to 4.0(2)

If your server runs Cisco CallManager 3.3 and operating system version 2000.2.3 (or later), you can use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to 2000.2.6sr1 or later. For detailed instructions, refer to "Upgrading from Cisco CallManager 3.3 or Cisco CallManager 4.0(1) (If You Are Not Replacing Hardware)" section on page 3-1.

You must use the Cisco CallManager 4.0(2) software kit to upgrade the Cisco CallManager software to version 4.0(2)

For Cisco CallManager 4.0(1) Upgrade to 4.0(2)

If your server runs Cisco CallManager 4.0(1), you can use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to 2000.2.6sr1 or later. For detailed instructions, refer to "Upgrading from Cisco CallManager 3.3 or Cisco CallManager 4.0(1) (If You Are Not Replacing Hardware)" section on page 3-1.

You can upgrade to Cisco CallManager 4.0(2) using the Cisco CallManager 4.0(2) software kit or the Cisco CallManager 4.0(2) web download file.

What disks do I need to gather before I upgrade?

If you are upgrading from Cisco CallManager 3.2, you must upgrade via the disks that come in the software kit.

Before you upgrade from Cisco CallManager 3.2, locate the following disks.

- Cisco IP Telephony Server Operating System Hardware Detection Disk
- Cisco IP Telephony Server Operating System Installation and Recovery Disk

  If you are upgrading to Cisco CallManager 4.0 from 3.2, you must use the server-specific operating system disk that comes in the software kit. During the operating system installation, you receive a prompt to insert the appropriate disk into the drive.
- Cisco IP Telephony Server Operating System OS Upgrade Disk

  This disk upgrades the operating system on existing (not new) servers in the cluster.
- Cisco CallManager 4.0 Backup Utility Disk (For Cisco CallManager Publisher Servers)

  You use this disk to start the publisher database server upgrade. This disk installs the backup utility that you must use prior to the upgrade.
- Cisco CallManager 4.0 Subscriber Preparation Disk

  You use this disk to start all subscriber server upgrades. This disk installs the ServPrep utility.
- Cisco CallManager 4.0 Installation, Upgrade, and Recovery Disk 1 and 2

  You use these disks to complete the Cisco CallManager upgrade. This disk installs Cisco CallManager, Microsoft SQL Server 2000, and DC Directory. If you are upgrading from Cisco CallManager 3.2, the disk also installs Microsoft SQL Server 2000 Service Pack 3a (or later).

Which server in the cluster do I upgrade first?

Caution When you perform the Cisco CallManager portion of the upgrade, you must upgrade one server at a time, so the subscriber servers can pull the replicas of the database from the publisher database server. For the subscriber servers to pull the replicas, the publisher database server must be running, and you must not make any changes on the publisher database server while you are upgrading the subscriber servers. After you complete the upgrade on one server and reboot the server, you can start the upgrade on the next server.

Caution This document assumes that all servers are functional and running. If the servers are not functional and running, failover will not occur.

You must upgrade all the servers in the cluster. The order varies depending on the cluster configuration.

Cisco CallManager Runs on the Publisher

If the Cisco CallManager service runs on the publisher database server (two-server cluster), upgrade the servers in the following order:

1. Upgrade the publisher database server.

   When you perform an upgrade, the Cisco CallManager service automatically stops, and the devices that are homed to the publisher database server failover to the subscriber server.
2. Upgrade the subscriber.

Cisco CallManager Does Not Run on the Publisher

If the Cisco CallManager service does not run on the publisher database server, upgrade the servers in the following order:

1. Upgrade the publisher database server.
2. Upgrade the Cisco TFTP server, if it exists separately from the publisher database server.
3. Upgrade servers, one server at a time, that have only Cisco CallManager-related services (Music on Hold, Cisco IP Media Streaming Application, and so on) running on them.

   Make sure that you upgrade only one server at a time.

   Make sure that the Cisco CallManager service does not run on these servers.
4. Upgrade each secondary server, one server at a time.

   If you choose to oversubscribe the secondary server(s) during the upgrade, Cisco strongly recommends that you have no more than 5,000 devices that are registered to the secondary server during the upgrade and that you oversubscribe the secondary server(s) for no more than a few hours. Cisco strongly recommends that you perform the upgrade during off-peak hours when low call volume occurs (less than 1,000 busy hour call attempts).

   If you configured your Cisco CallManager cluster by using approved Cisco configuration standards, which include configuring four primary servers and two secondary servers in the cluster, you can minimize call-processing interruptions if you register all devices to servers that are running the same version of Cisco CallManager during the entire upgrade process; for example, you register all devices to the secondary Cisco CallManager servers or the primary Cisco CallManager servers, but not to both types of servers.
5. Upgrade each primary server that has the Cisco CallManager service running on it. Remember to upgrade one server at a time.

Caution When you upgrade the primary server(s), call-processing interruptions may occur for up to 30 minutes while the devices attempt to obtain the device loads and register to the upgraded version of Cisco CallManager.

6. Upgrade servers that have Cisco IP telephony applications running on them; for example, Cisco Conference Connection or Cisco Emergency Responder. Remember to upgrade one server at a time. Refer to the application documentation for more information.

How does a coresident upgrade work if I have CRS installed with Cisco CallManager?

For information on how to perform the upgrade on a coresident server, refer to the CRS documentation that is compatible with this version of Cisco CallManager.

How long does it take to upgrade the cluster?

To minimize call-processing downtime, Cisco strongly recommends that you perform all upgrade procedures for the Cisco CallManager and all upgrades/reinstallations for Cisco IP telephony applications within a consecutive time period (within one maintenance window).

Before you perform an upgrade, consider the time that it takes to perform pre-/post-upgrade tasks, Cisco IP telephony application upgrades/reinstallations, and Cisco-verified application upgrades/reinstallations.

For the time that it takes to perform specific tasks on the publisher database server, see the following sections:

- From Cisco CallManager 3.2—Upgrading from Cisco CallManager 3.2 (If You Are Not Replacing Hardware), page 2-1
- From Cisco CallManager 3.3—Upgrading from Cisco CallManager 3.3 or Cisco CallManager 4.0(1) (If You Are Not Replacing Hardware), page 3-1

Will I experience call-processing interruptions and a loss of services during the upgrade?

Review the following information before you upgrade.

About Minimizing Call-Processing Interruptions

When you upgrade a cluster, two separate versions of Cisco CallManager run in the cluster at the same time. Be aware that the different Cisco CallManager versions that are running in the cluster will not interact and may cause call-processing interruptions to occur.

If you configured your Cisco CallManager cluster by using approved Cisco configuration standards, which include configuring four primary servers and two backup servers in the cluster, you can minimize call-processing interruptions if you register all devices to servers that are running the same version of Cisco CallManager during the entire upgrade process; that is, you register all devices to the backup Cisco CallManager servers or the primary Cisco CallManager servers, but not to both types of servers.

About a Loss of Services

During the upgrade, Cisco CallManager places Cisco CallManager-related services that display in Cisco CallManager Serviceability in an inactive state. After the upgrade completes, migrated services activate and start after the server reboots. To use additional services, you must activate the service on each server on which you want the service to run. For information on activating services, refer to the *Cisco CallManager Serviceability Administration Guide* or to online help in the Cisco CallManager application.

Caution Cisco strongly recommends that you perform the upgrade during a single maintenance window to minimize call-processing interruptions.

May I use Terminal Services, Virtual Network Computing, and Integrated Lights Out to remotely upgrade the server?

Do not use Terminal Services to upgrade to Cisco CallManager Release 4.0(2). Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote administration and troubleshooting tasks. Cisco does not support upgrades through Terminal Services.

Caution Before the upgrade, Cisco strongly recommends that you disable Terminal Services and immediately reboot the server to prevent remote access to the server. Accessing the server via Terminal Services may cause the upgrade to fail.

After you upgrade the server, you must enable Terminal Services.

If you want to use Virtual Network Computing (VNC) to remotely upgrade the publisher database server, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm to obtain the latest version of the VNC document.

Caution If you have installed VNC but do not plan to use it to perform the upgrade, disable it to prevent remote access to the server. If you do not disable VNC and a user/administrator accesses the server during the upgrade, the upgrade will fail.

Do not use Integrated Lights Out (ILO) to perform upgrade or installation tasks. Cisco supports ILO for remote management and configuration tasks only.

May I configure a server in the cluster as a Domain Controller?

Do not configure any server in the cluster as a Domain Controller. If you configure any server in the cluster as a Domain Controller, you cannot upgrade or reinstall Cisco CallManager on the server.

May I perform configuration tasks during the upgrade?

Caution Do not attempt to perform any configuration tasks during the upgrade. Before the upgrade begins, disable all services that allow any administrator to perform remote configuration tasks. For example, disable Terminal Services or VNC before the upgrade to prevent an administrator from browsing into the server during the upgrade.

Notify all users that the upgrade is occurring, so users do not browse into the server during the upgrade.

Performing configuration tasks during the upgrade causes an upgrade failure.

May I remove a drive before I upgrade?

Caution You cannot remove a drive if you have the MCS-7815, MCS-7820, MCS-7822, MCS-7825, or customer-provided IBM xSeries 330 server.

Removing a Drive If the Server Runs Cisco CallManager 3.2—Replacement Drive Required

After you verify that you have a good backup of the data, you can remove a drive to save configured data; however, you must insert a replacement drive into the server before you begin the operating system procedures. The "Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)" section on page 2-19 describes how to properly perform this task.

This task may require that you purchase a new drive.

Before you begin the operating system installation, make sure that you have all drives in the server and verify that the drives are functional. For example, insert two drives for the MCS-7835 and four drives for the MCS-7845. Neglecting to perform these tasks causes the failure of the Cisco CallManager installation and the loss of data/configuration settings from drive mirroring.

Removing a Drive If the Server Runs Cisco CallManager 3.3—Inserting a Replacement Drive and Drive Mirroring Prior to the Upgrade

The "Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)" section on page 3-11 describes how to properly perform this task.

Removing a Drive If the Server Runs Cisco CallManager 3.3—Upgrading With One Drive In the Server

Perform the following procedure if you plan to remove a drive and upgrade with only one hard drive in the server.

Step 1 Power off the publisher database server.

Step 2 For all servers except the MCS-7845, remove the hard drive from Slot 0 and label the drive with the machine name, slot number, and current version of Cisco CallManager.

For the MCS-7845, remove the drives from Slot 0 and Slot 2 and label them with the appropriate information.

Step 3 Power on the system.

Cisco MCS

Step 4 Perform the following procedure for the Cisco MCS (The MCS-7845 requires two spare hard drives):

a. To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845, press **F2**.

Note The MCS-7835H-2.4 (or later) and MCS-7845H-2.4 (or later) default to F2, and the process automatically continues after a 10-second delay.

b. This step applies only for the MCS-7830, MCS-7835, or MCS-7845. When prompted, press **F1** to continue.

Step 5 Log in to the server by using the Administrator password.

IBM xSeries Server

Step 6 To enable interim recovery mode on the customer-provided IBM xSeries 342 server, press **F5**.

Step 7 Log in to the server by using the Administrator password.

Which third-party, Cisco-verified applications may I install on the Cisco CallManager server?

Caution Cisco supports a limited list of applications on the servers where Cisco CallManager is installed. If you are uncertain whether a third-party application is supported, do not install it on the server.

To review a list of third-party, Cisco-verified applications that you may install on the server, perform the following procedure:

Procedure

Step 1 Click http://www.cisco.com/pcgi-bin/ecoa/Search.

Step 2 In the Solution pane, click **IP Telephony**.

Step 3 From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**.

Step 4 Click **Search**.

Caution Installing or using Netscape Navigator on the Cisco MCS or the Cisco-approved, customer-provided server causes severe performance problems.

Which Cisco IP telephony applications may I install on the Cisco CallManager server?

Consider the following information before you install other software besides Cisco CallManager on the Cisco MCS or the customer-provided server:

- You can install a compatible version of Cisco Customer Response Solutions (CRS), which you must purchase separately from Cisco CallManager.
- Do not install Cisco Unity, Cisco Conference Connection, Cisco Personal Assistant, or Cisco Emergency Responder on the server where Cisco CallManager is installed.
- Cisco strongly recommends that you install a security agent to protect your servers against unauthorized intrusion. Cisco offers two security agent options: Cisco Security Agent (CSA) for Cisco CallManager and Management Center for Cisco Security Agent (CSA MC).

  CSA for Cisco CallManager designates a standalone agent and security policy that is designed to be used on all servers in the voice cluster. The policy that is included with this agent gets configured specifically for Cisco CallManager and Customer Response Applications (CRA), and you cannot update or view it. You can download the agent from CCO at http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des.

  If you want to add, change, delete, or view rules and policies that CSA for Cisco CallManager includes, or if you want to add support for non-Cisco approved, third-party applications, you must purchase and install the fully managed console, CSA MC. CSA MC requires a separate dedicated server to be used as the management center. This management center allows you to create agent kits that are then distributed to agents that are installed on other network systems and servers.

  To access information on Cisco Security Agent, see http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm and http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/csa_4_0/index.htm

Caution If you are uncertain whether a Cisco IP telephony application is supported on the Cisco CallManager server, do not install it.

What additional information should I know before I upgrade?

This document assumes that all servers in your cluster are currently in an operational state.

About Security and Account Policies

Caution If you change any security or account policies from the default, the upgrade may fail. For more information on security and account policies, refer to Microsoft documentation.

About Service and Enterprise Parameters in Cisco CallManager Administration

Cisco CallManager always updates service parameters with nonnumeric values to the suggested value.

If your service parameters are set to the suggested value, Cisco CallManager automatically updates the value during the upgrade to match the new suggested value.

If your customized value exists between the range of minimum and maximum values, Cisco CallManager does not change the customized value.

If you configured customized values that are not between the minimum and maximum range of values, the customized value changes during the upgrade to the maximum or minimum value. For example, if the maximum value equals 10 and the value that you configured is 12, Cisco CallManager automatically sets the value to 10.

During the upgrade, some non-servicewide parameters may change to clusterwide parameters (formerly known as servicewide parameters).

About H.323 Intercluster Trunks

A registration problem occurs when multiple Cisco CallManager clusters have the same device name assigned to more than one H.323 intercluster trunk in Cisco CallManager Administration. You must assign a unique device name to each H.323 intercluster trunk. Refer to the *Cisco CallManager Administration Guide* for information on the trunk configuration procedure.

About H.323 Gateways

Cisco no longer provides the Run H.225D On Every Node option in Cisco CallManager Administration for H.323 gateways. Before you upgrade, verify that all H.323 dial-peer(s) point to a Cisco CallManager server in the device profile for which they are assigned. If the session target statements in the dial-peer(s) do not point to the appropriate Cisco CallManager server, calls fail.

About the Database

After you upgrade Cisco CallManager, the database name automatically increments; for example, from CCM0300 to CCM0301. Third-party CDR software may have SQL triggers that are hard coded to the original database name. The triggers may point to the previous database name and cause all CDR flat files to write to the BAD directory on the publisher database server. If you need technical assistance with this issue, directly contact the third-party software vendor.

About Cisco CallManager Extension Mobility

If you run Cisco CallManager Extension Mobility and Cisco CallManager 3.2 before the upgrade, you must perform additional configuration tasks after the upgrade, so Cisco CallManager Extension Mobility runs as expected. For more information on configuration tasks, refer to the Cisco CallManager Extension Mobility upgrade section of the *Cisco CallManager Features and Services Guide for 4.0(1)*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

When should I perform post-upgrade tasks?

Do not perform any post-upgrade tasks until you complete the upgrade on all servers in the cluster.

What if I encounter problems during the upgrade?

Cisco recommends that if you encounter problems during the upgrade, take the following actions:

1. During the upgrade if you receive a message that displays in a dialog box, see the "Error Messages" section on page 6-1 and perform the recommended corrective action.
2. Obtain and review all log files from C:\Program Files\Common Files\Cisco\Logs; for example, C:Dcdsrvr\log, C:*.log, C:*txt.

Be aware that not all messages that display in the log file are catastrophic. MSI generates messages in the log file for many reasons; for example, attempts to access a service that Cisco CallManager does not use.

Upgrading from Cisco CallManager 3.2 (If You Are Not Replacing Hardware)

You must upgrade Cisco CallManager on the publisher database server and all subscriber servers in the cluster. For the order of the upgrade, see the "Which server in the cluster do I upgrade first?" section on page 1-4.

Caution To successfully upgrade the publisher and subscriber database servers, you must perform all procedures exactly as stated in this document.

This section contains procedures and information on the following topics:

Before You Begin

Before you start the upgrade, make sure that you perform the following tasks:

	Pre-Upgrade Task	Related Topics
Step 1	Make sure that you run a recommended version of Cisco CallManager on all servers in the cluster.	From which versions of Cisco CallManager can I upgrade to Cisco CallManager Release 4.0(2)?, page 1-2
Step 2	Make sure that you understand the order in which you must upgrade the cluster.	Which server in the cluster do I upgrade first?, page 1-4 How does a coresident upgrade work if I have CRS installed with Cisco CallManager?, page 1-5

	Pre-Upgrade Task	Related Topics
Step 3	In Cisco CallManager Administration, make sure that you only add each server once on the Server Configuration window (**System > Server**). If you add a server using the host name and add the same server using the IP address, Cisco CallManager cannot accurately determine component versions for the server after a Cisco CallManager upgrade. If you have two entries in Cisco CallManager Administration for the same server, delete one of the entries before you upgrade.	Refer to the *Cisco CallManager Administration Guide*.
Step 4	Make sure that your server configuration supports this upgrade.	Which servers and operating system versions does Cisco support for this upgrade?, page 1-3
Step 5	Make sure you have enough available disk space on each of your servers for the Cisco CallManager upgrade. If you use the Cisco CallManager disks to upgrade, you need 2.0 gigabytes of disk space. If you use the web file to upgrade, you need 3.0 gigabytes of disk space.	
Step 6	If you run Cisco CallManager Extension Mobility and Cisco CallManager 3.2 before the upgrade, you must perform additional configuration tasks after the upgrade, so Cisco CallManager Extension Mobility runs as expected.	For more information, refer to the Cisco CallManager Extension Mobility upgrade section of the *Cisco CallManager Features and Services Guide for 4.0(1)*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
Step 7	If you are using Cisco Unity as your voice-messaging system, configure the voice mail ports in Cisco CallManager to ensure proper migration.	For more information, refer to the *Release Notes for Cisco CallManager.* To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
Step 8	You must assign a unique device name to each H.323 intercluster trunk. A registration problem occurs when multiple Cisco CallManager clusters have the same device name assigned to H.323 intercluster trunks in Cisco CallManager Administration.	Refer to the *Cisco CallManager Administration Guide* for information on the trunk configuration procedure.
Step 9	Verify that all H.323 dial-peer(s) point to a Cisco CallManager server in the device profile for which they are assigned. Cisco no longer provides the Run H.225D On Every Node option in Cisco CallManager Administration for H.323 gateways. If the session target statements in the dial-peer(s) do not point to the appropriate Cisco CallManager server, calls fail.	Refer to the *Cisco CallManager Administration Guide* for information on the gateway configuration procedure.

	Pre-Upgrade Task	Related Topics
Step 10	Perform the recommended backup procedures for all coresident software applications that are installed on the server. **Caution** Failing to complete a backup causes a loss of data and configuration settings. For information on performing the backup, refer to the documentation that supports the applications. The Cisco IP Telephony Applications Backup Utility does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Using Cisco IP Telephony Applications Backup Utility, Version 3.5.52* (or later). To obtain the latest version of the document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.	How does a coresident upgrade work if I have CRS installed with Cisco CallManager?, page 1-5
Step 11	Be aware that if you change any security or account policies from the default, the upgrade may fail.	For more information on security and account policies, refer to Microsoft documentation.
Step 12	Understand how Cisco CallManager updates service parameters. **For Service Parameters with Nonnumeric Values** Cisco CallManager always updates service parameters with non-numeric values to the suggested value. **For Service Parameters with Numeric Values** If your service parameters are set to the suggested value, Cisco CallManager automatically updates the value during the upgrade to match the new suggested value. If your customized value exists between the range of minimum and maximum values, Cisco CallManager does not change the customized value. If you configured customized values that are not between the minimum and maximum range of values, the customized value changes during the upgrade to the maximum or minimum value. For example, if the maximum value equals 10 and the value that you configured is 12, Cisco CallManager automatically sets the value to 10. During the upgrade, some non-servicewide parameters may change to clusterwide parameters (formerly known as servicewide parameters).	For more information on service parameters, refer to the *Cisco CallManager Administration Guide* and the *Cisco CallManager System Guide*.

	Pre-Upgrade Task	Related Topics
Step 13	Disable Cisco Real-time Information Server (RIS) Data Collector to minimize system problems and prevent false alerts.	"Disabling RIS Data Collector" section on page 2-4
Step 14	Before the upgrade, obtain the local Administrator account password, the SQL server SA password, the Private Password Phrase, and the computer name of the publisher database server.	"Information That You May Need During the Upgrade" section on page 2-5

Disabling RIS Data Collector

Before upgrading to Cisco CallManager Release 4.0 and above, Cisco recommends that the administrator disables the RIS Data Collector to minimize system problems and prevent false alerts. The following procedure describes how to disable the RIS Data Collector.

Procedure

Step 1 From Cisco CallManager Administration, choose **Service > Service Parameters**.

The Service Parameters Configuration window displays.

Step 2 From the Server pull-down menu, choose any server.

Step 3 From the Service pull-down menu, choose RIS Data Collector.

Step 4 In the Data Collection Enabled field, choose False.

Step 5 Click **Update**.

You can now perform the upgrade to Cisco CallManager 4.0 and above.

Note After you complete the Cisco CallManager upgrade, be sure to reset the parameter to "True" in the Data Collection Enabled field from the Service Parameters Configuration window to enable RIS data collection.

Information That You May Need During the Upgrade

Use the information in the following table when you perform the upgrade procedures.

Caution When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, enter alphanumeric characters only. The account password must match on every server in the cluster. For each of the accounts, you must enter the same password on every server in the cluster.

The upgrade prompts you for a Private Password Phrase. The upgrade uses the string that you enter to create a unique, encrypted password. You must enter the same phrase on all servers in the cluster.

Table 2-1 Information That You May Need During the Upgrade

Data	Your Entry
Destination where the backup file is stored during the backup	
WorkGroup Name	
Name of your organization	
Computer name of the publisher database server	
Local Administrator account password (same password for all servers in cluster)	
LDAP (DC) Directory Manager password (same password for all servers in cluster)	
SQL Server SA password (same password for all servers in cluster)	
Private Password Phrase for the cluster (same phrase for all servers in cluster)	

Upgrading the Cisco CallManager 3.2 Publisher Database Server

Perform the following upgrade tasks on the publisher database server if you do not need to replace server. To successfully migrate data and upgrade the publisher database server, you must perform all procedures exactly as stated in this section.

	Task	Important Information	Time It Takes To Perform Task
Step 1	Verify that you have performed all pre-upgrade tasks.	See the "Before You Begin" section on page 2-1 and the "Disabling RIS Data Collector" section on page 2-4.	Depends on the size of the cluster
Step 2	Remove all servers in the cluster from the NT Domain or Microsoft Active Directory Domain.	See the "Installing Cisco CallManager (Required)" section on page 2-23.	Depends on the size of the cluster
Step 3	Manually disable and stop all third-party, Cisco-verified, and Cisco-provided coresident applications that are installed on your server.	Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-approved McAfee services), intrusion detection (for example, Cisco Security Agent), and remote management services, ensures that the upgrade does not encounter issues that are associated with these services. See the "Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)" section on page 2-13.	20 minutes

	Task	Important Information	Time It Takes To Perform Task
Step 4	Manually remove versions of the Cisco IP Telephony Applications Backup.	Cisco recommends that you perform this task before you insert Cisco CallManager Backup Utility Disk. If the backup utility installation detects a previous version of the utility, verify that no backup utility exists under the Add/Remove Programs option in Microsoft Windows. Then, continue the installation, even if a error states that a previous version is detected. **Note** You cannot uninstall Cisco IP Telephony Applications Backup Utility version 3.5.6 if you installed the utility during the Cisco CallManager 3.2(3) installation. See the "Remove Previous Versions of the Cisco IP Telephony Applications Server Backup Utility (Required)" section on page 2-14.	5 minutes
Step 5	Manually install and configure Cisco IP Telephony Applications Server Backup, Version 3.5.53 (or later).	The Cisco CallManager Backup Utility Disk contains the utility that you must install. **About Backup Utility Configuration** When the installation software prompts you to configure the Cisco IP Telephony Applications Backup Utility, be aware that you must configure the publisher database server as the Backup Server, so data and configuration migration can occur. **About the Network Directory** If you choose a network directory as the destination for the backup server, the directory must be shared in Windows 2000. To share a directory, log in on that server, right-click the directory folder icon that you want to share, click **Sharing...**, click **Share this folder**, and then click **OK**. **About the Files That the Utility Backs Up** The Cisco IP Telephony Applications Backup Utility does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Using Cisco IP Telephony Applications Backup Utility, Version 3.5.52* (or later). To obtain the latest version of the document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm. For step-by-step instructions on how to install and configure the backup utility, see the "Install and Configure Cisco IP Telephony Applications Server Backup Utility, Version 3.5.53 or Later (Required)" section on page 2-15.	15 minutes

	Task	Important Information	Time It Takes To Perform Task
Step 6	Manually back up the data that is on the publisher database server to either a network directory or local tape drive.	Consider the following information before you back up the server: **About the Backup Utility Version** To back up the data, you must use Cisco IP Telephony Applications Backup Utility, Version 3.5.53 or later, with this release of Cisco CallManager. **About Data Deletion** Do not back up the data to a local directory; the operating system installation erases all data that is stored on the local directory. **About Temporary Disk Space** If the server does not have enough temporary disk space to complete the backup, the backup fails. **About Data Preservation** Only data that is contained on the publisher database server restores. For example, if Cisco Trivial File Transfer Protocol (TFTP) does not reside on the publisher database server, the restoration at the end of the upgrade erases all customized TFTP information, such as specific phone or gateway loads. If you want to retain this information, you must reconfigure the system, so the loads exist on the publisher database server, or you must manually save this data before the restoration. After the backup, verify that no errors exist. Failure to successfully troubleshoot any problems could cause a total loss of data. For step-by-step instructions on how to perform the backup, see the "Back Up Existing Data (Required)" section on page 2-17. **Tip** To significantly improve the speed of the Cisco CallManager upgrade, archive or remove CDRs before backing up your system.	30 to 60 minutes, depending on the size of the Cisco CallManager and Call Detail Record (CDR) database
Step 7	After you verify that the backup completed successfully, verify that the dbname.ini and backup.ini files exist. Copy the files to the network directory or tape device where the MCS.sti file is stored.	See the "Verify That the dbname.ini and backup.ini Files Exist for the STI_DATA Drive; Copy the Files to the Network Directory Where the MCS.sti File Exists (Strongly Recommended)" section on page 2-18.	5 minutes

	Task	Important Information	Time It Takes To Perform Task
Step 8	Run Cisco CallManager Upgrade Assistant 4.0(2) on all servers in the cluster. You must perform this task on one server in the cluster at a time, beginning with the publisher database server.	The Cisco CallManager Upgrade Assistant Utility verifies that your server is in a healthy state before the upgrade. Perform this task on one server in the cluster at a time, beginning with the publisher database server. See the "Run the Cisco CallManager Upgrade Assistant Utility on All Servers in the Cluster (Strongly Recommended)" section on page 2-19.	1 to 20 minutes per server
Step 9	If the server supports drive removal, remove a drive, insert a replacement drive, and mirror the drives.	See the "Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)" section on page 2-19.	15 to 60 minutes, depending on the server type

	Task	Important Information	Time It Takes To Perform Task
Step 10	Using the Cisco-provided operating system disks (Cisco IP Telephony Server Operating System Hardware Detection Disk and Cisco IP Telephony Server Operating System Installation and Recovery Disk), install operating system version 2000.2.4 or later. You must install Cisco-provided operating system 2000.2.4 or later via the Same Server Recovery method. If you are currently running Cisco-provided operating system version 2000.2.4 or later, you must install the operating system again by using same server recovery method with disks that ship with this version of Cisco CallManager. You cannot upgrade to Cisco-provided operating system version 2000.2.4 (or later) from a previous version of the operating system.	**About Removing Drives** After you verify that you have a good backup of data, you can remove a drive to save configured data; however, you must insert a replacement drive into the server before you begin the operating system procedures. Before you begin the operating system installation, make sure that you have all drives in the server and verify that the drives are functional. For example, insert two drives for the MCS-7835 and four drives for the MCS-7845. You must also remove additional hard drives from the server. Neglecting to perform these tasks causes failure of the Cisco CallManager installation and the loss of data/configuration settings from drive mirroring. **About Name Resolution** After installing the operating system and before installing Cisco CallManager, you must configure name resolution for the backup location. **About NT and Microsoft Active Directory Domains** Cisco requires that you remove and do not add any servers to the NT Domain or the Microsoft Active Directory Domain until you complete all installation procedures on all servers in the cluster. The installation fails if you do not perform this task. **About Data Recovery** Make sure that you choose **Same Server Recovery** during the operating system installation. Choosing this option ensures that the server retains the current network configuration data. **About Passwords** Make sure that you enter an Administrator password at the end of the operating system installation. If you leave the Administrator password blank, you cannot install Cisco CallManager on the server. Ensure that this password is the same on every server in the cluster. **About Operating System Service Releases** Cisco strongly recommends that you do not install any operating system service releases until you complete the upgrade on every server in the cluster. For step-by-step instructions on how to install the operating system, see the "Install the Operating System by Using Same Server Recovery (Required)" section on page 2-20.	45 to 75 minutes, depending on the server type

	Task	Important Information	Time It Takes To Perform Task
Step 11	Use Cisco IP Telephony Server Operating System OS/BIOS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.6 (or later).	Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml. For step-by-step instructions on upgrading the OS, see the "Upgrade the Operating System to Cisco-Provided Version 2000.2.6 (or Later) (Required)" section on page 2-22.	45 to 75 minutes, depending on the server type
Step 12	Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). (Required)	The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.	15 minutes, depending on the Internet connection
Step 13	Download and install the latest OS-related security hotfixes, if any. (Recommended)	The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. Refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.	5 minutes

	Task	Important Information	Time It Takes To Perform Task
Step 14	Use the Cisco CallManager Installation, Upgrade, and Recovery Disks to install Cisco CallManager. Microsoft SQL Server 2000, Microsoft SQL Server 2000 Service Pack 3a, and DC Directory automatically install when you install Cisco CallManager via the disks.	**About Configuring Name Resolution on the Backup Location** After installing the operating system installation and before installing Cisco CallManager, you must configure name resolution for the backup location. **About Data Restoration** The disks that you insert for the Cisco CallManager installation also restores the data that you backed up by using backup utility version 3.5.53 or later. The restoration retains all TCP/IP configuration settings, but you lose all NIC settings that you have manually configured; for example, hard-coded Speed/Duplex settings. You must manually configure these settings after you install all servers in the cluster. Only the data that is contained on the publisher database server restores to the destination that you specify. For example, if Cisco TFTP does not reside on the publisher database server, the restoration at the end of the upgrade erases all customized TFTP information, such as specific phone or gateway loads. If you want to retain this information, you must reconfigure the system, so the loads exist on the publisher database server, or you must manually save this data before the restoration. Be aware that the restoration launches automatically. During the restoration, if your location is a network directory, you must click the Browse button and manually highlight the MCS.sti file. Failure to highlight the file causes the upgrade to fail. **About Installed Services** All services that display in the Service Activation window of Cisco CallManager Serviceability install, but only the services that you configured prior to the upgrade activate after the upgrade completes and the server reboots. If you want to run additional services, you must activate the service on each server in which you want the service to run. You must perform this task by browsing into Cisco CallManager Serviceability from a PC that does not have Cisco CallManager installed. For more information on how to activate services and for service considerations, refer to the *Cisco CallManager Serviceability Administration Guide*. Cisco CallManager places services in an inactive state until the upgrade completes. For step-by-step instructions on installing Cisco CallManager, see the "Installing Cisco CallManager (Required)" section on page 2-23	Restoring the Data— up to 70 minutes, depending on the size of the Cisco CallManager and CDR database Installing Cisco CallManager —45 to 120 minutes per server depending on the size of the Cisco CallManager cluster.
Step 15	Upgrade the subscriber servers in the cluster.	See the "Upgrading Cisco CallManager 3.2 Subscriber Servers" procedure on page 2-26.	Depends on the size of the cluster.

Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)

Tip You can perform this task on all servers in the cluster at the same time.

The reboot causes call-processing interruptions if done at the same time.

Caution When a server exists in a domain during an upgrade, authentication between servers may fail, or the non-default domain security policies may restrict Cisco CallManager from building critical NT accounts. Failing to remove the system from the domain and add it to a work group may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Do not place the servers back into the domain until you have completed the upgrade procedures for every server in the cluster.

Convert any servers that exist in the NT Domain or Microsoft Active Directory Domain by performing the following procedure:

Procedure

Step 1 Choose **Start > Settings > Control Panel > System**.

Step 2 Click the **Network Identification** tab.

Step 3 Click the **Properties** button.

Step 4 Click the **Workgroup** radio button and enter a name, for example, WRKGRP, in the corresponding field.

Step 5 Click **OK**.

Step 6 When prompted to do so, reboot the server.

Step 7 Log in to the server by using the Administrator password.

Step 8 Perform this procedure on every server in the cluster that exists in the NT Domain.

Step 9 Go to the Domain Controller and remove the computer accounts for the Cisco CallManager servers in the cluster.

Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)

Tip You must perform this task on all servers in the cluster at the same time.

The reboot may cause call-processing interruptions.

To review a list of Cisco-verified applications that Cisco supports and that you should disable before the installation, click http://www.cisco.com/pcgi-bin/ecoa/Search. In the Solution pane, click **IP Telephony**. From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**. Click **Search**.

The following platform agents may interfere with the Cisco CallManager installation: antivirus services, intrusion detection services (for example, Cisco Security Agent), OEM server agents, server management agents, VOIP monitoring/performance monitoring, or remote access/remote management agents. Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-verified McAfee services), intrusion detection, and remote management services, ensures that you do not encounter issues that are associated with these services.

This document provides procedures for disabling Cisco-verified McAfee antivirus services only. If you need assistance with disabling other services or applications, refer to the corresponding documentation that accompanies the product.

To disable the McAfee antivirus services, perform the following tasks:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Services window, right-click one of the antivirus services; that is, Network Associates Alert Manager, Network Associates McShield, or Network Associates Task Manager, and choose **Properties**.

Step 3 In the Properties window, verify that the General tab displays.

Step 4 In the Service Status area, click **Stop**.

Step 5 From the Startup type drop-down list box, choose **Disabled**.

Step 6 Click **OK**.

Step 7 Perform Step 1 through Step 6 for all Cisco-approved McAfee antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, and Network Associates Task Manager.

Step 8 Reboot the server and verify that the services are not running.

Caution Make sure that the services do not start after the reboot.

Caution If Cisco-verified antivirus or intrusion detection software is not currently installed on the server, Cisco strongly recommends that you do not install the software until you complete the entire upgrade/installation of all servers in the cluster.

Remove Previous Versions of the Cisco IP Telephony Applications Server Backup Utility (Required)

Uninstall any previous versions of the Cisco IP Telephony Applications Backup Utility by performing the following procedure.

Note You cannot uninstall Cisco IP Telephony Applications Backup Utility version 3.5.6 if you installed the utility during the Cisco CallManager 3.2(3) installation.

Procedure

Step 1 Choose **Start > Settings > Control Panel**.

Step 2 Double-click **Add/Remove Programs**.

Step 3 Click **Cisco IP Telephony Applications Backup Utility**.

Step 4 Click **Remove**.

Step 5 Reboot the server and log in to the server by using the Administrator password.

Install and Configure Cisco IP Telephony Applications Server Backup Utility, Version 3.5.53 or Later (Required)

The Cisco IP Telephony Applications Backup Utility does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Using Cisco IP Telephony Applications Backup Utility, Version* 3.5.52 (or later). To obtain the latest version of the document, see http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Item Needed: Cisco CallManager Backup Utility Disk Or the Backup Utility That Is Available on the Web

Perform the following procedure to remove the existing backup utility, install the new backup utility, and configure the utility:

Procedure

Step 1 Decide if you are going to install the backup utility via disk or via the web.

Tip To install the backup utility from the web, refer to *Using Cisco IP Telephony Applications Backup Utility, Version 3.5.52* (or later) for more information on how to perform this task.

To install via disk, continue with Step 2.

Step 2 To install via disk, insert the Cisco CallManager Backup Utility disk into the drive.

Step 3 When the Upgrade Warning displays, read the information carefully before starting the upgrade.

Step 4 At the bottom of the window, click **Backup Utility**.

Step 5 Click the **Run the program from the current location** radio button and click **Next**.

Step 6 When a prompt asks you to install the utility, click **Yes**.

Step 7 If the software detects that a previous version of the backup utility exists on the server, click Yes to proceed.

Note Even if you uninstall the previous version of the backup utility, you may receive a message that the backup utility exists on the server. Continue the backup utility installation.

Step 8 When the Welcome window displays, click **Next**.

Step 9 Accept the terms of the license agreement by clicking the **I accept the terms in the license agreement** radio button and click **Next**.

Step 10 In the Backup Role window, perform the following procedure:

a. Click the **Backup Server** radio button.

b. Click **Next**.

Step 11 Enter the BackAdmin Private Password Phrase; enter the phrase again in the Confirm Password field. Click **Next**.

Step 12 Click the version of Cisco CallManager that is currently running in the cluster; then, click **Next**.

Step 13 In the Ready to Install the Program window, click **Install**.

The installation occurs, as indicated in the status bar. Do not click Cancel. Continue to wait while the installation completes.

Step 14 When the Backup Utility Configuration window displays, perform the following procedure:

a. With the CallManager tab open, verify that the publisher database server name displays in the CallManager Targets list. If the publisher database server name does not display, add it to the target list.

b. To test for Cisco CallManager components, click **Verify**.

c. When you receive the authentication results in the dialog box, click **OK**.

Caution If you have installed CDR Analysis and Reporting (CAR) on the publisher database server, verify that you have added the publisher database server name (not IP address) to the Cisco CallManager and Cisco CAR target lists. Use the same naming conventions in each list, so the restore utility can restore CAR during the Cisco CallManager database restoration.

Step 15 Click the **CER**, **CRA** (Cisco Customer Response Applications), or **CAR** (Cisco CDR Administrative and Reporting Tool) tab and repeat Step 14 to configure the backup for CER, CRA, or Cisco CAR.

Step 16 Click the **Destination** tab.

Step 17 Configure the destination, the location where the backup utility stores the data. Cisco allows you to choose only one Destination for all stored data.

To configure a network directory, see Step 18 through Step 21.

To configure a tape device, see Step 22 through Step 24.

Caution When you configure the destination, do not click the **Local Directory** radio button, or the operating system installation erases all existing data that is stored on the local directory.

To Configure a Network Directory

If you choose a network directory as the destination for the backup server, the directory must be shared in Windows 2000. To share a directory, log in on that server, right-click the directory folder icon that you want to share, click **Sharing...**, click **Share this folder**, and then click **OK**.

Step 18 Click **Network Directory**.

Step 19 Browse to the location of the directory and click the directory that you want to specify as the location.

Step 20 Enter a user name and password with administrative privileges and click **Verify**; then, click **OK**.

Step 21 In the lower, right corner of the window, click **OK**; then, go to Step 25.

To Configure a Tape Device

Step 22 Click **Tape Device**.

Step 23 From the drop-down list box, choose the device that you want to use.

Step 24 Click **OK**.

Step 25 When a prompt asks you to save the settings and exit, click **Yes**.

Step 26 When the installation completes, click **Finish**.

Step 27 To restart the server, click **Yes**.

Step 28 Log in to the server by using the local Administrator account and password.

Back Up Existing Data (Required)

Caution The Cisco IP Telephony Applications Backup Utility does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Using Cisco IP Telephony Applications Backup Utility, Version* 3.5.52 (or later). To obtain the latest version of the document, see http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

You must back up the publisher database before you install the operating system. Perform the following procedure:

Procedure

Step 1 Right-click the Cisco IP Telephony Applications Backup Utility icon in the Windows 2000 system tray and choose **Start backup now**.

Step 2 In the pane on the left side of the window, choose the publisher database server.

Step 3 Click **Start backup**.

Step 4 After the backup completes, verify that the backup completed successfully. The Backup Utility Viewer displays the status of the backup operation by highlighting each task as it occurs. Use the information that is generated in the log window to help identify problems. When the current status returns to "Waiting until <time> on <date>," the backup is complete. The last line in the log file indicates that the log is closed.

You can obtain the StiBack.log from C:\Program Files\Common Files\Cisco\Logs on the backup server. If you receive the following error messages or other error messages in the log file, the process did not successfully back up the data:

- Cisco CallManager database could not be found on <Server Name>.
- Could not determine APPS version
- Could not find a CCM/ART/CDR SQL database on <Server Name>

- Error finding SQL database
- Error enumerating registry keys on <Server Name>
- Open file request returned Not Enough Space

Step 5 After the backup completes and you verify that no errors occurred, remove the Cisco CallManager Backup Utility Disk from the drive.

Caution If you have not backed up coresident applications on the server, you will lose the data when you perform the operating system installation. Back up these applications now.

Verify That the dbname.ini and backup.ini Files Exist for the STI_DATA Drive; Copy the Files to the Network Directory Where the MCS.sti File Exists (Strongly Recommended)

Caution Cisco strongly recommends that you verify that the dbname.ini and backup.ini files exist on the publisher database server. Cisco IP Telephony Applications Backup Utility, Version 3.5.52 (or later), creates these files during the backup. If these files do not exist, you cannot restore the MCS.sti file.

The files exist in the Recovery directory on the STI_Data drive. Depending on the system, these files exist on the D: or E: drive. For example, the files may exist on the publisher database server in one of the following locations: D:\recover\<name of file> or E:\recover\<name of file>.

After you locate the files, Cisco recommends that you copy the files to the network directory where the MCS.sti file exists.

Run the Cisco CallManager Upgrade Assistant Utility on All Servers in the Cluster (Strongly Recommended)

Tip You must perform this task on one server in the cluster at a time, beginning with the publisher database server.

The reboot may cause call-processing interruptions.

Item Needed: Web Download of Utility

Run the Cisco CallManager Upgrade Assistant Utility to verify that your server is in a healthy state before the upgrade. The document that posts next to the utility on the web provides detailed information about the utility. To obtain the utility and the document, perform the following procedure:

Procedure

Step 1 Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 2 Click **Cisco CallManager Version 4.0**.

The Cisco CallManager 4.0 software page displays.

Step 3 Locate and download the document.

Step 4 Using the document as a reference, download and run the utility on every server in the cluster where Cisco CallManager is installed.

Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)

Item Needed: Newly Purchased Hard Drive

You cannot remove a drive if you have the MCS-7815, MCS-7820, MCS-7822, MCS-7825, or the customer-provided IBM xSeries 330 server.

After you verify that you have a good backup of the data, you can remove a drive to save configured data; however, you must insert a replacement drive into the server before you begin the operating system procedures. This task may require that you purchase a new drive.

This process may take between 30 minutes to 60 minutes, depending on the size of the drive.

Perform the following steps to remove a drive, to insert a replacement drive, and to mirror the drives:

Procedure

Step 1 Power off the publisher database server.

Step 2 For all servers except the MCS-7845, remove the hard drive from Slot 0 and label the drive with the machine name, slot number, and current version of Cisco CallManager.

For the MCS-7845, remove the drives from Slot 0 and Slot 2.

Step 3 Power on the system.

Cisco MCS

Step 4 Perform the following procedure for the Cisco MCS (The MCS-7845 requires two spare hard drives.):

a. To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845, press **F2**.

Note The MCS-7835H-2.4 (or later) and MCS-7845H-2.4 (or later) default to F2, and the process automatically continues after a 10-second delay.

b. This step applies only for the MCS-7830, MCS-7835, or MCS-7845.

When prompted, press **F1** to continue.

c. After Windows 2000 finishes booting, insert the replacement hard drive in Slot 0.

Note On the MCS-7845, do not insert the replacement drive into Slot 2 until the mirror process completes for the drive in Slot 0.

d. On the MCS-7830, MCS-7835, or MCS-7845, choose **Start > Compaq Systems Tools > Compaq Array Configuration Utility**. When the Array Configuration Utility Warning window opens, click **OK**.

e. Watch the status bar in the lower, right corner to determine when the mirroring process completes.

f. This step applies for the MCS-7845 only.

After the mirroring process completes in Slot 0, insert the next drive into Slot 2. The mirroring process launches automatically after you insert the drive into Slot 2.

IBM xSeries Server

Step 5 Perform the following procedure for the IBM xSeries server:

a. Insert a replacement drive into Slot 0.

b. Press **F5**.

c. Choose **Start > Programs > ServeRaid Manager > ServeRaid Manager**. You can view the progression of the drive mirroring.

Install the Operating System by Using Same Server Recovery (Required)

Item Needed: Cisco IP Telephony Server Operating System Hardware Detection Disk

Procedure

Step 1 Locate the Cisco IP Telephony Server Operating System Hardware Detection Disk.

Step 2 Insert the disk into the drive and then immediately restart the system. Do not press any keys during the reboot.

Step 3 When the Cisco IP Telephony Applications Server QuickBuilder welcome window opens, click **Next**.

Step 4 When the Type of Installation window opens, choose **Same Server Recovery**; then, click **Next**.

Step 5 A warning message states that the installation erases all data. Click **Next**.

Step 6 In the Ready to Install window, click **Next**.

Step 7 When the Server Configuration Wizard window displays, click **Next**.

Caution In the following configuration windows, Cisco CallManager automatically populates the data entry fields.

If the server does not belong to a Workgroup, join a Workgroup during this operating system installation. The Cisco CallManager installation requires joining a Workgroup.

Likewise, to successfully complete the upgrade, you must configure DNS or WINS, if you have not already done so.

Step 8 The user name and the name of your organization display in the appropriate fields. The computer name and DNS domain suffix display. Click **Next**.

Step 9 The Join Domain window displays whether the server is in a Workgroup or Domain. If the server exists in a Domain, Cisco requires that you place the server in a Workgroup. To join a Workgroup, perform the following procedure:

a. Enter a name of the Workgroup; for example, WRKGRP.

b. Click **Next**.

Step 10 From the drop-down box, choose the appropriate time zone. Reset the current date and time, if applicable; then, click **Next**.

Step 11 If you chose **Use the following IP address** during the original installation, the IP information for the server displays in the next window.

If your server was configured for Domain Name System (DNS) or Windows Internet Name Service (WINS), the IP addresses of the primary DNS and WINS servers display. If DNS or WINS was not configured, empty IP addresses fields display.

Click **Next**.

Step 12 If you configured your server with a static IP address and you did not configure DNS/WINS, you must update the lmhosts file, so it contains a mapping of the IP address and hostname of each server in the cluster. Perform the following steps to configure the lmhosts file:

a. In the LMHost window, check the **Check if you want to edit LMHosts file** check box.

b. Enter the IP Address and Server Name.

For example:

```
172.16.0.10 dallascm1
```

c. Click **Add Server**.

d. Click **Next** to continue.

Note The Windows 2000 SNMP agent provides security through the use of community names and authentication traps. All SNMP implementations universally accept the default name “public.” Cisco sets the community rights to none for security reasons. If you want to use SNMP with this server, you must configure it.

Step 13 To ensure security within the Windows 2000 SNMP agent, Cisco recommends that you change the default public community name. Enter a new name; then, click **Next**.

Step 14 The installation process automatically enables Terminal Services. If you want, you can disable these services; then, click **Next**.

Step 15 The disk drive automatically opens. Remove the hardware detection disk from the drive and insert the server-specific Cisco IP Telephony Server Operating System Installation and Recovery Disk into the drive. The configuration process continues automatically after detection of the appropriate disk. The server begins an installation and reboot process that takes about 10 minutes to complete.

Step 16 The disk drive automatically opens. Remove the operating system disk; if prompted, press any key to reboot. If you do not receive a prompt, the server reboots automatically.

Windows 2000 setup begins and takes about 10 minutes to complete. Do not power down the server or press any keys during setup.

Caution If you receive a message that the configuration file is not found, manually enter the information and continue the installation.

Step 17 When the dialog box displays, enter an administrative password in the Password field; enter the same password in the Confirm Password field and click **OK**.

If you leave the password fields blank, you cannot install any Cisco IP telephony applications on the server.

Tip Make sure that you enter the same password on all servers in the cluster.

Step 18 Log in to the server by using the local Administrator account and password.

Caution After performing the operating system installation and before installing Cisco CallManager, you must configure name resolution for the backup location.

Upgrade the Operating System to Cisco-Provided Version 2000.2.6 (or Later) (Required)

Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Perform the upgrade on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.

Cisco recommends that you upgrade to install Cisco IP Telephony operating system version 2000.2.6 with the latest service release 2000.2.6.sr1 (or later) before you upgrade to Cisco CallManager Release 4.0(2).

Download and Install the Latest Cisco IP Telephony Server Operating System Service Release (Required)

Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Download and Install the Latest OS-Related Security Hotfixes (If Any) (Recommended)

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Installing Cisco CallManager (Required)

Items Needed: Cisco CallManager Installation, Upgrade, and Recovery Disks 1 and 2

Perform the following procedure to install the directory, the database, and Cisco CallManager via disks. The disks also prompts you to restore the data that the backup utility stored to a network directory or tape device.

Caution You may not see any indication that the installation and restoration are progressing. Do not reboot the server unless the installation prompts you to do so. You may not see any activity for up to an hour, depending on the size of your system. Do not remove the disks during the installation process unless prompted to do so. The installation does not prompt you to remove the disk at the end of the installation, so verify that the installation is complete before you remove the disk.

Procedure

Step 1 After you complete the operating system installation, insert Cisco CallManager 4.0 Installation, Upgrade, and Recovery Disk 1 of 2 into the drive.

The installation process automatically starts.

To acknowledge that you disabled/uninstalled Cisco-verified applications, click **Yes**.

Note This extraction may take several minutes. Do not reboot.

Step 2 The following message displays: “The Same System Recovery flag was detected. Is this server being configured as a Cisco CallManager Publisher?” Click **Yes**.

Step 3 The Preparing to Install window displays. Do not click Cancel.

Step 4 In the Welcome window, click **Next**.

Step 5 Accept the terms of the license agreement by clicking the **I accept the terms in the license agreement** radio button and click **Next**.

Step 6 In the Customer Information window, the User Name and Organization that you entered during the operating system installation display.

Cisco automatically populates the product key fields with the product key that you entered during the operating system installation. Click **Next**.

Step 7 In the Setup Type window, ensure that the **Complete** radio button is chosen; then, click **Next**.

Step 8 In the Setup Type window, the **Publisher** radio button automatically gets selected and grayed out. Click **Next**.

Step 9 In the Administrator Password window, enter the Administrator password that you entered during the operating system installation.

Caution When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, enter alphanumeric characters only. The account password must match on every server in the cluster.

Step 10 Enter the Private Password Phrase for the cluster; confirm the private password phrase and click **Next**.

The private password phrase contains 1 to 15 characters. This phrase may contain English lowercase letters, English uppercase letters, Westernized Arabic numerals, and the following nonalphanumeric special characters: { } . < > : ? / | \ ` ~ ! @ $ ^ & * ( ) _ - +.

Step 11 In the SQL Password window, enter the SA (SQL Server system administrator) password. To confirm the password, enter the password again in the next field; then, click **Next**.

Step 12 In the Ready to Install the Program window, click **Install**.

The status bar indicates the progression of the installation. Continue to wait while the installation progresses.

Step 13 A message displays that indicates that you need to install the next upgrade disk. Insert the Cisco CallManager 4.0 Installation, Upgrade, and Recovery Disk 2 of 2 and click **OK**.

Microsoft SQL Server 2000, Microsoft SQL Server 2000 Service Pack 3a (or later), and DC Directory install. This process takes 15 to 20 minutes.

A message displays that indicates that you need to install the first upgrade disk again.

Step 14 Insert the Cisco CallManager 4.0 Installation, Upgrade, and Recovery Disk 1 of 2 and click **OK**.

Step 15 To reboot the server, click **Yes**. Do not remove the disk from the drive.

Step 16 Log in to the server by using the Administrator password.

Step 17 The Cisco CallManager installation automatically launches. Continue to wait while the Cisco CallManager installation completes.

Step 18 The Cisco IP Telephony Applications Restore Utility automatically launches the restoration of the Cisco CallManager data that you stored to a network directory or tape device.

Step 19 In Step 1 of the restore utility, perform the following procedure:

a. Choose the location of the data, the place where the data is stored.

   If you chose a network directory, you must browse to and manually highlight the MCS.sti file. Failure to highlight the file causes the upgrade to fail.

b. Enter a username and password with administrator access rights on the server and then click **Verify**.

c. When you receive the authentication results in the dialog box, click **OK**.

d. Click **Next**.

Step 20 In Step 2 of the restore utility, perform the following procedure:

a. Highlight the CallManager target, which is the server that you want to restore.

b. Make sure that the SA password remains blank; then, click **Verify**.

c. A dialog box shows that authentication occurred successfully. Click **OK**.

d. Click **Next** to continue.

Step 21 To accept that you will overwrite the target server and lose all existing data if you proceed, click **Yes**.

The utility restores the files to the server where you want the utility to send the files.

Step 22 The restoration log displays. Verify that no errors exist in the log. If the following error messages or other error messages display in the log file, the process did not successfully restore the data:

- Failed to drop CCM/ART/CDR database from <Server Name>
- Failed to restore DC Directory
- Failed to stop DC Directory service
- Failed to restart DC Directory service

Step 23 After you verify that no errors exist, click **OK**.

The Cisco CallManager installation takes approximately 45 to 90 minutes. Although you may see no indication that the installation is progressing, continue to wait while the installation completes.

Step 24 After the installation completes, click the **Finish** button.

Step 25 When a prompt asks you to reboot the server, click **Yes**.

Step 26 After you reboot the server, remove the disk from the drive.

Step 27 Log on to the server by using the Administrator password.

Step 28 Verify that your data and configuration restored to the server.

Step 29 If the publisher database server is the only server where you plan to install Cisco CallManager, see the "Performing Post-Upgrade Tasks" section on page 4-1.

If you have subscriber servers that you need to install, see the "Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)" section on page 2-26.

Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)

Tip You can perform this task on all servers in the cluster at the same time.

The reboot causes call-processing interruptions if done at the same time.

Caution When a server exists in a domain during an upgrade, authentication between servers may fail, or the non-default domain security policies may restrict Cisco CallManager from building critical NT accounts. Failing to remove the system from the domain and add it to a work group may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Do not place the servers back into the domain until you have completed the upgrade procedures for every server in the cluster.

Convert any servers that exist in the NT Domain or Microsoft Active Directory Domain by performing the following procedure:

Procedure

Step 1 Choose **Start > Settings > Control Panel > System**.

Step 2 Click the **Network Identification** tab.

Step 3 Click the **Properties** button.

Step 4 Click the **Workgroup** radio button and enter a name, for example, WRKGRP, in the corresponding field.

Step 5 Click **OK**.

Step 6 When prompted to do so, reboot the server.

Step 7 Log in to the server by using the Administrator password.

Step 8 Perform this procedure on every server in the cluster that exists in the NT Domain.

Step 9 Go to the Domain Controller and remove the computer accounts for the Cisco CallManager servers in the cluster.

Upgrading Cisco CallManager 3.2 Subscriber Servers

When you upgrade a subscriber server from Cisco CallManager 3.2 to 4.0(1), you will need to reimage the server. This involves reinstalling the operating system so that you have a fresh installation, and then installing the Cisco CallManager software.

To complete installation tasks on each subscriber server, you should allot 60 to 120 minutes, depending on the server type. Consider the time that it takes to perform pre-/post-upgrade tasks.

Perform the following tasks to upgrade the subscriber database servers.

	Task	Important Information and Resources
Step 1	Verify that you have performed all pre-upgrade tasks.	See the "Before You Begin" section on page 2-1.
Step 2	Verify that you have removed all servers from the NT or Microsoft Active Directory Domain.	See the "Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)" section on page 2-26.
Step 3	Verify that you have disabled and stopped all third-party, Cisco-verified, and Cisco-provided coresident applications that run on the server. Make sure that you have rebooted the server.	See the "Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)" section on page 2-28.
Step 4	Run the ServPrep utility.	See the "Run the ServPrep Utility (Required)" section on page 2-29.
Step 5	Using the Cisco-provided operating system disk, install Cisco-provided operating system 2000.2.4 (or later).	If you are currently running Cisco-provided operating system version 2000.2.4 or later, you must install the operating system again using same server recovery method with disks that ship with this version of Cisco CallManager. You cannot upgrade to Cisco-provided operating system version 2000.2.4 from a previous version of the operating system. See the "Install the Operating System by Using Same Server Recovery (Required)" section on page 2-30. Consider the same guidelines for the subscriber servers that you used for the publisher database server.
Step 6	Use Cisco IP Telephony Server Operating System OS/BIOS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.6 (or later).	Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.
Step 7	Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1or later). (Required)	The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

	Task	Important Information and Resources
Step 8	Download and install the latest OS-related security hotfixes, if any. (Recommended)	The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.
Step 9	**Task That You Perform Serially** Perform the Cisco CallManager installation on one server at a time.	See the "Installing Cisco CallManager on Subscriber Database Server(s)" section on page 2-33. **Caution** You must perform the Cisco CallManager installation serially; that is, on one server at a time. After you reboot the server and after you verify that the server pulled the subscription from the publisher database server, you can begin the upgrade on the next server.
Step 10	After you complete the installation on all servers in the cluster, perform post-upgrade tasks.	See the "Performing Post-Upgrade Tasks" section on page 4-1.

Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)

Tip You must perform this task on all servers in the cluster at the same time.

The reboot may cause call-processing interruptions.

To review a list of Cisco-verified applications that Cisco supports and that you should disable before the installation, click http://www.cisco.com/pcgi-bin/ecoa/Search. In the Solution pane, click **IP Telephony**. From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**. Click **Search**.

The following platform agents may interfere with the Cisco CallManager installation: antivirus services, intrusion detection services (for example, Cisco Security Agent), OEM server agents, server management agents, VOIP monitoring/performance monitoring, or remote access/remote management agents. Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-verified McAfee services), intrusion detection, and remote management services, ensures that you do not encounter issues that are associated with these services.

This document provides procedures for disabling Cisco-verified McAfee antivirus services only. If you need assistance with disabling other services or applications, refer to the corresponding documentation that accompanies the product.

To disable the McAfee antivirus services, perform the following tasks:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Services window, right-click one of the antivirus services; that is, Network Associates Alert Manager, Network Associates McShield, or Network Associates Task Manager, and choose **Properties**.

Step 3 In the Properties window, verify that the General tab displays.

Step 4 In the Service Status area, click **Stop**.

Step 5 From the Startup type drop-down list box, choose **Disabled**.

Step 6 Click **OK**.

Step 7 Perform Step 1 through Step 6 for all Cisco-approved McAfee antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, and Network Associates Task Manager.

Step 8 Reboot the server and verify that the services are not running.

Caution Make sure that the services do not start after the reboot.

Caution If Cisco-verified antivirus or intrusion detection software is not currently installed on the server, Cisco strongly recommends that you do not install the software until you complete the entire upgrade/installation of all servers in the cluster.

Run the ServPrep Utility (Required)

Item Needed: Cisco CallManager Subscriber Upgrade Disk 1

Before you install Cisco CallManager, you must run the ServPrep utility and install Cisco IP Telephony Operating System by using the Cisco-provided operating system disks and upgrade to the latest operating sytem 2000.2.6sr1 (or later).

The ServPrep utility, which you run on subscriber servers, updates the network configuration by creating the file, STISys.inf, which contains network information. The utility saves TCP/IP settings, but you lose manually configured NIC settings; for example, hard-coded Speed/Duplex settings. After you complete the installation on all servers in the cluster, you must manually configure previous NIC settings.

Caution This utility supports all Cisco Media Convergence Servers, customer-provided HP DL320 and DL380 servers, and customer-provided IBM xSeries 330, 340, 342, and 345 servers that meet Cisco-approved configuration standards. Do not run this utility on any other servers, including customer-provided servers.

Procedure

Step 1 Insert the Cisco CallManager Subscriber Upgrade Disk 1 into the drive as soon as you can do so.

Step 2 When the Upgrade Warning window displays, carefully read the information and click the **ServPrep Utility** link at the bottom of the window.

Step 3 Run the program from the current location; follow the prompts that display.

Install the Operating System by Using Same Server Recovery (Required)

Item Needed: Cisco IP Telephony Server Operating System Hardware Detection Disk

Procedure

Step 1 Locate the Cisco IP Telephony Server Operating System Hardware Detection Disk.

Step 2 Insert the disk into the drive and then immediately restart the system. Do not press any keys during the reboot.

Step 3 When the Cisco IP Telephony Applications Server QuickBuilder welcome window opens, click **Next**.

Step 4 When the Type of Installation window opens, choose **Same Server Recovery**; then, click **Next**.

Step 5 A warning message states that the installation erases all data. Click **Next**.

Step 6 In the Ready to Install window, click **Next**.

Step 7 When the Server Configuration Wizard window displays, click **Next**.

Caution In the following configuration windows, Cisco CallManager automatically populates the data entry fields.

If the server does not belong to a Workgroup, join a Workgroup during this operating system installation. The Cisco CallManager installation requires joining a Workgroup.

Likewise, to successfully complete the upgrade, you must configure DNS or WINS, if you have not already done so.

Step 8 The user name and the name of your organization display in the appropriate fields. The computer name and DNS domain suffix display. Click **Next**.

Step 9 The Join Domain window displays whether the server is in a Workgroup or Domain. If the server exists in a Domain, Cisco requires that you place the server in a Workgroup. To join a Workgroup, perform the following procedure:

a. Enter a name of the Workgroup; for example, WRKGRP.

b. Click **Next**.

Step 10 From the drop-down box, choose the appropriate time zone. Reset the current date and time, if applicable; then, click **Next**.

Step 11 If you chose **Use the following IP address** during the original installation, the IP information for the server displays in the next window.

If your server was configured for Domain Name System (DNS) or Windows Internet Name Service (WINS), the IP addresses of the primary DNS and WINS servers display. If DNS or WINS was not configured, empty IP addresses fields display.

Click **Next**.

Step 12 If you configured your server with a static IP address and you did not configure DNS/WINS, you must update the lmhosts file, so it contains a mapping of the IP address and hostname of each server in the cluster. Perform the following steps to configure the lmhosts file:

a. In the LMHost window, check the **Check if you want to edit LMHosts file** check box.

b. Enter the IP Address and Server Name.

For example:

```
172.16.0.10 dallascm1
```

c. Click **Add Server**.

d. Click **Next** to continue.

Note The Windows 2000 SNMP agent provides security through the use of community names and authentication traps. All SNMP implementations universally accept the default name “public.” Cisco sets the community rights to none for security reasons. If you want to use SNMP with this server, you must configure it.

Step 13 To ensure security within the Windows 2000 SNMP agent, Cisco recommends that you change the default public community name. Enter a new name; then, click **Next**.

Step 14 The installation process automatically enables Terminal Services. If you want, you can disable these services; then, click **Next**.

Step 15 The disk drive automatically opens. Remove the hardware detection disk from the drive and insert the server-specific Cisco IP Telephony Server Operating System Installation and Recovery Disk into the drive. The configuration process continues automatically after detection of the appropriate disk. The server begins an installation and reboot process that takes about 10 minutes to complete.

Step 16 The disk drive automatically opens. Remove the operating system disk; if prompted, press any key to reboot. If you do not receive a prompt, the server reboots automatically.

Windows 2000 setup begins and takes about 10 minutes to complete. Do not power down the server or press any keys during setup.

Caution If you receive a message that the configuration file is not found, manually enter the information and continue the installation.

Step 17 When the dialog box displays, enter an administrative password in the Password field; enter the same password in the Confirm Password field and click **OK**.

If you leave the password fields blank, you cannot install any Cisco IP telephony applications on the server.

Tip Make sure that you enter the same password on all servers in the cluster.

Step 18 Log in to the server by using the local Administrator account and password.

Caution After performing the operating system installation and before installing Cisco CallManager, you must configure name resolution for the backup location.

Upgrade the Operating System to Cisco-Provided Version 2000.2.6 (or Later) (Required)

Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Perform the upgrade on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.

Cisco recommends that you upgrade to install Cisco IP Telephony operating system version 2000.2.6 with the latest service release 2000.2.6.sr1 (or later) before you upgrade to Cisco CallManager Release 4.0(2).

Download and Install the Latest Cisco IP Telephony Server Operating System Service Release (Required)

Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Download and Install the Latest OS-Related Security Hotfixes (If Any) (Recommended)

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Installing Cisco CallManager on Subscriber Database Server(s)

Item Needed: Cisco CallManager Installation, Upgrade, and Recovery Disks 1 and 2

After you install Cisco CallManager on the publisher database server, you install the application on the subscriber database servers. For each subscriber database server, the installation takes 45 to 90 minutes, depending on the server type.

Caution Perform the installation on one server at a time. This process ensures that the subscriber server(s) can receive a copy of the database from the publisher database server.

Caution The installation procedure prompts you to remove the Cisco CallManager Installation, Upgrade, and Recovery Disks. Do not remove the disk unless the installation procedure directs you to do so.

Procedure

Step 1 After you install the operating system and log in to the server by using the Administrator account and password, obtain the Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 and insert it into the drive.

Step 2 To acknowledge that you disabled/uninstalled all Cisco-verified applications, click **Yes**.

Step 3 The Preparing to Install window displays while the installation program copies files to your server. This process takes approximately 10 minutes. Do not click Cancel.

Step 4 When the Welcome window displays, click **Next**.

Step 5 Accept the Cisco CallManager license agreement by clicking the **I accept the terms in the license agreement** radio button; then, click **Next**.

Step 6 In the Customer Information window, the User Name and Organization that you entered during the operating system installation automatically display.

Cisco automatically populates the product key fields with the product key that you entered during the operating system installation. Click **Next**.

Note The publisher database server functions as the master database for all servers in the cluster. All servers except the publishing database server maintain subscriber databases, which are copies of the publisher database server. If you are configuring a subscriber database server, make sure that the server that you are installing can connect to the publishing database server, so the installation can continue. The installation process necessitates this connection, so the publisher database server can be copied to the local drive on the subscriber server. To make sure that a good connection exists between the servers, issue a ping command from the subscriber server to the publisher database server before you try to authenticate to it. If the ping command is not successful, you can also try to access the publisher database server from all subscriber servers by choosing **Start > Run**, entering \\<**Publisher Server Name**>**\C$**, and then by clicking **OK**. If the publisher database server cannot access the subscriber server, you must exit the installation program, fix the problem, and begin the installation process again on the subscriber server.

Step 7 Ensure that the **Complete** radio button is chosen.

Step 8 In the Server Type window, perform the following procedure:

a. Click the **Subscriber** radio button.

b. Enter the computer name of the publisher database server.

Caution If you enter the IP address or fully qualified DNS of the publisher database server, the installation fails.

c. Click **Next**.

Caution When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, enter alphanumeric characters only. The account password must match on every server in the cluster.

Step 9 In the Administrator password window, enter the local Windows administrator password.

This password must match the Windows administrator password that is used on the publisher database server.

Click **Next**.

Step 10 Enter the Private Password Phrase for the cluster; confirm the private password phrase and click **Next**.

The private password phrase contains 1 to 15 characters. This phrase may contain English lowercase letters, English uppercase letters, Westernized Arabic numerals, and the following nonalphanumeric special characters: { } . < > : ? / | \ ` ~ ! @ $ ^ & * ( ) _ - +.

This password must match the Private Password Phrase that you entered on the publisher database server.

Step 11 In the SQL Password window, perform the following procedure:

a. Enter the SA (SQL Server system administrator) password.

This password must match the SA password that you entered on the publisher database server.

b. Press the **Tab** key.

c. To confirm the password, enter the password again; then, click **Next**.

Step 12 Now that the Cisco CallManager and other included software are ready to be installed, click **Install**. This part of the installation takes about 30 to 45 minutes, depending on your server type.

Continue to wait while the installation progresses.

Step 13 A message displays indicating that you need to insert the next upgrade disk. Insert Cisco CallManager 4.0(2) Installation, Upgrade, and Recovery Disk 2 and click **OK**.

A message displays indicating that you need to install the first upgrade disk again.

Step 14 Insert the Cisco CallManager 4.0 Installation, Upgrade, and Recovery Disk 1 of 2 and click **OK**.

Step 15 When the Cisco CallManager installation completes, click **Finish** to exit the wizard.

Step 16 To restart the server, click **Yes**.

Step 17 After the server reboots, remove the disk from the drive.

Step 18 Log in by using the Administrator account and password.

Tip Repeat the procedures in the "Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)" section on page 2-26 on each subscriber server until you have upgraded all of the servers in your cluster. After you update all the servers, perform the appropriate procedures in the "Performing Post-Upgrade Tasks" section on page 4-1.

CHAPTER 3

Upgrading from Cisco CallManager 3.3 or Cisco CallManager 4.0(1) (If You Are Not Replacing Hardware)

You must upgrade Cisco CallManager on the publisher database server and all subscriber servers in the cluster. For the order of the upgrade, see the "Which server in the cluster do I upgrade first?" section on page 1-4.

Note If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.0(2) software kit.

If you are upgrading from Cisco CallManager 4.0(1), you can upgrade by using the disks from the Cisco CallManager 4.0(2) software kit or by using the web download file.

Before You Begin

Before you start the upgrade, make sure that you perform the following tasks:

	Pre-Upgrade Task	Related Topics
Step 1	Make sure that you run a recommended version of Cisco CallManager on all servers in the cluster.	From which versions of Cisco CallManager can I upgrade to Cisco CallManager Release 4.0(2)?, page 1-2
Step 2	Make sure that you understand the order in which you must upgrade the cluster.	Which server in the cluster do I upgrade first?, page 1-4 How does a coresident upgrade work if I have CRS installed with Cisco CallManager?, page 1-5

	Pre-Upgrade Task	Related Topics
Step 3	In Cisco CallManager Administration, make sure that you only add each server once on the Server Configuration window (**System > Server**). If you add a server using the host name and add the same server using the IP address, Cisco CallManager cannot accurately determine component versions for the server after a Cisco CallManager upgrade. If you have two entries in Cisco CallManager Administration for the same server, delete one of the entries before you upgrade.	Refer to the *Cisco CallManager Administration Guide*.
Step 4	Make sure that your server configuration supports this upgrade.	Which servers and operating system versions does Cisco support for this upgrade?, page 1-3
Step 5	Make sure you have enough available disk space on each of your servers for the Cisco CallManager upgrade. If you use the Cisco CallManager disks to upgrade, you need 2.0gigabytes of disk space. If you use the web file to upgrade, you need 3.0 gigabytes of disk space.	
Step 6	If you run Cisco CallManager Extension Mobility and Cisco CallManager 3.2 before the upgrade, you must perform additional configuration tasks after the upgrade, so Cisco CallManager Extension Mobility runs as expected.	For more information, refer to the Cisco CallManager Extension Mobility upgrade section of the *Cisco CallManager Features and Services Guide for 4.0(1)*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
Step 7	If you are using Cisco Unity as your voice-messaging system, configure the voice mail ports in Cisco CallManager to ensure proper migration.	For more information, refer to the *Release Notes for Cisco CallManager*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
Step 8	You must assign a unique device name to each H.323 intercluster trunk. A registration problem occurs when multiple Cisco CallManager clusters have the same device name assigned to H.323 intercluster trunks in Cisco CallManager Administration.	Refer to the *Cisco CallManager Administration Guide* for information on the trunk configuration procedure.
Step 9	Verify that all H.323 dial-peer(s) point to a Cisco CallManager server in the device profile for which they are assigned. Cisco no longer provides the Run H.225D On Every Node option in Cisco CallManager Administration for H.323 gateways. If the session target statements in the dial-peer(s) do not point to the appropriate Cisco CallManager server, calls fail.	Refer to the *Cisco CallManager Administration Guide* for information on the gateway configuration procedure.

	Pre-Upgrade Task	Related Topics
Step 10	Perform the recommended backup procedures for all coresident software applications that are installed on the server. **Caution** Failing to complete a backup causes a loss of data and configuration settings. For information on performing the backup, refer to the documentation that supports the applications. The Cisco IP Telephony Backup and Restore System (BARS) does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.	How does a coresident upgrade work if I have CRS installed with Cisco CallManager?, page 1-5
Step 11	Be aware that if you change any security or account policies from the default, the upgrade may fail.	For more information on security and account policies, refer to Microsoft documentation.
Step 12	Understand how Cisco CallManager updates service parameters. **For Service Parameters with Nonnumeric Values** Cisco CallManager always updates service parameters with nonnumeric values to the suggested value. **For Service Parameters with Numeric Values** If your service parameters are set to the suggested value, Cisco CallManager automatically updates the value during the upgrade to match the new suggested value. If your customized value exists between the range of minimum and maximum values, Cisco CallManager does not change the customized value. If you configured customized values that are not between the minimum and maximum range of values, the customized value changes during the upgrade to the maximum or minimum value. For example, if the maximum value equals 10 and the value that you configured is 12, Cisco CallManager automatically sets the value to 10. During the upgrade, some non-servicewide parameters may change to clusterwide parameters (formerly known as servicewide parameters).	For more information on service parameters, refer to the *Cisco CallManager Administration Guide* and the *Cisco CallManager System Guide*.

	Pre-Upgrade Task	Related Topics
Step 13	Disable Cisco Real-time Information Server (RIS) Data Collector to minimize system problems and prevent false alerts.	"Disabling RIS Data Collector" section on page 3-4
Step 14	Before the upgrade, obtain the local Administrator account password, the SQL server SA password, the Private Password Phrase, and the computer name of the publisher database server.	Information That You May Need During the Upgrade, page 3-5

Disabling RIS Data Collector

Before upgrading to Cisco CallManager Release 4.0 and above, Cisco recommends that the administrator disables the RIS Data Collector to minimize system problems and prevent false alerts. The following procedure describes how to disable the RIS Data Collector.

Procedure

Step 1 From Cisco CallManager Administration, choose **Service > Service Parameters**.

The Service Parameters Configuration window displays.

Step 2 From the Server pull-down menu, choose any server.

Step 3 From the Service pull-down menu, choose RIS Data Collector.

Step 4 In the Data Collection Enabled field, choose False.

Step 5 Click **Update**.

You can now perform the upgrade to Cisco CallManager 4.0(2) and above.

Note After you complete the Cisco CallManager upgrade, be sure to reset the parameter to "True" in the Data Collection Enabled field from the Service Parameters Configuration window to enable RIS data collection.

Information That You May Need During the Upgrade

Use the information in the following table when you perform the upgrade procedures.

Caution When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, enter alphanumeric characters only. The account password must match on every server in the cluster. For each of the accounts, you must enter the same password on every server in the cluster.

The upgrade prompts you for a Private Password Phrase. The upgrade uses the string that you enter to create a unique, encrypted password. You must enter the same phrase on all servers in the cluster.

Table 3-1 Information That You May Need During the Upgrade

Data	Your Entry
Destination where the backup file is stored during the backup	
WorkGroup Name	
Name of your organization	
Computer name of the publisher database server	
Local Administrator account password (same password for all servers in cluster)	
LDAP (DC) Directory Manager password (same password for all servers in cluster)	
SQL Server SA password (same password for all servers in cluster)	
Private Password Phrase for the cluster (same phrase for all servers in cluster)	

Upgrading the Cisco CallManager 3.3 or Cisco CallManager 4.0(1) Publisher Database Server

Review the following upgrade tasks, designated time to perform the task, and the location where you obtain the procedure:

	Task	Procedure	Designated Time
Step 1	Verify that you have performed all pre-upgrade tasks.	See the "Before You Begin" section on page 3-1 and the"Information That You May Need During the Upgrade" section on page 3-5.	Depends on the size of the cluster
Step 2	Remove all servers in the cluster from the NT Domain or the Microsoft Active Directory Domain.	See the "Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)" section on page 3-8. **Tip** You can perform this task on all servers in the cluster at the same time.	Depends on the size of the cluster
Step 3	Manually disable and stop all platform agents, Cisco-verified applications (Cisco AVVID Partner Applications), Cisco-provided coresident applications that run on the servers in the cluster. Reboot the server.	Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-approved McAfee services), intrusion detection (for example, Cisco Security Agent), and remote management services, ensures that the upgrade does not encounter issues that are associated with these services. See the "Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)" section on page 3-9. **Tip** You can perform this task on all servers in the cluster at the same time.	20 minutes
Step 4	Manually install and configure the CIPT Backup and Restore System (BARS), version 4.0(2) (or later).	If you have not already done so, Cisco recommends that you install and configure the backup utility on the publisher database server. The CIPT Backup and Restore System (BARS) does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.	15 minutes

	Task	Procedure	Designated Time
Step 5	Using the Backup and Restore System (BARS), version 4.0(2) (or later), manually back up the Cisco CallManager data to either a network directory or tape drive.	For information on backing up your system, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm. **Tip** To significantly improve the speed of the Cisco CallManager upgrade, archive or remove CDRs before backing up your system.	30 to 60 minutes, depending on the size of the Cisco CallManager and Call Detail Record (CDR) database
Step 6	Run the Cisco CallManager Upgrade Assistant Utility 4.0(2) on all servers in the cluster. You must perform this task on one server in the cluster at a time, beginning with the publisher database server.	The Cisco CallManager Upgrade Assistant Utility verifies that your server is in a healthy state before the upgrade. Perform this task on one server in the cluster at a time, beginning with the publisher database server. See the "Run the Cisco CallManager Upgrade Assistant Utility on All Servers in the Cluster (Strongly Recommended)" section on page 3-11.	1 to 20 minutes for the publisher database server; 1 to 5 minutes for the subscriber server
Step 7	If the server supports drive removal, remove a drive from the server to save your data and configuration.	See the "Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)" section on page 3-11.	15 to 60 minutes, depending on the server type
Step 8	Use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to Cisco-provided version 2000.2.6 (or later).	Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml. Perform the upgrade on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.	45 to 75 minutes per server, depending on the server type
Step 9	Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). (Required)	The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.	15 minutes

	Task	Procedure	Designated Time
Step 10	Download and install the latest OS-related security hotfixes, if any. (Recommended)	The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.	5 minutes
Step 11	Verify that you installed Microsoft SQL Server 2000, Service Pack 3a (or later).	For information on how to verify and install the service pack, refer to the readme documentation that accompanies the service pack. **Tip** Install this service pack on the publisher database server; complete the Cisco CallManager upgrade on the publisher database server before you install this service pack on the subscriber servers.	20 minutes
Step 12	Upgrade Cisco CallManager.	If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.0(2) software kit. If you are upgrading from Cisco CallManager 4.0(1), you can upgrade by using the disks from the Cisco CallManager 4.0(2) software kit or by using the web download file. **Caution** You must perform the Cisco CallManager installation serially; that is, on one server at a time. After you reboot the server and after you verify that the server pulled the subscription from the publisher database server, you can begin the upgrade on the next server. See the "Inserting the Disk or Downloading the Web File" section on page 3-13.	45 to 120 minutes per server, depending on the server type and the size of the Cisco CallManager cluster
Step 13	Upgrade all of the subscriber servers in the cluster.	See the "Upgrading the Cisco CallManager Subscriber Server(s)" procedure on page 3-16.	Depends on the size of the cluster.

Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)

Tip You can perform this task on all servers in the cluster at the same time.

The reboot causes call-processing interruptions if done at the same time.

Caution When a server exists in a domain during an upgrade, authentication between servers may fail, or the non-default domain security policies may restrict Cisco CallManager from building critical NT accounts. Failing to remove the system from the domain and add it to a work group may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Do not place the servers back into the domain until you have completed the upgrade procedures for every server in the cluster.

Convert any servers that exist in the NT Domain or Microsoft Active Directory Domain by performing the following procedure:

Procedure

Step 1 Choose **Start > Settings > Control Panel > System**.

Step 2 Click the **Network Identification** tab.

Step 3 Click the **Properties** button.

Step 4 Click the **Workgroup** radio button and enter a name, for example, WRKGRP, in the corresponding field.

Step 5 Click **OK**.

Step 6 When prompted to do so, reboot the server.

Step 7 Log in to the server by using the Administrator password.

Step 8 Perform this procedure on every server in the cluster that exists in the NT Domain.

Step 9 Go to the Domain Controller and remove the computer accounts for the Cisco CallManager servers in the cluster.

Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)

Tip You must perform this task on all servers in the cluster at the same time.

The reboot may cause call-processing interruptions.

To review a list of Cisco-verified applications that Cisco supports and that you should disable before the installation, click http://www.cisco.com/pcgi-bin/ecoa/Search. In the Solution pane, click **IP Telephony**. From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**. Click **Search**.

The following platform agents may interfere with the Cisco CallManager installation: antivirus services, intrusion detection services (for example, Cisco Security Agent), OEM server agents, server management agents, VOIP monitoring/performance monitoring, or remote access/remote management agents. Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-verified McAfee services), intrusion detection, and remote management services, ensures that you do not encounter issues that are associated with these services.

This document provides procedures for disabling Cisco-verified McAfee antivirus services only. If you need assistance with disabling other services or applications, refer to the corresponding documentation that accompanies the product.

To disable the McAfee antivirus services, perform the following tasks:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Services window, right-click one of the antivirus services; that is, Network Associates Alert Manager, Network Associates McShield, or Network Associates Task Manager, and choose **Properties**.

Step 3 In the Properties window, verify that the General tab displays.

Step 4 In the Service Status area, click **Stop**.

Step 5 From the Startup type drop-down list box, choose **Disabled**.

Step 6 Click **OK**.

Step 7 Perform Step 1 through Step 6 for all Cisco-approved McAfee antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, and Network Associates Task Manager.

Step 8 Reboot the server and verify that the services are not running.

Caution Make sure that the services do not start after the reboot.

Caution If Cisco-verified antivirus or intrusion detection software is not currently installed on the server, Cisco strongly recommends that you do not install the software until you complete the entire upgrade/installation of all servers in the cluster.

Install and Configure CIPT Backup and Restore (BARS) Version 4.0(2) (or Later) (Strongly Recommended)

If you have not already done so, Cisco recommends that you install and configure the backup utility on the publisher database server. The CIPT Backup and Restore System (BARS) does not back up any operating system files except for Host/LMhost, if these files exist on the server.

For a list of files that the utility backs up, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Back Up Existing Data (Strongly Recommended)

For information on backing up your system, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Run the Cisco CallManager Upgrade Assistant Utility on All Servers in the Cluster (Strongly Recommended)

Tip You must perform this task on one server in the cluster at a time, beginning with the publisher database server.

The reboot may cause call-processing interruptions.

Item Needed: Web Download of Utility

Run the Cisco CallManager Upgrade Assistant Utility to verify that your server is in a healthy state before the upgrade. The document that posts next to the utility on the web provides detailed information about the utility. To obtain the utility and the document, perform the following procedure:

Procedure

Step 1 Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 2 Click **Cisco CallManager Version 4.0**.

The Cisco CallManager 4.0 software page displays.

Step 3 Locate and download the document.

Step 4 Using the document as a reference, download and run the utility on every server in the cluster where Cisco CallManager is installed.

Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)

Item Needed: Newly Purchased Hard Drive

You cannot remove a drive if you have the MCS-7815, MCS-7820, MCS-7822, MCS-7825, or the customer-provided IBM xSeries 330 server.

After you verify that you have a good backup of the data, you can remove a drive to save configured data; however, you must insert a replacement drive into the server before you begin the operating system procedures. This task may require that you purchase a new drive.

This process may take between 30 minutes to 60 minutes, depending on the size of the drive.

Perform the following steps to remove a drive, to insert a replacement drive, and to mirror the drives:

Procedure

Step 1 Power off the publisher database server.

Step 2 For all servers except the MCS-7845, remove the hard drive from Slot 0 and label the drive with the machine name, slot number, and current version of Cisco CallManager.

For the MCS-7845, remove the drives from Slot 0 and Slot 2.

Step 3 Power on the system.

Cisco MCS

Step 4 Perform the following procedure for the Cisco MCS (The MCS-7845 requires two spare hard drives.):

a. To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845, press **F2**.

Note The MCS-7835H-2.4 (or later) and MCS-7845H-2.4 (or later) default to F2, and the process automatically continues after a 10-second delay.

b. This step applies only for the MCS-7830, MCS-7835, or MCS-7845.

When prompted, press **F1** to continue.

c. After Windows 2000 finishes booting, insert the replacement hard drive in Slot 0.

Note On the MCS-7845, do not insert the replacement drive into Slot 2 until the mirror process completes for the drive in Slot 0.

d. On the MCS-7830, MCS-7835, or MCS-7845, choose **Start > Compaq Systems Tools > Compaq Array Configuration Utility**. When the Array Configuration Utility Warning window opens, click **OK**.

e. Watch the status bar in the lower, right corner to determine when the mirroring process completes.

f. This step applies for the MCS-7845 only.

After the mirroring process completes in Slot 0, insert the next drive into Slot 2. The mirroring process launches automatically after you insert the drive into Slot 2.

IBM xSeries Server

Step 5 Perform the following procedure for the IBM xSeries server:

a. Insert a replacement drive into Slot 0.

b. Press **F5**.

c. Choose **Start > Programs > ServeRaid Manager > ServeRaid Manager**. You can view the progression of the drive mirroring.

Upgrade the Operating System to Cisco-Provided Version 2000.2.6 (or Later) (Required)

Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Perform the upgrade on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.

Cisco recommends that you upgrade to install Cisco IP Telephony operating system version 2000.2.6 with the latest service release 2000.2.6.sr1 (or later) before you upgrade to Cisco CallManager Release 4.0(2).

Download and Install the Latest Cisco IP Telephony Server Operating System Service Release (Required)

Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Download and Install the Latest OS-Related Security Hotfixes (If Any) (Recommended)

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Install Microsoft SQL Server 2000, Service Pack 3a (Required)

For information on how to verify and install the service pack, refer to the readme documentation that accompanies the service pack.

Tip Install this service pack on the publisher database server; complete the Cisco CallManager upgrade on the publisher database server before you install this service pack on the subscriber servers.

Inserting the Disk or Downloading the Web File

Note If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.0(2) software kit.

If you are upgrading from Cisco CallManager 4.0(1), you can upgrade by using the disks from the Cisco CallManager 4.0(2) software kit or by using the web download file.

Items Needed: Cisco CallManager 4.0(2) Installation and Recovery Disk or Cisco CallManager 4.0(2) web download file

Perform the following procedure:

Procedure

Step 1 If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator password.

Step 2 Choose whether you want to upgrade via disk or the web.

- Using the Disk, Step 3 through Step 4
- Using the Web File, Step 5 through Step 10

Using the Disk

Step 3 Locate the Cisco CallManager 4.0 Installation, Upgrade, and Recovery Disk 1 of 2 into the drive.and insert it into the drive.

The installation process automatically starts.

Tip Do not remove the disk until you are directed to do so by procedure.

Step 4 Continue the installation by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Using the Web File

Step 5 Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 6 Click **Cisco CallManager Version 4.0**.

Step 7 Download the Cisco CallManager 4.0(2) upgrade file to your hard drive.

Step 8 Note the location where you save the downloaded file.

Step 9 Double-click the downloaded file to begin the installation.

Step 10 A message displays that you run this file for web upgrades only. Click **Yes**.

The extraction window opens.

Step 11 Continue the upgrade by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Upgrading Related Cisco CallManager Services and Detecting the Server (Required)

Continue the upgrade by performing the following procedure.

Note If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator account.

Procedure

Step 1 To confirm which version of Cisco CallManager you are upgrading from and which version you are upgrading to, click **Yes**.

Step 2 To confirm that you have disabled antivirus and intrusion detection software, click **Yes**.

If you have not installed Microsoft SQL 2000 Service Pack 3a (or a later version), an error message displays. To obtain the service pack and corresponding readme documentation, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Tip If you just installed the service pack, you must insert the Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 again after the service pack installs and the server reboots; continue to wait while the Cisco IP telephony application prepares to install.

Step 3 The Preparing to Install window displays while the installation program copies files to your server. This process takes approximately 10 minutes. Do not click Cancel.

Step 4 The Resuming the InstallShield Wizard window displays. Click **Next**.

Step 5 Enter the administrator password. Click **Next**.

Step 6 Enter the private password phrase for the cluster; confirm the private password phrase and click **Next**.

Step 7 To begin the installation, click **Install**.

The status window displays. Do not click Cancel.

Step 8 If you are using the Cisco CallManager 4.0(2) installation disks, a message displays that indicates that you need to insert the next upgrade disk. Perform the following steps:

a. Insert the Cisco CallManager 4.0(2) Installation, Upgrade, and Recovery Disk 2 and click **OK**.

A message displays that indicates that you need to install the first upgrade disk again.

b. Insert the Cisco CallManager 4.0(2) Installation, Upgrade, and Recovery Disk 1 of 2 and click **OK**.

Step 9 Click **Finish**.

Step 10 Click **Yes**.

Upgrading the Cisco CallManager Subscriber Server(s)

Perform the following tasks to upgrade the subscriber servers.

	Task	Important Information and Resources
Step 1	Perform pre-upgrade tasks.	See the "Before You Begin" section on page 3-1 and the"Information That You May Need During the Upgrade" section on page 3-5.
Step 2	Verify that you removed all servers from the NT or Microsoft Active Directory Domain.	See the "Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)" section on page 3-17.
Step 3	Verify that you have disabled and stopped all third-party, Cisco-verified, and Cisco-provided coresident applications that run on the server. Make sure that you have rebooted the server.	See the "Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)" section on page 3-18.
Step 4	**Optional Task** Run the ServPrep utility.	You can run the utility only via the Cisco CallManager Subscriber Preparation Disk. Cisco does not provide this utility on the web. See the "Run the ServPrep Utility (Optional)" section on page 3-19.
Step 5	Use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to Cisco-provided version 2000.2.6 (or later).	Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml. **Caution** If you choose to do so, you can upgrade the operating system on all subscriber servers in the cluster at the same time. This task causes call-processing interruptions.
Step 6	Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). (Required)	The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

	Task	Important Information and Resources
Step 7	Download and install the latest OS-related security hotfixes, if any. (Recommended)	The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.
Step 8	Verify that you installed Microsoft SQL Server 2000, Service Pack 3a (or later).	For information on how to verify and install the service pack, refer to the readme documentation that accompanies the service pack. **Caution** This task causes call-processing interruptions.
Step 9	**Task That You Should Perform Serially** Perform the Cisco CallManager upgrade on one server at a time.	If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.0(2) software kit. If you are upgrading from Cisco CallManager 4.0(1), you can upgrade by using the disks from the Cisco CallManager 4.0(2) software kit or by using the web download file. **Caution** You must perform the Cisco CallManager installation serially; that is, on one server at a time. After you reboot the server and after you verify that the server pulled the subscription from the publisher database server, you can begin the upgrade on the next server. You use the same Cisco CallManager Installation, Upgrade, and Recovery Disks or web download for the publisher database server and subscriber servers. See the "Inserting the Disk or Downloading the Web File" section on page 3-21.
Step 10	After you complete the installation on all servers in the cluster, perform post-upgrade tasks.	See the "Performing Post-Upgrade Tasks" section on page 4-1.

Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)

Tip You can perform this task on all servers in the cluster at the same time.

The reboot causes call-processing interruptions if done at the same time.

Caution When a server exists in a domain during an upgrade, authentication between servers may fail, or the non-default domain security policies may restrict Cisco CallManager from building critical NT accounts. Failing to remove the system from the domain and add it to a work group may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Do not place the servers back into the domain until you have completed the upgrade procedures for every server in the cluster.

Convert any servers that exist in the NT Domain or Microsoft Active Directory Domain by performing the following procedure:

Procedure

Step 1 Choose **Start > Settings > Control Panel > System**.

Step 2 Click the **Network Identification** tab.

Step 3 Click the **Properties** button.

Step 4 Click the **Workgroup** radio button and enter a name, for example, WRKGRP, in the corresponding field.

Step 5 Click **OK**.

Step 6 When prompted to do so, reboot the server.

Step 7 Log in to the server by using the Administrator password.

Step 8 Perform this procedure on every server in the cluster that exists in the NT Domain.

Step 9 Go to the Domain Controller and remove the computer accounts for the Cisco CallManager servers in the cluster.

Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)

Tip You must perform this task on all servers in the cluster at the same time.

The reboot may cause call-processing interruptions.

To review a list of Cisco-verified applications that Cisco supports and that you should disable before the installation, click http://www.cisco.com/pcgi-bin/ecoa/Search. In the Solution pane, click **IP Telephony**. From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**. Click **Search**.

The following platform agents may interfere with the Cisco CallManager installation: antivirus services, intrusion detection services (for example, Cisco Security Agent), OEM server agents, server management agents, VOIP monitoring/performance monitoring, or remote access/remote management agents. Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-verified McAfee services), intrusion detection, and remote management services, ensures that you do not encounter issues that are associated with these services.

This document provides procedures for disabling Cisco-verified McAfee antivirus services only. If you need assistance with disabling other services or applications, refer to the corresponding documentation that accompanies the product.

To disable the McAfee antivirus services, perform the following tasks:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Services window, right-click one of the antivirus services; that is, Network Associates Alert Manager, Network Associates McShield, or Network Associates Task Manager, and choose **Properties**.

Step 3 In the Properties window, verify that the General tab displays.

Step 4 In the Service Status area, click **Stop**.

Step 5 From the Startup type drop-down list box, choose **Disabled**.

Step 6 Click **OK**.

Step 7 Perform Step 1 through Step 6 for all Cisco-approved McAfee antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, and Network Associates Task Manager.

Step 8 Reboot the server and verify that the services are not running.

Caution Make sure that the services do not start after the reboot.

Caution If Cisco-verified antivirus or intrusion detection software is not currently installed on the server, Cisco strongly recommends that you do not install the software until you complete the entire upgrade/installation of all servers in the cluster.

Run the ServPrep Utility (Optional)

Item Needed: Cisco CallManager Subscriber Upgrade Disk 1

Before you install Cisco CallManager, you must run the ServPrep utility and install Cisco IP Telephony Operating System by using the Cisco-provided operating system disks and upgrade to the latest operating sytem 2000.2.6sr1 (or later).

The ServPrep utility, which you run on subscriber servers, updates the network configuration by creating the file, STISys.inf, which contains network information. The utility saves TCP/IP settings, but you lose manually configured NIC settings; for example, hard-coded Speed/Duplex settings. After you complete the installation on all servers in the cluster, you must manually configure previous NIC settings.

Caution This utility supports all Cisco Media Convergence Servers, customer-provided HP DL320 and DL380 servers, and customer-provided IBM xSeries 330, 340, 342, and 345 servers that meet Cisco-approved configuration standards. Do not run this utility on any other servers, including customer-provided servers.

Procedure

Step 1 Insert the Cisco CallManager Subscriber Upgrade Disk 1 into the drive as soon as you can do so.

Step 2 When the Upgrade Warning window displays, carefully read the information and click the **ServPrep Utility** link at the bottom of the window.

Step 3 Run the program from the current location; follow the prompts that display.

Upgrade the Operating System to Cisco-Provided Version 2000.2.6 (or Later) (Required)

Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Perform the upgrade on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.

Cisco recommends that you upgrade to install Cisco IP Telephony operating system version 2000.2.6 with the latest service release 2000.2.6.sr1 (or later) before you upgrade to Cisco CallManager Release 4.0(2).

Download and Install the Latest Cisco IP Telephony Server Operating System Service Release (Required)

Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Download and Install the Latest OS-Related Security Hotfixes (If Any) (Recommended)

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Install Microsoft SQL Server 2000, Service Pack 3a (Required)

For information on how to verify and install the service pack, refer to the readme documentation that accompanies the service pack.

Tip Install this service pack on the publisher database server; complete the Cisco CallManager upgrade on the publisher database server before you install this service pack on the subscriber servers.

Inserting the Disk or Downloading the Web File

Note If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.0(2) software kit.

If you are upgrading from Cisco CallManager 4.0(1), you can upgrade by using the disks from the Cisco CallManager 4.0(2) software kit or by using the web download file.

Items Needed: Cisco CallManager 4.0(2) Installation and Recovery Disk or Cisco CallManager 4.0(2) web download file

Perform the following procedure:

Procedure

Step 1 If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator password.

Step 2 Choose whether you want to upgrade via disk or the web.

- Using the Disk, Step 3
- Using the Web File, Step 5 through Step 10

Using the Disk

Step 3 Locate the Cisco CallManager 4.0 Installation, Upgrade, and Recovery Disk 1 of 2 into the drive.and insert it into the drive.

The installation process automatically starts.

Tip Do not remove the disk until you are directed to do so by procedure.

Step 4 Continue the upgrade by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Using the Web File

Step 5 Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 6 Click **Cisco CallManager Version 4.0**.

Step 7 Download the Cisco CallManager 4.0(2) upgrade file to your hard drive.

Step 8 Note the location where you save the downloaded file.

Step 9 Double-click the downloaded file to begin the installation.

Step 10 A message displays that you run this file for web upgrades only. Click **Yes**.

The extraction window opens.

Step 11 Continue the installation by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Upgrading Related Cisco CallManager Services and Detecting the Server (Required)

Continue the upgrade by performing the following procedure:

Note If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator account.

Procedure

Step 1 To confirm which version of Cisco CallManager you are upgrading from and which version you are upgrading to, click **Yes**.

Step 2 To confirm that you have disabled antivirus and intrusion detection software, click **Yes**.

If you have not installed Microsoft SQL 2000 Service Pack 3a (or a later version), an error message displays. To obtain the service pack and corresponding readme documentation, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Tip If you just installed the service pack, you must insert the Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 again after the service pack installs and the server reboots; continue to wait while the Cisco IP telephony application prepares to install.

Step 3 The Preparing to Install window displays while the installation program copies files to your server. This process takes approximately 10 minutes. Do not click Cancel.

Step 4 The Resuming the InstallShield Wizard window displays. Click **Next**.

Step 5 Enter the administrator password. Click **Next**.

Step 6 Enter the private password phrase for the cluster; confirm the private password phrase and click **Next**.

Step 7 To begin the installation, click **Install**.

The status window displays. Do not click Cancel.

Step 8 If you are using the Cisco CallManager 4.0(2) installation disks, a message displays that indicates that you need to insert the next upgrade disk. Perform the following steps:

a. Insert the Cisco CallManager 4.0(2) Installation, Upgrade, and Recovery Disk 2 and click **OK**.

A message displays that indicates that you need to install the first upgrade disk again.

b. Insert the Cisco CallManager 4.0(2) Installation, Upgrade, and Recovery Disk 1 of 2 and click **OK**.

Step 9 Click **Finish**.

Step 10 Click **Yes**.

Tip Repeat the procedures in the "Upgrading the Cisco CallManager Subscriber Server(s)" section on page 3-16 on each subscriber server until you have upgraded all the servers in your cluster. After you update all of the servers, perform the appropriate procedures in the "Performing Post-Upgrade Tasks" section on page 4-1.

Performing Post-Upgrade Tasks

After you complete the upgrade, perform the appropriate tasks as described below:

	Post-Upgrade Task	Related Information and Procedures
Step 1	Enable all Cisco-verified and Cisco-provided coresident applications, antivirus service or security agent that you previously disabled on the server.	Refer to the following information: • The documentation that accompanies your application • Enabling Third-party Applications, Antivirus Services, or Security Agents, page 4-4
Step 2	Verify that the subscriber servers pulled the copy of the database.	See the "Verifying and Reinitializing Subscriber Connections" section on page 4-5.
Step 3	Verify that all of the appropriate services started. Verify that you can make internal calls. Verify that you can place and receive a call across gateways.	See the "Verifying Services, Patches, and Hotfixes" section on page 4-5. See the "Enabling RIS Data Collector" section on page 4-6. **Caution** If you have third-party software, such as CDR software, integrated with Cisco CallManager and the third-party software does not run as expected after the upgrade, verify that you entered the same SA password on all servers in the cluster.
Step 4	If you have CRS and Cisco CallManager installed on the same server, complete the upgrade by referring to the appropriate documentation.	See the "How does a coresident upgrade work if I have CRS installed with Cisco CallManager?" section on page 1-5.

	Post-Upgrade Task	Related Information and Procedures
Step 5	After you complete the Cisco CallManager upgrade on every server in the cluster, reinstall all Cisco-verified applications and all plug-ins that were previously installed on the server except the Cisco CDR Analysis and Reporting plug-in. For example, if you have integrated your enterprise directory with Cisco CallManager, you must reinstall the Cisco Customer Directory Configuration Plugin on all servers in the cluster after the upgrade, starting with the publisher database server. Reinstalling the plug-in populates your enterprise directory with any additional schema extensions and data entries that Cisco CallManager needs.	Refer to the appropriate documentation that accompanies the applications.
Step 6	Upgrade Cisco TAPI, Cisco JTAPI, Cisco TSP (for the voice-messaging system), and the Cisco TSP for Cisco SoftPhone.	See the following sections for more information: • Upgrading TAPI, JTAPI, and Cisco Telephony Service Provider (TSP), page 4-8 • Upgrading the Cisco TAPI/TSP for Cisco SoftPhone, page 4-8
Step 7	If you are using Cisco Unity as your voice-messaging system, configure the appropriate settings to ensure proper failover.	For more information, refer to the *Release Notes for Cisco CallManager*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
Step 8	Verify that all Cisco IP telephony applications that are integrated with Cisco CallManager run properly. If you need to do so, upgrade the Cisco IP telephony applications that are integrated with your Cisco CallManager system.	Refer to the *Cisco CallManager Compatibility Matrix* by clicking the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm If the application is compatible with this version of Cisco CallManager, refer to the appropriate Cisco IP telephony application documentation.
Step 9	For your migrated version of Cisco CallManager Attendant Console to work, you must check the Call Park Retrieval Allowed check box for the ac user that you configured in the Global Directory. The attendant console does not initialize if you do not check this check box.	For more information on how to perform this task, refer to the *Cisco CallManager Administration Guide*.
Step 10	After you upgrade Cisco CallManager, the database name automatically increments; for example, from CCM0300 to CCM0301. Third-party CDR software may have SQL triggers that are hard coded to the original database name. The triggers may point to the previous database name and cause all CDR flat files to write to the BAD directory on the publisher database server.	If you need technical assistance with this issue, directly contact the third-party software vendor.

	Post-Upgrade Task	Related Information and Procedures
Step 11	If you want to use Norton AntiVirus, install the application and perform post-installation tasks.	Refer to *Using Symantec/Norton AntiVirus with Cisco CallManager.*
Step 12	The locale, English_United_States, installs automatically on the server. To upgrade existing locales or to add additional locales to the server, install the Cisco IP Telephony Locale Installer.	You can obtain locale-specific versions of the Cisco IP Telephony Network Locale installer for Cisco CallManager 4.0 when they become available at http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml. Refer to the readme file that is posted next to the Cisco IP Telephony Locale Installer software for the complete list of supported languages and localized features. For more information on installing the locale installer, refer to U*sing the Cisco IP Telephony Locale Installer.* **Note** The locale installer has version-specific support for Cisco CallManager releases. Cisco IP Telephony Locale Installer, Version 4.0(1) supports Cisco CallManager Version 4.0(1) or later.
Step 13	You must configure the Network Interface Card (NIC) Speed and Duplex settings of the Cisco CallManager server to match the configuration of the LAN switch port to which the server is connected. Failure to match these settings between the server and switch may cause degraded network performance and unexpected errors to occur. Contact your network administrator or see the Cisco IOS configuration documentation to determine your current settings of the LAN switch port to which the Cisco CallManager NIC is connected.	Some administrators have found that the 100/Full setting works well.
Step 14	Verify the version of hotfixes and service packs that are installed on the server. Download the latest hotfixes, service packs, and Cisco CallManager service release that are available on the web. This task requires a reboot of the server after you install the files. **Tip** Perform this task on an ongoing basis to maintain your system.	See Verifying Services, Patches, and Hotfixes, page 4-5 See Enabling RIS Data Collector, page 4-6 **Tip** The service releases may post to the web after the Cisco CallManager upgrade is available.
Step 15	Set Data Collection Enable to true in Cisco RIS Data Collector service	Enabling RIS Data Collector, page 4-6

	Post-Upgrade Task	Related Information and Procedures
Step 16	To ensure optimal load balance, reassign the route lists to Cisco CallManager groups that you configured if you had more than one primary Cisco CallManager server configured.	Reassigning Route Lists, page 4-7
Step 17	Back up the Cisco CallManager server. **Tip** Perform this task daily to ensure that you have a recent backup of your system.	Refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide, Version 4.0(1)* (or later). To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Enabling Third-party Applications, Antivirus Services, or Security Agents

After you log in to the server, enable all third-party applications, antivirus services, or security agents through the Control Panel by completing the following procedure:

Step 1 Choose **Start > Programs > Administrative Tools > Services.**

Step 2 Locate the third-party application, antivirus service or security agent that you wish to start, right-click the service and choose Properties.

Step 3 In the Properties window, click the General tab.

Step 4 From the Startup type drop-down list box, choose **Automatic**.

Step 5 Click **OK.**

Step 6 In the Services window, right-click the application or service and click **Start**.

Verifying and Reinitializing Subscriber Connections

If the connections between the publisher database server and the subscriber servers within a cluster are broken for any reason, you cannot copy the database to the subscriber servers.

Verifying the Status of the Subscription

To determine whether the connections between the publisher database server and the subscriber servers within a cluster are broken, wait 35 minutes after you have installed the last subscriber server in the cluster. Then, open SQL Server Enterprise Manager. If a red X icon appears next to the subscription, the subscription is broken.

Reinitializing the Subscription/Starting the Replication Snapshot Agent

If you determine that one or more subscription connections are broken, as indicated by the red X icon next to the subscriptions, reinitialize the subscriptions and start the replication snapshot agent on the publisher database server.

Procedure

Step 1 Open SQL Server Enterprise Manager by choosing **Start > Programs > Microsoft SQL Server > Enterprise Manager**.

Step 2 In the following path, choose the name of the publisher database that you are configuring: Microsoft SQL Servers/SQL Server Group/<this server's hostname>/Databases/<the publisher database name>Publications.

Step 3 In the main window, right-click the subscription name and choose **Reinitialize all Subscriptions**. Click **Yes** to confirm.

Step 4 In the following path, choose the **Snapshot Agents** folder: Microsoft SQL Servers/SQL Server Group/<this server's hostname>/Replication Monitor/Agents.

Step 5 Right-click the publication name that matches the database name that you are configuring; then, click **Start**.

In rare cases, the reinitialization of the subscriptions may not work. If you determine that the previous procedure did not work as expected, contact the team that provides technical assistance for this product; for example, your Cisco AVVID Partner or the Cisco Technical Assistance Center (TAC).

Verifying Services, Patches, and Hotfixes

Perform the following tasks:

- Verify that the appropriate services run on each server in the cluster (About Services, page 4-6)
- Verify that you have installed the latest Microsoft patches and hotfixes (About Microsoft Patches and Hotfixes, page 4-6)
- Verify that you have installed the latest Cisco CallManager service release (About Cisco CallManager Service Releases, page 4-6)

About Services

Open Cisco CallManager Serviceability and verify that all migrated services are running. To review service activation procedures and service recommendations, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Caution Do not start and stop services through the Microsoft Computer Management window. Starting and stopping services through the window causes problems with the Cisco CallManager database.

About Microsoft Patches and Hotfixes

Refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

About Cisco CallManager Service Releases

After you install this version of Cisco CallManager on all servers in the cluster, Cisco strongly recommends that you install the latest Cisco CallManager service release on all servers in the cluster. These service releases provide bug fixes for your system.

Be aware that Cisco CallManager service releases are cumulative. Cisco rolls these bug fixes into the next Cisco CallManager release.

Tip Make sure that you install the same version of the service release on every server in the cluster.

To obtain the latest Cisco CallManager service release, perform the following procedure:

Step 1 Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 2 Click **Cisco CallManager Version 4.0**.

The Cisco CallManager 4.0 software page displays.

Step 3 Locate and download the readme file for the service release.

The readme file provides procedures, caveats, and descriptive information for installing the files.

Step 4 Using the readme file as a reference, install the Cisco CallManager service release on every server in the cluster where Cisco CallManager is installed.

Enabling RIS Data Collector

Procedure

Step 1 From Cisco CallManager Administration, choose **Service > Service Parameters**.

The Service Parameters Configuration window displays.

Step 2 From the Server pull-down menu, choose any server.

Step 3 From the Service pull-down menu, choose RIS Data Collector.

Step 4 In the Data Collection Enabled field, choose True.

Step 5 Click **Update**.

Reassigning Route Lists

If you more than one primary Cisco CallManager server in a cluster was configured prior to upgrading to Cisco CallManager 4.0(2), you will need to reassign the route list to the Cisco CallManager group that you configured in Cisco CallManager Administration to maintain optimal load balance. To ensure call-processing redundancy, the upgrade program created a Cisco CallManager group that contains a primary server and a backup server for every primary Cisco CallManger server in the cluster and then assigned route lists to each Cisco CallManager group by using a round-robin algorithm. The following name format applies for the created Cisco CallManager group: RLCMG_<primary Cisco Callmanager name>.

Procedure

Step 1 Evaluate the Cisco CallManger group and route list configuration for load balancing and redundancy, as described in the *Cisco CallManager System Guide* and the *Cisco CallManager Network Solutions Design Guide.*

Step 2 Assign the route list(s) to the Cisco CallManger group(s) that you have configured in Cisco CallManager Administration.

Step 3 Delete the migrated CCM group, RLCMG_<primary CM-server-name>.

Viewing the Component Versions That Are Installed on the Server

The mcsver.exe program reports the current version of all installation components, including the operating system. Be aware that Cisco does not report the actual Cisco CallManager version through this program. Recognize that most of these components, which run from the installation disks during the initial installation, no longer exist on the system.

The version for OS Image equals your operating system disk version number. The version of OS Image will change only if you do a new installation with the Cisco IP Telephony Server Operating System Hardware Detection disk.

The version for stiOSUpg.exe equals the version of the operating system upgrade that you last ran either via disk or via the web. When Cisco updates and releases the Cisco IP Telephony Server Operating System OS Upgrade disk (Disk 2), the version of stiOSUpg changes.

Perform the following procedure to view the component versions that are installed on the server:

Procedure

Step 1 Use Windows Explorer to browse to the following folder:

C:\utils\mcsver

Step 2 View the versions of the components that are running on your server.

Upgrading TAPI, JTAPI, and Cisco Telephony Service Provider (TSP)

You must upgrade the Telephony Application Programming Interface and Java Telephony Application Programming Interface (TAPI/JTAPI) client software on any application server or client workstation on which TAPI/JTAPI applications are installed. If you do not upgrade the TAPI/JTAPI client, your application will fail to initialize.

The following information applies if you have integrated a Cisco Unity system with Cisco CallManager. TSP makes the voice-mail ports available to Cisco Unity. To ensure that Cisco Unity integrates properly with Cisco CallManager, you may need to upgrade the TSP that is integrated with the voice-messaging system. To ensure that you upgrade to the appropriate TSP release, refer to the *Cisco CallManager Compatibility Matrix*.

Upgrading the Cisco TAPI/TSP for Cisco SoftPhone

Perform the following procedure to upgrade the Cisco SoftPhone TAPI/TSP to the version that is stated in the *Cisco CallManager Compatibility Matrix*.

Procedure

Step 1 From each Cisco Softphone client, browse into server that is running Cisco CallManager Administration and log in with administrative privileges.

Tip To browse into the server, enter http://<CM-server-name>/CCMAdmin/main.asp, where <CM-server-name> equals the name of the server, in the Address bar in the web browser.

Step 2 From the Application menu, choose **Install Plugins**.

Step 3 Click the **Cisco Telephony Service Provider** icon that is associated with the plug-in.

Step 4 To complete the upgrade, follow the prompts in the window.

Step 5 Verify that a basic call works as expected for Cisco SoftPhone.

Using the Cisco CallManager Music On Hold Disk or Download

Note This section applies if you have never downloaded the Cisco CallManager Music On Hold files from the web or used the Cisco CallManager Music On Hold disk.

When you initially install Cisco CallManager on your server, a default music on hold audio file sample automatically installs for customer use. To increase your music on hold (MOH) selection, you may download one of the following two files via the web:

- ciscocm-MusicOnHold, which is a set of wav files that provide the entire music selection from the disk
- ciscocm-MusicOnHoldSampler, which is a small set of files that offers a sample of music that is available on the disk

For information on the MOH feature, refer to the latest version of the *Cisco CallManager Administration Guide* and the latest version of the *Cisco CallManager System Guide*.

As a Cisco CallManager user, you can use any disk/file with music on hold. Because of licensing restrictions, you must not distribute the Cisco CallManager Music on Hold disk/files to anyone else, and you must not use the files for any other purpose.

CHAPTER 5

Reverting to the Previous Configuration After an Upgrade Attempt

In the unlikely event of an upgrade failure, or if you prefer an earlier version of Cisco CallManager, perform the following steps to return the Cisco IP Telephony Applications Server to the configuration that was in effect prior to the upgrade.

Reconfiguring If You Did Not Remove a Drive Before the Upgrade

This procedure assumes that you have a good backup file on a tape device or network directory. For a list of files that the utility backs up, refer to the appropriate backup documentation:

- If you upgraded from Cisco CallManager 3.2, refer to *Using Cisco IP Telephony Applications Backup Utility, Version 3.5.52* (or later) at http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.
- If you upgraded from Cisco CallManager 3.3, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Perform the following procedure:

Procedure

Step 1 Perform the following procedure, depending on whether you are reverting the publisher database server or the subscriber server(s):

Publisher Database Server

Step 2 Reinstall the operating system by using Cisco-provided operating system version 2000.2.4 or later.

You must perform this task by using the Cisco-provided disks that shipped with Cisco CallManager server.

Step 3 Using the disks that originally shipped with Cisco CallManager, reinstall a version of Cisco CallManager 3.2, 3.3, or 4.0 (depends on the original disks).

Do not install or configure the backup utility that automatically displays during the installation.

Step 4 If you want to do so, install and configure the appropriate backup utility by using the Cisco CallManager Backup Utility Disk that shipped with Cisco CallManager Release 4.0(2):

- If upgraded from Cisco CallManager 3.2, install and configure the Cisco IP Telephony Applications Backup Utility, Version 3.5.53 (or later).
- If you upgraded from Cisco CallManager 3.3, install and configure the Cisco IP Telephony Backup and Restore System (BARS).

Step 5 Perform the necessary upgrade(s) to match the most recent successful backup.

Note To revert to the pre-upgrade configuration, you must restore the version of Cisco CallManager that was in effect when the last successful backup occurred.

Step 6 Restore the data.

Subscriber Server(s)

Step 7 Reinstall the operating system by using Cisco-provided operating system version 2000.2.4 or later.

You must perform this task by using the Cisco-provided disks that shipped with Cisco CallManager server.

Step 8 Using the disks that originally shipped with Cisco CallManager, reinstall a version of Cisco CallManager 3.2, 3.3, or 4.0 (depends on the original disks).

Do not install or configure the backup utility that automatically displays during the installation.

Step 9 If you want to do so, install and configure the appropriate backup utility by using the Cisco CallManager Backup Utility Disk that shipped with Cisco CallManager Release 4.0(2):

- If you upgraded from Cisco CallManager 3.2, install and configure the Cisco IP Telephony Applications Backup Utility, Version 3.5.53 (or later).
- If you upgraded from Cisco CallManager 3.3, install and configure the Cisco IP Telephony Backup and Restore System (BARS).

You install and configure the backup utility on the subscriber when a Cisco IP telephony application, for example, CRS, exists on the subscriber server.

Reconfiguring If You Removed a Drive Before the Upgrade

This process may take from 15 minutes to 60 minutes, depending on the size of the drive.

Perform the following procedure:

Procedure

Step 1 Shut down the server.

Step 2 Remove the existing hard drive from Slot 0. Insert the hard drive that was removed prior to the upgrade into Slot 0.

Note On the MCS-7845, perform this additional step. Remove the existing hard drive from Slot 2 and insert the hard drive that you removed prior to the upgrade into Slot 2.

Step 3 Slightly pull the drive in Slot 1; for the MCS-7845, also slightly pull the drive in Slot 3. Do not completely remove the drives from the server.

Step 4 Power on the system.

Cisco MCS

Note Step 5 does not apply for MCS-7835I-2.4 and MCS-7835I-3.0 servers.

Step 5 Perform the following procedure for all Cisco MCS where you removed a drive:

a. To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845, press **F2**.

Note The MCS-7835H-2.4 (or later) and MCS-7845H-2.4 (or later) default to F2, and the process automatically continues after a 10-second delay.

b. This step applies only for the MCS-7830, MCS-7835, or MCS-7845. When prompted, press **F1** to continue.

c. Push the drive that was slightly pulled in Step 3 into Slot 1.

d. For the MCS-7830, MCS-7835, or MCS-7845, choose **Start > Compaq Systems Tools > Compaq Array Configuration Utility**.

e. Watch the status bar in the lower, right corner to determine when drive mirroring completes.

f. This step applies only for the MCS-7845. After the mirroring process completes in Slot 1, push the drive into Slot 3 that was pulled in Step 3.

g. Verify that the process completed successfully.

MCS-7835I-2.4 or MCS7835I-3.0 or IBM xSeries Servers

Step 6 Press **F5**.

Step 7 Press **Ctrl + I**.

Step 8 Using the arrow keys, choose **Advanced functions**.

Step 9 Using the arrow keys, choose **Copy the configuration from drives to the controller**.

Step 10 Press **Y** for Yes.

Processing begins.

Step 11 Press any key to continue.

Step 12 Using the arrow keys, press **Exit**.

Step 13 only Press **Ctrl + Alt + Del**.

Step 14 Log in to the server by using the Administrator password.

Step 15 Push the drive that was slightly pulled in Step 3 into Slot 1.

Note Messages display about the drive state. Proceed with the process. Do not remove the drive.

This process takes about 35 to 40 minutes, depending on the server.

Step 16 Choose **Start > Programs > ServeRaid Manager > ServeRaid Manager**. You can view the progression of the drive mirroring.

Step 17 Verify that the process completed successfully.

Reverting the Hard Drive After Drive Mirroring Completes

If you want to revert a hard drive after drive mirroring and you have made changes that affect the domain trust relationship, you must remove the server from the domain and then add it back to the domain. You must have rights to join the server to the domain before you perform this procedure.

Procedure

Step 1 Choose **Start > Settings > Control Panel > System**.

Step 2 Click the **Network Identification** tab.

Step 3 Click the **Properties** button.

Step 4 Click the **Workgroup** radio button and enter **WRKGRP** in the corresponding field.

Step 5 Click **OK**.

Step 6 When prompted to do so, reboot the server.

Step 7 Log in to the server by using the Administrator password.

Step 8 Perform Step 1 through Step 3.

Step 9 Click the **Domain** radio button and enter the domain name for the server.

Step 10 Click **OK**.

Step 11 When prompted to do so, reboot the server.

Reverting Upgraded Cisco IP Telephony Applications After You Revert Cisco CallManager

After you revert the entire cluster to a previous version of Cisco CallManager, you must revert integrated Cisco IP telephony applications. You must revert these integrated applications to the version that is compatible with the reverted Cisco CallManager. To revert the application, perform the following procedure:

Procedure

Step 1 In the *Cisco CallManager Compatibility Matrix,* identify the telephony product and compatible version that matches the cluster reversion. Go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm to locate this document.

Step 2 From the application server or the client workstation, if applicable, browse into the reverted server that is running Cisco CallManager Administration and log in with administrative privileges.

Tip To browse into the server, enter http://<CM-server-name>/CCMAdmin/main.asp, where <CM-server-name> equals the name of the server, in the Address bar in the web browser.

Step 3 From the Application menu, choose **Install Plugins**.

Step 4 Click the appropriate plugin, as seen in the following list:

- **Cisco Telephony Service Provider** for Cisco SoftPhone
- **Cisco JTAPI** for any application that interfaces with Cisco CallManager by using JTAPI.

Step 5 To complete the installation, follow the prompts in the window.

Step 6 Perform this procedure on all servers where the application is installed.

CHAPTER 6

Error Messages

The following error messages may display in dialog boxes (not the log file) during the upgrade. You can obtain and review the log file, ccminst <data/time stamp>.log, from C:\Program Files\Common Files\Cisco\Logs.

Table 6-1 Installation Error Messages

Error Message	Reason	Corrective Action
You must provide the Computer Name of the publisher server. IP addresses or fully qualified DNS names are not allowed.	You must not enter periods (.) when you enter the publisher database server name.	Reenter the information correctly.
You must provide the publisher server name when installing a subscriber.	This message displays when you install Cisco CallManager on the subscriber server and do not provide the publisher database server name.	Reenter the information correctly.
You have entered an invalid product key. Please re-enter the key.	You entered an invalid product key.	See the Cisco CRS installation documentation to obtain the Cisco CRS product keys. See I*nstalling Cisco CallManager Release 4.0(2)* for the Cisco CallManager product key.
You must enter a password.	This message displays when you do not enter a password, but the application requires a password for the installation to occur.	Enter the correct password.
The passwords that you entered do not match.	This error message displays when you enter a password more than one time, but the password that you enter does not match the password on the server.	Enter the same password on all servers in the cluster.
The password that you entered is not valid.	You entered an invalid password.	Enter the correct password.
You must enter a phrase from 1 to 15 characters in length. This phrase may contain English lower-case letters, English upper-case letters, Westernized Arabic Numerals, and the following Non-alphanumeric “special characters” { } . < > : ? / | \ ` ~ ! @ $ ^ & * ( ) _ - +	You entered invalid characters for the private password phrase.	Enter valid characters.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
Pending file operations are occurring. Reboot the server and then install Cisco CallManager.	Pending file operations are occurring.	Reboot the server and then install Cisco CallManager.
You are not logged on as 'Administrator'. You must log in by using local Administrator user name and password to install Cisco CallManager.	You did not log in to the server with the local Administrator user name and password.	Log in to the server with the local Administrator user name and password.
You do not have administrator privileges. You must have administrator privileges to install Cisco CallManager.	You do not have administrative privileges.	Log in to the server with an account that has administrative privileges.
Windows 2000 Server is not installed. Install Windows 2000 Server before you install Cisco CallManager.	You did not install the appropriate version of the operating system.	Make sure that you installed the operating system version 2000.2.3 (or later) on all dedicated and coresident servers. Upgrade to 2000.2.6 (or later) and install the latest service release (2000-2-6sr1 or later) before installing Cisco CallManager.
Windows 2000 Service Pack 3 or later is not installed. You must have Windows 2000 Service Pack 3 or later installed before you install Cisco CallManager.	You did not install the appropriate version of the operating system.	Make sure that you installed the operating system version 2000.2.3 (or later) on all dedicated and coresident servers. Upgrade to 2000.2.6 (or later) and install the latest service release (2000-2-6sr1 or later) before installing Cisco CallManager.
You must install CallManager by double clicking CCMSetup.exe.	You tried to install Cisco CallManager by double clicking the msi file that is part of the Cisco CallManager package.	Double-click the CCMSetup.exe.
You must apply SQL 2000 Service Pack 3 (or later) before proceeding with this installation.	You did not install Microsoft SQL 2000 Service Pack 3.	Install Microsoft SQL 2000 Service Pack 3 and perform the Cisco CallManager upgrade.
If you have installed intrusion detection or anti-virus protection software, you must stop and disable these applications from the Services Control console before you continue with the Cisco CallManager installation. All other installed third-party applications must be uninstalled before proceeding with the CallManager installation. Failure to follow these directives could result in un-recoverable errors. Would you like to proceed?	This message always displays to alert the administrator of the requirements.	If you have Cisco-verified applications (Cisco AVVID Partner Applications) or platform agents that are installed on the server, you must disable/uninstall them and stop the services.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
Because the <BUILDVERSION> of this Cisco CallManager MSI package is not compatible with the Cisco CallManager setup file (ccmsetup.exe), make sure that you are using the ccmsetup.exe that was distributed with this version of Cisco CallManager. The installation will now abort.	This message indicates that the MSI package is not compatible with the Cisco CallManager setup file.	Use the ccmsetup.exe file that was distributed with this version of Cisco CallManager.
You are attempting to upgrade Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION>. Direct upgrades from this version of Cisco CallManager are not supported. You must first upgrade to a compatible Cisco CallManager version before upgrading to this version. The installation will now abort.	You tried to upgrade from a version other than Cisco CallManager 3.2 or Cisco CallManager 3.3.	Upgrade to Cisco CallManager 3.2 or Cisco CallManager 3.3 before attempting to upgrade to Cisco CallManager 4.0.
You are attempting to upgrade Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION>. Upgrades from this version of Cisco CallManager require using the Same-Server Recovery method. Please refer to the Upgrading Cisco CallManager Release 4.0(2) documentation for more information. The installation will now abort.	You attempted upgrade directly from Cisco CallManager 3.2 to Cisco CallManager 4.0(2) without following the Same Server Recovery procedures.	You must perform a Same Server Recovery by using the operating system disks that ship with this version of Cisco CallManager to install operating system. For publisher servers, see the "Install the Operating System by Using Same Server Recovery (Required)" section on page 2-20. For subscriber servers, see the "Install the Operating System by Using Same Server Recovery (Required)" section on page 2-30.
You are attempting to upgrade Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION> by using the web download file. You cannot use the web download to upgrade from this version of Cisco CallManager directly. You must obtain the upgrade CD-ROM disks from your Cisco account representative to complete this upgrade. The installation will now abort.	You cannot upgrade Cisco CallManager 3.3(x) to 4.0(2) by using the package for web (PFW) download file.	You must use the upgrade CD-ROM disks from the Cisco CallManager 4.0(2) software kit. Contact your Cisco account representative.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
The Same System Recovery flag was detected. Same Server Recovery is required for upgrades from Cisco CallManager 3.2 to Cisco CallManager 4.0. Are you upgrading a Cisco CallManager 3.2 publisher database server to Cisco CallManager 4.0?	You chose the same server recovery option when you installed the operating system.	If you are upgrading from Cisco CallManager 3.2 to Cisco CallManager 4.0(2), refer to the *Upgrading Cisco CallManager Release 4.0(2)* document. If you are installing Cisco CallManager on a publisher server for the first time, click **No** and continue with the installation. If you are installing Cisco CallManager on a subscriber server for the first time, click **No** and continue with the installation. **Note** If you click Yes, the installation program configures your server as a publisher server.
The installation has detected that the server exists in a domain. When a server exists in a domain, authentication between servers may fail or the non-default domain security policies may be too restrictive for the Cisco CallManager installation to build critical NT Accounts during an upgrade. Failure to remove the server from the domain and add to a workgroup may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Would you like to proceed?	The server exists in a domain.	Before you continue the installation, Cisco strongly recommends that you remove all servers in the cluster from the domain.
This release of Cisco CallManager is not supported on this server model. The installation will now abort.	You cannot install this version of Cisco CallManager on this server.	Refer to the *Cisco CallManager Compatibility Matrix* for a list of servers on which you can install this version of Cisco CallManager. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
The installation program does not have enough disk space on the C drive to complete the installation. The installation program requires that you have 3.0 gigabytes of disk space available on your server. Make at least 3.0 gigabytes of disk space available and restart the installation. For information, refer to the Upgrading Cisco CallManager guide.	You attempted an upgrade and do not have enough free disk space.	Make 3.0 gigabytes of disk space available and restart the installation program.
This version of Cisco CallManager is currently installed.	This message displays when you attempt to install the same version of Cisco CallManager that is currently on the server.	Remove the disk from the drive.
A newer version of this package has already been installed.	This message displays when you attempt to install a previous version of Cisco CallManager after a successful installation of a later version.	Remove the disk from the drive.
Cisco CallManager install did not complete successfully. Review the log file for more information.	The Cisco CallManager installation failed.	Obtain and examine the log file.
Unable to locate MSI package associated with this bootstrapper.	You did not copy all the files that came with the Cisco CallManager installation package to the server.	Copy the complete installation package to the server and rerun the Cisco CallManager installation.
Error opening MSI package	Cisco CallManager Setup cannot find the MSI package.	This message displays if you encounter a media problem; insert the disk again.
This package has already been installed.	This message displays when you attempt to install the same version of Cisco CallManager again after a successful installation.	Remove the disk from the drive.
An unexpected error occurred.	An error occurred during the Cisco CallManager Setup.	Obtain and examine the log file.
An unexpected error occurred while creating the log directory.	The installation could not create the log file directory.	Verify that security policies on the server are not restrictive.
The local security policy “Restrict CD-ROM access to locally logged-on user only” is enabled. This setting interferes with the Cisco CallManager installation. Please disable this setting using the Local Security Policy utility, reboot, and rerun the Cisco CallManager installation.	This message indicates that the “Restrict CD-ROM access to locally logged-on user only” local security policy is enabled on your server.	Disable this setting by using the Local Security Policy utility, reboot, and rerun the Cisco CallManager installation. For more information, see the “cm1.mydomain.com” section on page 6-13.
Failure occurred trying to get DBNAME value from registry. Aborting Cisco CallManager installation.	The installation could not read DBNAME value from registry on the local machine.	Reboot the server and rerun the Cisco CallManager installation.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
Failure occurred trying to validate the format of DBNAME value. Aborting Cisco CallManager installation.	The registry contains an invalid format of the DBNAME value. This error only occurs if you have manually modified this value.	Make sure that the DBNAME value is in the format CCM0xxx, where x stands for any digits.
Current OS version does not meet minimum requirements. Aborting Cisco CallManager install.	Cisco CallManager Release 3.3(4) requires Cisco-provided operating system version 2000.2.6 (or later) and the service release 2000-2-6sr1 (or later.)	Refer to *Cisco Compatibility Matrix* to review which versions are compatible for installation. To access the document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.
Installing Cisco CallManager using Terminal Services is not allowed. Install will now abort.	Cisco does not support Terminal Services for Cisco CallManager installations, upgrades, or configuration tasks. Cisco Technical Assistance Center (TAC) uses Terminal Services for remote management and troubleshooting tasks.	If you want to use Virtual Network Computing (VNC), obtain the most recent version of the documentation at http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.
Failed to launch <name of executable>, aborting install	The installation attempted to launch the executable, and the launch failed.	Obtain and examine the log file. You may have a media problem.
Failure occurred during the Cisco Directory installation. Refer to the log file C:\Program Files\Common Files\Cisco\Directory\IntegratedSetup.trc for details. Aborting Cisco CallManager install.	The DC Directory installation failed.	Obtain and examine the log file.
The Cisco CallManager installation detected an error while copying files. Stop all platform agents and Cisco-verified applications, and restart the installation. For more information, refer to the Upgrading Cisco CallManager document.	The Cisco CallManager installation failed to copy files to your server.	Stop all platform agents and Cisco-verified applications, and restart the installation. For more information if you are upgrading from Cisco CallManager 3.2, see "Before You Begin" section on page 2-1. For more information if you are upgrading from Cisco CallManager 3.3, see "Before You Begin" section on page 3-1.
Failure occurred during the Cisco CallManager installation. Please look at the Cisco CallManager installation log file for details. Aborting Cisco CallManager installation.	The Cisco CallManager installation detected an error while copying files. Stop all platform agents and Cisco-verified applications, and restart the installation. For more information, refer to the Upgrading Cisco CallManager document.	Obtain and examine the log file.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
The password of [X] does not match the password on the publisher [Y]. For details, review the log file [Z].	The username and/or password of the user installing Cisco CallManager on the subscriber server does not match the username and/or password on the publisher database server.	Make sure that you entered the correct publisher server name and that the username and password on the publisher and subscriber match.
Because no network connectivity exists or you entered the incorrect publisher server name, the installation could not verify the password of [X] against the publisher [Y]. For details, review the log file [Z].	During the subscriber server installation, this error occurs if no network connection exists between the subscriber and publisher database servers or you did not enter the correct name of the publisher database server.	Verify the connection between the publisher database server and subscriber server and make sure that you entered the correct publisher database server name.
Either the password of [X] does not match the password on the publisher [Y], or a network connectivity error occurred. For details, review the log file [Z].	One of the following problems occurred: • No network connectivity exists between the publisher database server and the subscriber server. • The username and/or password of the user installing Cisco CallManager on the subscriber server does not match the username and/or password on the publisher database server. • You entered the incorrect publisher database server name.	Do each of the following tasks: • Verify the connection between the publisher database server and subscriber server. • Make sure you installed Cisco CallManager on the publisher database server and subscriber server using the Administrator username and password. • Make sure you entered the correct publisher database server name.
The private password phrase does not match the private password phrase on the publisher [X]. For details, review the log file [Y].	During the subscribe server installation, one of the following problems occurred: • The passwords of the NT service accounts did not match. • You entered the incorrect publisher database server name • You entered a different private password phase on the publisher database server than you did on the subscriber server.	Do each of the following tasks: • Make sure that a trusted connection exists between the subscriber server and the publisher database server. • Make sure that you entered the correct publisher database server. • Make sure you entered the same private password phrase that you entered on the publisher database server.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
The installation could not verify the private password phrase on the publisher <server name>, because the user does not have permission to access the publisher server over the network. For details, review the log file <log file name>.	The installation could not verify the private password phrase on the publisher <server name>, because the user does not have permission to access the publisher server over the network. For details, review the log file <log file name>.	During the installation of a subscriber server, the installation program could not verify the private password phrase against the publisher server because of the security settings on either the Publisher or the Subscriber. The probable causes include the following: • The Publisher or the Subscriber server was in a domain during the installation. • There were some local security policy settings on the machine that prevented the installation program from performing this operation.
The installation failed to verify the Cisco CallManager version that runs on the publisher database server. Cancel the installation, and review the log file at C:\Program Files\ Common Files\Cisco\Logs\ CCMUIInst.log.	During the subscriber server installation, this error occurs if no network connection exists between the subscriber and publisher database servers or you did not enter the correct name of the publisher database server.	Verify the connection between the publisher database server and subscriber database server and make sure that you entered the correct publisher database server name.
The Cisco CallManager version you are installing on this subscriber does not match the version running on the publisher database server. Cancel the installation and ensure the publisher is upgraded to this Cisco CallManager version before you continue.	You attempted to install a different version of Cisco CallManager on the subscriber database server than you installed on the publisher database server.	Install the same version of Cisco CallManager on the subscriber database server that you installed on the publisher database server.
UMX.dll failed to register. After you complete the installation, review the log file.	UMX.dll failed to register because the process creation failed, the process terminated abnormally, or an error occurred when the system was executing regsvr32.	Verify that you rebooted the server after the installation. Execute a command prompt, enter regsvr32 C:\dcdsrvr\lib\UMX.dll, and press Enter. To verify that you corrected the problem, try to add a new user in Cisco CallManager Administration on this server.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
Indexing directory data did not finish. After you complete the installation, review the log file. The log file C:\dcdsrvr\log\DirInstallValidation.log.	The installation could not determine whether the DC Directory completed the indexing of its data.	Continue with installation. At the end of the installation, reboot the server when prompted to do so. After you reboot the server, bring up the services control and wait for DC Directory Server to have a status of *started*. If this is a publisher database server, you can install Cisco CallManager on the subscriber database servers. If this is a subscriber database server, go to a command window and enter **dcdrepcl trigger all**. Depending on the number of users that are configured in your system, the service may be in the starting state for a long time before changing to a started state.
The Cisco CallManager installation failed to stop <list of services> service(s). Please reboot the server, manually stop the service(s), and rerun the Cisco CallManager installation program.	The installation program failed to stop the services during installation.	Reboot the server, manually stop the service(s), and rerun the Cisco CallManager installation program.
The installation encountered an unknown error while trying to resolve the Publisher server name [X]. For more information, review the log file CCMInstUI.log.	The name resolution of the publisher server failed.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 6-11.
The installation could not resolve the Publisher server name [X] to a valid IP address. Verify that you entered the correct publisher server name, and review the log file CCMInstUI.log for more information.	You entered the wrong publisher server name, or the hosts file has the wrong information.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 6-11.
The installation successfully resolved the Publisher server name [X] to IP address [Y] but could not resolve the IP address back to a host name.	The reverse name resolution of the Cisco CallManager publisher server failed.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 6-11.
The installation successfully resolved the Publisher server name [X] to IP address [Y] and resolved the IP address back to the host name [Z]. The resolved host name does not match the server name that you entered.	The publisher server name that you entered does not match the server name that the installation program retrieved after completing forward and reverse name resolution.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 6-11.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
Because mapped network drives exist on the server, the installation could not verify the password of [x] against the publisher [y]. Disconnect all the mapped drives, reboot the system, and rerun the installation. For details, review the log file [z].	The installation could not verify that the password on the subscriber server matches the password on the publisher database server.	Disconnect all the mapped drives, reboot the system, and rerun the installation.
Because mapped network drives exist on the server, the installation could not verify the private password phrase against the publisher [y]. Disconnect all the mapped drives, reboot the system, and rerun the installation. For details, review the log file [z].	The installation could not verify that the private password phrase on the subscriber server matches the private password phrase on the publisher database server.	Disconnect all the mapped drives, reboot the system, and rerun the installation.
The Cisco CallManager installation detected an unrecoverable error during database migration. You must revert to the original version of Cisco CallManager. For more information, refer to the *Installing the Operating System on the Cisco IP Telephony Applications Server* and *Upgrading Cisco CallManager* documents.	The installation program failed to migrate the Cisco CallManager data.	Revert to the original version of Cisco CallManager by performing the following procedures: • Install the operating system by using the same server recovery method. • Install the version of Cisco CallManager that was running on your server before you attempted to upgrade. • Restore the Cisco CallManager data from the backup file. For more information, see the "Reverting to the Previous Configuration After an Upgrade Attempt" section on page 5-1.
You are upgrading Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION> which does NOT support the following features:· • Force Authorization Code and Client Matter Codes· • Call Block for Extension to Extension Transfer If you continue to upgrade, these features will no longer be available, and any associated data will be lost. Do you want to continue the upgrade process?	If you upgrade from 3.3(4) and above to 4.0(2), you will forfeit the listed features.	None. This is an informational message.

Table 6-1 Installation Error Messages (continued)

Error Message	Reason	Corrective Action
InsertCDR.exe – Application Error, The instruction at "0x10250fe7" referenced memory at "0x0000000". The memory could not be "read". Click OK to terminate program.	This is a harmless error message.	You should click OK to exit the dialog box and to continue with the installation of Cisco CallManager. Clicking OK does not terminate your installation; in fact, clicking OK will allow you to successfully upgrade your Cisco CallManager system.
The upgrade that you are attempting is not supported. To verify which versions of Cisco CallManager are compatible for upgrade, please refer to the Cisco CallManager Compatibility Matrix on CCO. The installation will now abort.	The version of Cisco CallManager that you are attempting to upgrade from is not supported.	Refer to *Cisco Compatibility Matrix* to review which versions are compatible for installation. To access the document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.

Resolving Name Resolution Failures

Cisco CallManager requires NetBIOS and IP name resolution. An incorrect WINS (NetBIOS) or DNS (IP) configuration could result in a service outage.

To resolve name resolution failures, consult with your network administrator to confirm NetBIOS and IP name resolution within the entire network, which includes local device IP configurations, local device name resolution (LMHOSTS and HOSTS), network-based name resolution systems (WINS and DNS) and DHCP systems.

Note Cisco recommends that you use either local or network-based name resolution and not both at the same time.

Note If you use local name resolution and you change the IP address of any server, you must update the LMHOSTS and HOSTS files of every affected server within the network accordingly. For the changes to take effect, either reboot each affected server or complete the tasks in Step 4.

Note If you use a network-based name resolution and you change the IP address of any server, you must update the WINS and DNS (including RARP) systems. For the changes to take effect, either reboot each affected server or complete the tasks in Step 4.

Procedure

Step 1 Obtain the IP address, hostname, and DNS suffix of each server in the cluster by using the *ipconfig /all* and *hostname* commands on each server.

Step 2 Populate the hosts files on each server in the cluster with the names and IP addresses of all servers in the cluster. Find the hosts files in c:\winnt\system32\drivers\etc.

The following example illustrates a hosts file where cm1 represents the hostname and mydomain.com represents the default DNS suffix or connection-specific DNS suffix from the ipconfig /all command output.

127.0.0.1 localhost
1.3.5.9 cm1 cm1.mydomain.com
1.2.4.8 cm2 cm2.mydomain.com

Step 3 Populate the lmhosts files on each server in the cluster with the names and IP addresses of all servers in the cluster. Find the lmhosts files in c:\winnt\system32\drivers\etc.

The following example illustrates a lmhosts file where cm1 represents the hostname.

1.3.5.9 cm1 #PRE
1.2.4.8 cm2 #PRE

Step 4 For the changes to take effect, issue the following commands on each server:

ipconfig /flushdns
nbtstat -R

Note Be aware that the letter "R" is case sensitive in the command.

Step 5 Confirm the changes were successfully loaded by performing the following procedures:

a. Examine the output of *nbtstat -c*

The names of all other servers in the cluster should appear with a life of -1. The names appear multiple times.

The following example represents the output of the nbtstat -c command:

Example 1 NetBIOS Remote Cache Name Table

Name		Type	Host Address	Life [sec]
CM2	<03>	UNIQUE	1.3.5.9	-1
CM2	<00>	UNIQUE	1.3.5.9	-1
CM2	<20>	UNIQUE	1.3.5.9	-1
CM1	<03>	UNIQUE	1.2.4.8	-1
CM1	<00>	UNIQUE	1.2.4.8	-1
CM1	<20>	UNIQUE	1.2.4.8	-1

b. Examine the output of *ipconfig /displaydns*. You should have at least one forward and one reverse entry for every server in the cluster. The following example contains two forward entries and two reverse entries per server.

Forward Entries

```
cm1.mydomain.com.
----------------------------------------------------
Record Name . . . . . : cm1.mydomain.com
Record Type . . . . . : 1
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . :
>                   1.2.4.8
```

```
cm1.
----------------------------------------------------
Record Name . . . . . : cm1
Record Type . . . . . : 1
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . :
>                     1.2.4.8
```

Reverse Entries

```
8.4.2.1.in-addr.arpa.
-----------------------------------------------------------
Record Name . . . . . : 8.4.2.1.in-addr.arpa
Record Type . . . . . : 12
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
PTR Record  . . . . . :
>                     cm1

Record Name . . . . . : 8.4.2.1.in-addr.arpa
Record Type . . . . . : 12
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
PTR Record  . . . . . :
cm1.mydomain.com
```

Disabling the Restrict CD-ROM Access to Locally Logged-On User Only Security Policy

If you receive the error message that the local security policy “Restrict CD-ROM access to locally logged-on user only” is enabled, you must disable the setting, reboot the server, and rerun the Cisco CallManager installation. Use the following procedure to disable the security policy.

Procedure

Step 1 To open the Local Security Policy utility, choose **Start > Programs > Administrative Tools > Local Security Policy**.

Step 2 Expand the Local Policies folder in the left pane and choose the Security Options folder.

Step 3 In the right pane, choose the **Restrict CD-ROM access to locally logged-on user only** policy and press **Enter**.

The Local Security Policy dialog box displays.

Step 4 Choose the **Disabled** radio button and click OK.

Step 5 Exit the Local Security Policy utility.

Step 6 Reboot the server.

Step 7 Restart the Cisco CallManager installation.

Replacing Servers During the Upgrade

This document assumes that Cisco CallManager is the only application that runs on the server. This document does not provide procedures for replacing coresident servers where Cisco CallManager, Cisco Customer Response Solutions (CRS), and Cisco-verified, third-party applications are installed on the same server.

By using these procedures, you can replace the publisher database server only, a subscriber server only, multiple subscriber servers, or both the publisher database server and the subscriber server(s) during the upgrade. Unless otherwise indicated in the document, remember to perform all procedures serially; that is, on one server at a time.

Caution These procedures cause call-processing interruptions. Cisco strongly recommends that you perform this procedure during a maintenance window. After you perform a backup, do not make any changes to the existing publisher database server that runs Cisco CallManager 3.2. Any changes that you make after a backup will not exist in the new database.

Replacing the Cisco CallManager 3.2 Publisher Database Server During the Cisco CallManager 4.0 Upgrade

Caution If you are replacing the publisher database server, you must perform the procedures for the new publisher database server on a physically isolated network (a dead net). See Step 15.

If you are performing installation procedures on a dead net, you must have network or media access to the backup file, MCS.sti file, or a tape drive and the tape if you originally backed up to a tape device. You must have network or media access to the Recovery folder and contents from the STI_DATA drive of the publisher database server. Before you start the Cisco CallManager installation, verify file access and DNS name resolution to the MCS.sti file in the dead net through the computer browser.

Procedure

Step 1 Perform Step 2 through Step 14 for the existing Cisco CallManager 3.2 publisher database server.

Performing Tasks on the Existing Cisco CallManager 3.2 Publisher Database Server (Required)

Step 2 Record all network configuration settings, including the computer name, network card speed and duplex settings, IP address, subnet mask, gateway, DNS, and WINS for the current system. Record the configuration of the servers in the existing cluster; record all software versions, Cisco CallManager services, coresident applications, and plug-ins, so you can reinstall them after the upgrade. Use Table 7-1 to record the information.

Table 7-1 Server Configuration Settings

Server Configuration Settings	Your Entry
Computer Name	
NIC Speed/Duplex settings	
IP Address	
Subnet Mask	
Default Gateway	
DNS Settings	
WINS Settings	
Cisco CallManager services (See Cisco CallManager Serviceability.)	
Coresident applications (Note the application type and version.)	
Cisco-verified, third-party applications (Note the application type and version.)	
Plug-ins from Cisco CallManager Administration	
Other Pertinent Information	

Step 3 If you are replacing a server with four drives, Cisco recommends that you set the trace directory path on the server to the default C: drive. Refer to *Cisco CallManager Serviceability Administration Guide.*

Step 4 Refer to the document, *Using the Cisco IP Telephony Applications Backup Utility Version 3.5.53* (or later), to perform the following tasks. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

a. Uninstall any prior versions of the backup utility; reboot the server when you are instructed to do so.

Note You cannot uninstall Cisco IP Telephony Applications Backup Utility version 3.5.6 if you installed the utility during the Cisco CallManager 3.2(3) installation.

b. Install and configure Cisco IP Telephony Applications Backup Utility Version 3.5.53 (or later) on the publisher database server.

c. Right-click the backup icon in the Windows 2000 system tray and back up the existing Cisco CallManager data.

Caution Make sure that you back up the data to a network directory or a local tape device. After you perform a backup, do not make any changes to the existing publisher database server that runs Cisco CallManager 3.2. Any changes that you make after a backup will not exist in the new database.

Caution If additional data besides Cisco CallManager data exists on the publisher database server, make sure that you back up the data before you continue with this procedure. Use the backup utility and documentation that applies to the application. This procedure does not outline migration of any data besides Cisco CallManager data. After you perform the Cisco CallManager upgrade, you must reinstall additional applications and restore the data by using the specified restoration procedures for the application.

Step 5 Copy the Recovery folder (with dbname.ini and backup.ini files) from the STI_DATA drive (usually the D:\Recover folder) to the network directory where the MCS.sti file (the backed up data) is stored. You can perform this task on a floppy drive.

Caution If these files do not exist on the server before the Cisco CallManager installation starts, the restoration of data fails.

Step 6 Copy the HOST and/or LMHOST files from C:\WINNT\SYSTEM32\DRIVERS\ETC to the network directory where the MCS.sti file (the backed up data) is stored. You can perform this task on a floppy drive.

Preparing the New Publisher Database Server

Step 7 Locate the disks for the Cisco-provided 2000.2.4 (or later) operating system.

Step 8 Power on the new publisher database server that has no data on it.

Step 9 Install the operating system by using the Cisco-provided disks and the document, *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.

Caution During the operating system installation, make sure that you choose the **New Installation or Server Replacement** option.

You must enter the exact computer name and network configuration information as the publisher database server that runs Cisco CallManager 3.2.

Do not join the new publisher database server to a Windows domain. Joining the domain causes the Cisco CallManager installation to fail.

During the operating system installation, check the **I am recovering a system from backup check box** (to ensure that the Recover flag is created in the STI_DATA drive).

Step 10 Use Cisco IP Telephony Server Operating System OS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.6. Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 11 Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 12 Download and install the latest OS-related security hotfixes, if any.

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 13 Copy the stored Recovery folder, including the dbname.ini and backup.ini files that exist on the network directory or floppy diskette, to the D: drive on the new publisher database server.

Step 14 Copy the Host and/or LMHOST files to C:\WINNT\SYSTEM32\DRIVERS\ETC on the publisher database server; reboot the server.

Step 15 Obtain the Cisco CallManager Installation, Upgrade, and Recovery Disks and the document, *Installing Cisco CallManager Release 4.0(2)*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

Step 16 Perform a Cisco CallManager 4.0 installation.

Caution Do not remove the disk unless the installation process or this document prompts you to do so. When a prompt asks, "The Same System Recovery flag was detected. Is this server being configured as a Cisco CallManager Publisher," click **Yes**.

Moving the New Publisher Database Server to the Live Network

Step 17 After the Cisco CallManager installation completes, power off the new publisher database server.

Step 18 Connect the new publisher database server to the production network.

Step 19 Power off the publisher database server that runs Cisco CallManager 3.2 and disconnect it from the network.

Step 20 Power up the new publisher database server on the production network.

Tip After you install Cisco CallManager on the server, verify that the new server behaves as expected. Review post-installation and post-upgrade tasks and perform the necessary tasks as you verify. To obtain the Cisco CallManager 4.0(2) installation document for post-installation tasks, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm. To review post-upgrade tasks, see the "Performing Post-Upgrade Tasks" section on page 4-1.

Replacing Cisco CallManager 3.2 Subscriber Server(s) During a Cisco CallManager 4.0 Upgrade

You must install Cisco CallManager on subscriber servers serially, that is, on one server at a time.

Caution If you are replacing the publisher database server and subscriber server(s), make sure that you have replaced the publisher database server first and that the data migrated and that services started as expected.

Perform these procedures on a live network with a live publisher database server.

Timesaver If you choose to do so, you may perform the operating system installation simultaneously on all new servers if the new hardware is not connected to the same network as the current system. Make sure that you install the operating system on a physically isolated network by using the procedures in this document. Installing the operating system in this manner saves you about 1 hour per server when you perform the actual hardware migration to the production network.

Tip After you install the first subscriber server, verify that the server and application behave as expected. If the server does not behave as expected, power off the live (new) publisher database server and the subscriber server, power on the publisher database server that runs Cisco CallManager 3.2, and rebuild the subscriber server to its original state. If this was a hardware replacement for the subscriber server, restore power to the old subscriber server.

After you install the second subscriber server and verify that it behaves as expected, you may experience call-processing interruptions if you choose to revert the cluster to the original state.

Procedure

Step 1 Record all network configuration settings, including the computer name, network card speed and duplex settings, IP address, subnet mask, gateway, DNS, and WINS for the current system. Record the configuration of the servers in the existing cluster; record all software versions, Cisco CallManager services, coresident applications, and plug-ins, so you can reinstall them after the upgrade. Use Table 7-1 to record the information.

Step 2 Power off the subscriber server that runs Cisco CallManager 3.2 and disconnect it from the network.

Step 3 Connect the new server to the network and power on the server.

Step 4 Using the Cisco-provided Operating System disks, install operating system 2000.2.4 (or later) on the new server that has no data on it.

Caution During the operating system installation, make sure that you choose the **New Installation or Server Replacement** option.

Do not check the I am recovering a system from backup check box.

Do not join the server to a Windows Domain during the operating system installation. Joining the domain causes the Cisco CallManager installation to fail.

Step 5 Use Cisco IP Telephony Server Operating System OS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.6. Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 6 Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2.6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 7 Download and install the latest OS-related security hotfixes, if any.

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 8 Using the Cisco CallManager Installation disks, perform a complete subscriber installation on the new server where you installed the operating system. Refer to the Cisco CallManager installation document for more information. Go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

Tip After you install Cisco CallManager on the server, verify that the new server behaves as expected. Review post-installation and post-upgrade tasks and perform the necessary tasks as you verify. To obtain the Cisco CallManager 4.0(2) installation document for post-installation tasks, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm. To review post-upgrade tasks, see the "Performing Post-Upgrade Tasks" section on page 4-1.

Replacing the Cisco CallManager 3.3 Publisher Database Server During the Cisco CallManager 4.0(2) Upgrade

Perform the following procedure:

Procedure

Step 1 Perform Step 2 through Step 6 for the existing Cisco CallManager 3.3 publisher database server.

Performing Tasks on the Existing Cisco CallManager 3.3(2) Publisher Database Server (Required)

Step 2 Record all network configuration settings, including the computer name, network card speed and duplex, IP address, subnet mask, gateway, DNS, and WINS for the current system. Record the configuration of the servers in the existing cluster; record all software versions, Cisco CallManager services, coresident applications, and plug-ins, so you can reinstall them after the upgrade. Record the information in Table 7-1.

Step 3 If you are replacing a server with four drives, Cisco recommends that you set the trace directory path on the server to the default C: drive. Refer to the *Cisco CallManager Serviceability Administration Guide*.

Step 4 Refer to the document, *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*, to perform the following tasks. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

a. Install and configure the Cisco IP Telephony Backup and Restore System (BARS) Version 4.0(1) (or later) on the publisher database server; reboot the server.

b. Back up the existing Cisco CallManager data.

Caution Make sure that you back up the data to a network directory or a local tape device.

After you perform a backup, do not make any changes to the existing publisher database server that runs Cisco CallManager 3.3. Any changes that you make after a backup will not exist in the new database.

Step 5 Copy the HOST and/or LMHOST files from C:\WINNT\SYSTEM32\DRIVERS\ETC to the network directory where the backed-up data is stored. You can perform this task on a floppy drive.

Step 6 Power off the Cisco CallManager 3.3 publisher database server and disconnect it from the network.

Preparing the New Publisher Database Server

Step 7 Connect the new server to the network and power on the server. By using the Cisco-provided operating system disks, install operating system version 2000.2.4 on the new publisher database server that has no data on it. To obtain the operating system documentation, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.

Caution During the operating system installation, make sure that you choose the New Installation or Server Replacement option. You must enter the exact computer name and network configuration information as the publisher database server that runs Cisco CallManager 3.3. Do not check the I am recovering a system from backup check box. Do not join the new publisher database server to a Windows domain. Joining the domain causes the Cisco CallManager installation to fail.

Step 8 Use Cisco IP Telephony Server Operating System OS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.6. Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 9 Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2.6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 10 Download and install the latest OS-related security hotfixes, if any.

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 11 Copy the HOST and/or LMHOST files to C:\WINNT\SYSTEM32\DRIVERS\ETC on the new publisher database server; reboot the server.

Step 12 Obtain the document, *Installing Cisco CallManager Release 3.3*. Go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm to obtain the most recent version.

Step 13 While you refer to the document, perform a Cisco CallManager 3.3 installation.

Step 14 Restore the backed-up data to the new publisher database server. To obtain the backup and restore utility documentation, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Tip Verify that the new server behaves as expected. Review post-installation and post-upgrade tasks and perform the necessary tasks as you verify. To obtain the Cisco CallManager 3.3 installation document for post-installation tasks, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

Step 15 Using this document, perform a Cisco CallManager 4.0(1) upgrade.

Tip Verify that the new server behaves as expected. Review and post-upgrade tasks and perform the necessary tasks as you verify. To review post-upgrade tasks, see the "Performing Post-Upgrade Tasks" section on page 4-1.

Replacing the Cisco CallManager 3.3 Subscriber Server(s) During the Cisco CallManager 4.0(2) Upgrade

You must install Cisco CallManager on subscriber servers serially, that is, on one server at a time.

Caution If you are replacing the publisher database server and subscriber server(s), make sure that you have replaced the publisher database server first and that the data migrated and services started as expected.

Perform these procedures on a live network with a live publisher database server.

Timesaver If you choose to do so, you may perform the operating system installation simultaneously on all new servers if the new hardware is not connected to the same network as the current system. Make sure that you install the operating system on a physically isolated network by using the procedures in this document. Installing the operating system in this manner saves you about 1 hour per server when you perform the actual hardware migration to the production network.

Tip After you install the first subscriber server, verify that the server and application behave as expected. If the server does not behave as expected, power off the live (new) publisher database server and the subscriber server, power on the publisher database server that runs Cisco CallManager 3.2, and rebuild the subscriber server to its original state. If this was a hardware replacement for the subscriber server, restore power to the old subscriber server.

After you install the second subscriber server and verify that it behaves as expected, you may experience call-processing interruptions if you choose to revert the cluster to the original state.

Procedure

Step 1 Record all network configuration settings, including the computer name, network card speed and duplex settings, IP address, subnet mask, gateway, DNS, and WINS for the current system. Record the configuration of the servers in the existing cluster; record all software versions, Cisco CallManager services, coresident applications, and plug-ins, so you can reinstall them after the upgrade. Use Table 7-1 to record the information.

Step 2 Power off the Cisco CallManager 3.3 subscriber server and disconnect it from the network.

Step 3 Connect the new server to the network and power on the server.

Step 4 Using the Cisco-provided Operating System disks, install operating system 2000.2.4 (or later) on the new server that has no data on it.

Caution During the operating system installation, make sure that you choose the **New Installation or Server Replacement** option.

Do not check the I am recovering a system from backup check box.

Do not join the server to a Windows Domain during the operating system installation. Joining the domain causes the Cisco CallManager installation to fail.

Step 5 Use Cisco IP Telephony Server Operating System OS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.6. Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 6 Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-6sr1 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 7 Download and install the latest OS-related security hotfixes, if any.

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates*, and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 8 Using the Cisco CallManager Installation disks, perform a complete subscriber installation on the new server where you installed the operating system. Refer to the Cisco CallManager installation document for more information. Go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

Tip After you install Cisco CallManager on the server, verify that the new server behaves as expected. Review post-installation and post-upgrade tasks and perform the necessary tasks as you verify. To obtain the Cisco CallManager 4.0(2) installation document for post-installation tasks, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm. To review post-upgrade tasks, see the "Performing Post-Upgrade Tasks" section on page 4-1.

Troubleshooting Hardware Replacements During Upgrades

If the server does not behave as expected, power off the live (new) publisher database server and the subscriber server, if applicable, power on the publisher database server that runs Cisco CallManager 3.2 or 3.3, and rebuild the subscriber server to its original state. If you replaced the subscriber server, restore power to the subscriber server that runs Cisco CallManager 3.2 or 3.3.