Using Cisco IP Telephony Applications Backup Utility, Version 3.5.44

Document Title Change

Use this document if you are searching for the following documents:

- *Using Cisco IP Telephony Applications Backup Utility, Version 3.5.6* (or 3.5.18)
- *Backing Up and Restoring Cisco CallManager Release 3.3*
- *Backing Up and Restoring Cisco CallManager Release 3.2*
- *Backing Up and Restoring Cisco CallManager Release 3.1*
- *Installing Cisco CallManager Release 3.0*

Purpose of the Document

This document provides information on the following topics:

- Installing and configuring the backup utility
- Modifying existing configuration settings
- Changing the purpose of the server from a backup server to a backup target
- Starting a backup immediately
- Restoring the Cisco CallManager cluster
- Restoring the publisher database server
- Restoring the subscriber server(s)
- Restoring the data that you backed up by using the backup utility
- Replacing the publisher database server or co-resident servers

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

Contents

This document contains the following topics:

Conventions

Consider the following documentation conventions as you review this document:

Blue Text—To quickly navigate to a section or URL, 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.

Cisco Customer Response Applications (CRA) and Cisco Customer Response Solutions (CRS) refer to the same product.

Cisco CDR Analysis and Reporting (CAR) and the Cisco Administrative Reporting Tool (ART) refer to the same product.

Locating Related Cisco CallManager Documentation

Cisco strongly recommends that you review the following documents before you perform any backup and restore procedures:

- *Release Notes for Cisco IP Telephony Applications Backup Utility, Version 3.5.44* (or later)

  This document provides a list of resolved and open caveats for this release of the utility.

- The appropriate Cisco IP telephony application documentation

  Locate the release notes, installation/upgrade, and configuration guides for the applications that you want to integrate 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
Backup and restore release note documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Operating system documentation and Virtual Network Computing (VNC) documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Cisco CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager documentation, including Cisco CAR documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager support patches	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Related Cisco CRS, Cisco Unity, and Cisco uOne documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
Cisco Integrated Communication System (ICS) 7750 documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/ics/index.htm

Note If you need Cisco CallManager installation and backup/restore information for the Cisco Integrated Communication System (ICS) 7750, refer to the installation and configuration guide for the Cisco ICS documentation.

Frequently Asked Questions About the Cisco IP Telephony Applications Backup Utility

Review the following questions and responses before configuring or performing the backup.

Which Cisco IP telephony applications use this backup utility?

This utility supports the following applications:

- Cisco CallManager
- Cisco Customer Response Solutions (CRS)
- Cisco CDR Analysis and Reporting (CAR)
- Cisco Emergency Responder

Note This utility does not back up Cisco Unity or Cisco uOne data. To obtain Cisco Unity documentation, see Table 1. For more information on backing up Cisco uOne, see the backup and restore release notes for 3.5.44. To obtain the release notes, see Table 1.

Which versions of the applications does this utility support?

Cisco IP Telephony Applications Backup Utility 3.5.44 supports the following Cisco CallManager releases, which serve as minimum requirements:

- Cisco CallManager 3.3(2) or later
- All releases of Cisco CallManager 3.2
- All releases of Cisco CallManager 3.1
- All releases of Cisco CallManager 3.0
- All CRA/CRS and Cisco CAR releases that are compatible with Cisco CallManager

  To obtain compatibility information on CRA/CRS and Cisco CAR, refer to the *Cisco CallManager Compatibility Matrix*. To obtain the *Cisco CallManager Compatibility Matrix*, see Table 1.

Which version of the utility runs on my system?

The Add/Remove Programs window displays the version of the utility that runs on your system. Perform the following procedure to identify the version:

Procedure

Step 1 Right-click the backup icon in the Windows 2000 system tray.

Tip If the backup icon does not display in the Windows 2000 system tray, choose **Start > Programs > Cisco IP Telephony Applications Backup > Backup Configuration**.

Step 2 Choose **About Backup**.

How do I obtain the backup utility?

You can obtain the backup utility from the web or from the CD-ROM that may ship with the supported application. To obtain the latest backup utility, always download it from the web. The version that is available on the CD-ROM may not provide the latest utility.

See the "Using the Backup Utility" section on page 14 for utility installation procedures.

How do I obtain release notes for this utility?

The release notes document contains resolved/known issues and workarounds that apply to this version of the utility. To obtain the document, click the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm

If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats for this utility. To use the Bug Toolkit, click http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl

When do I install the utility?

Cisco strongly recommends that you install the utility before you install the supported Cisco IP telephony application.

You should upgrade the utility as later versions become available on the web; always verify that you have the latest utility installed on the backup server before you perform an application upgrade. Before the application upgrade, always back up the data to a network directory or tape device. If you store the data on the local directory, the application upgrade may overwrite the data.

May I use Terminal Services, Virtual Network Computing (VNC), or Integrated Lights Out (ILO) to install/upgrade the utility?

Do not use Terminal Services to install/upgrade the utility.

To eliminate remote access to the server during the installation/upgrade, Cisco recommends that you disable Terminal Services before the utility installation/upgrade and reboot the server. You must enable Terminal Services after the installation/upgrade.

If you want to use Virtual Network Computing (VNC) to remotely install supported applications, see Table 1 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 installation, disable it to prevent remote access to the server. If you do not disable VNC and a user/administrator accesses the server during the installation, the utility installation will fail.

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

Do I need to disable services and applications before the utility installation/upgrade?

Cisco recommends that you disable all Cisco-verified, third party applications before the utility installation or upgrade. Failing to do so could interrupt the installation.

The following platform agents may interfere with the installation/upgrade: antivirus services, intrusion detection services, OEM server agents, server management agents, and 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.

If you installed Cisco IDS Sensor Host Agents on the server, locate the corresponding product documentation for procedures on disabling and stopping the services.

Caution To eliminate remote access to the server during the installation/upgrade, Cisco recommends that you disable Terminal Services before the utility installation/upgrade and reboot the server. You must enable Terminal Services after the installation/upgrade.

Do not use Terminal Services to install/upgrade the utility.

Before the installation/upgrade, Cisco strongly recommends that you disable all services that allow remote access to the server. You must manually enable the service after the installation/upgrade.

How does the Cisco IP Telephony Applications Backup Utility work?

The Cisco IP Telephony Applications Backup Utility provides a reliable and convenient way to perform regularly scheduled automatic or user-invoked backups of your data.

About the Backup Server

The backup server actually performs the backup operation and the following tasks:

- Saves all backup utility settings
- Verifies authentication information that you provide during the configuration of the backup
- Backs up the data that you choose
- Stores the backup data in the backup destination that you specify
- Creates separate logs for the backup utility

Caution Although any server in the Cisco CallManager cluster can act as the backup server, Cisco recommends that you designate the publisher database server as the backup server.

To successfully back up the Cisco CallManager database, the backup server and target(s) must exist in the same cluster and have the same version of the backup utility installed.

About the Target Server(s)

The target server contains the data to be backed up; that is, data for Cisco CallManager, CAR, or CRS.

When you add a target server to the backup server, make sure that you enter the computer name (not the IP address or the fully qualified DNS name).

If the target server is a remote server, you must provide a user name and password that has administrative privileges to the remote server.

Caution Verify that the backup target(s) and backup server have the same version of the backup utility installed. Verify that the backup target(s) and backup server exist in the same cluster.

Verify that the same version of the Microsoft SQL Server database exists on the backup server and all backup targets. The backup fails if the same version does not run on the server.

Caution If the backup server and backup targets are not running and functional, the backup fails. Verify that all corresponding services, such as DC Directory, are running before you perform the backup. If the services are not running, the backup fails.

About Authentication

The utility installation prompts you for a BackAdmin Private Password Phrase. The installation uses the string that you enter to create a unique, encrypted password. You must enter the same phrase on the backup server and all backup targets.

When you choose a target server, the utility prompts you for the backup server computer name. The utility verifies that you entered the correct computer name for the backup server.

If the passwords do not match or if the utility cannot verify the passwords, you receive a warning message that asks whether you want to proceed. If you proceed and the passwords do not match, an error displays in the log file.

Caution Administrator and BackAdmin passwords must match on the backup server and the backup target. BackAdmin passwords synchronize during the backup utility installation because servers have the same private phrase. Synchronizing the administrator passwords ensures a successful configuration, backup, or restoration.

If the administrator passwords are different on the backup server and the backup target(s), the backup fails because the backup server cannot authenticate the backup target.

About Backup Data and the MCS.sti File

The Cisco CallManager publisher database contains all the information that you configure with Cisco CallManager Administration, and the database updates each time that you make a change. Cisco CallManager updates the directory, and configuration information also updates periodically. Cisco strongly recommends that you make a backup of the Cisco CallManager database, configuration, and directory information by using the Cisco IP Telephony Applications Backup Utility every time that you make changes through Cisco CallManager Administration.

Each Cisco CallManager cluster has only one publisher database, and you do not need to back up the subscriber database servers.

However, you can configure the Cisco IP Telephony Applications Backup Utility to back up more than one Cisco IP Telephony Applications Server, such as publishing database servers of other Cisco CallManager clusters, Cisco uOne servers, or Cisco Customer Response Solutions (CRS/CRA) servers.

During the backup, the utility sends the data to a staging directory, and by default, one file called MCS.sti archives all data that is backed up from the target servers in the target list.

Caution Each time that a backup is performed, the new backup file overwrites the existing MCS.sti file. If you want to retain previous backup data, you must archive or rename the existing MCS.sti file before the next backup is performed.

About the Staging Directory

The staging directory serves as a temporary directory where the backup utility places all files until it builds the single MCS.sti file.

Caution During the backup, heed warnings about the amount of temporary space that is available on the staging directory. If you do not have enough temporary space on the staging directory, the backup will fail.

About the Schedule

In the Schedule tab, you configure the day and time that you want the backup to run.

Cisco sets a default schedule for when the backup is to run. You can change the schedule at any time.

The utility backs up all data at the same time. You cannot configure a separate schedule for each application.

About the Location Where the Data is Stored (Destination)

For the backup destination, Cisco strongly recommends that you specify a tape drive or a network directory, not a local 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**.

If you choose to back up the data to a network directory, that server must have NETBIOS name resolution (use computer name) in place (not the IP address or the fully qualified DNS name).

About the Log File

The backup process creates the log file, stiBack.log, under C:\Program Files\Common Files\Cisco\Logs on the backup server. All errors that occur during the configuration or while the utility is running write to this file.

During the backup configuration, you can specify the number of days that you want to retain the log files.

See the "Reviewing Error Messages and Contacting Technical Support" section on page 28.

About the Backup Icon in the Windows 2000 System Tray

Figure 1 shows the backup icon that displays in the Windows 2000 system tray.

Figure 1 Backup Icon

When you right-click the backup icon in the Windows 2000 System tray, you can initiate the following tasks:

- View status of the backup utility as it runs.
- Configure backup settings.
- Catalog the backup files.

This option creates a catalog that lists the files that the utility backed up and compressed into the MCS.sti file.

- Access the restoration utility.
- Pause/restart the backup service.
- Start a backup now.
- Learn which version of the backup utility is installed.
- Exit the viewer.

Which server should I designate as the backup server?

See the "How does the Cisco IP Telephony Applications Backup Utility work?" section on page 7.

What if I forgot to choose a backup server when I installed Cisco CallManager?

If you did not designate a backup server during the installation, the backup utility cannot run. See "Using the Backup Utility" to learn how to install the backup server.

Can I change the purpose of the server?

You can change a backup server to a backup target, or vice versa, but you must uninstall the version and then reinstall the utility on the server; you can then specify the purpose by clicking the backup server or backup target radio button during the installation. If you change a backup target to the backup server, you must configure the backup settings on the backup server. If you change the backup server to a backup target, be aware that you must choose and configure another backup server for the utility to run.

Caution If you want to change the purpose of the publisher database server after a Cisco CallManager 3.3 upgrade, you should upgrade to a later version of the utility and configure it appropriately. You cannot uninstall the version that exists after the initial 3.3 upgrade.

What data does the Cisco IP Telephony Applications Backup Utility back up?

Caution The Cisco IP Telephony Applications Backup Utility does not back up any operating system files except for Host/LMhost, if these files exist on the server.

If you configure the backup settings as instructed in this document, the backup utility automatically backs up the information that displays in Table 2:

Table 2 Data Choices

Check Box	Data Backed Up
Cisco CallManager	The utility backs up the following data: • Cisco CallManager publisher database • DC Directory database **Note** This utility does not back up the Microsoft Active Directory or Netscape Directory Server database. • TFTP files from C:\Program Files\Cisco\TFTPPath (the default path) • TFTP files on subscriber servers that are configured as backup targets • Cisco Bulk Administration Tool (BAT) files • Cisco Call Detail Records (CDRs) • Registry keys **Note** This utility does not back up Cisco Multilevel Administration (MLA). Refer to the Cisco MLA documentation for information on how to back up that data.

Table 2 Data Choices (continued)

Check Box	Data Backed Up
Cisco Customer Response Applications (CRA)/(CRS)	**Note** This utility does not back up Cisco TAPS. The utility backs up the following data, depending on the release: **All versions of CRA** • CRA configuration file - Ccndir.ini • Files from C:\Program Files\Wfavvid, including Workflows (.aef), Java (.java), Jar (.jar), Properties (.properties), and .WAV (.wav) **CRA Release 3.0 and later** Files from C:\Program Files\Wfavvid, including XML (.xml), Class(.class), WAR (.war), GSL (.gsl), and Digit (.digit), JobRunner.ini, Cfg files (.CFG) from C:\Program Files\Common, Cfg files (.CFG) from C:\Program Files\Desktop, .GSL/.wav and .Digit from user and system grammar paths, databases DB_CRA, DB_CRA_CCDR, SCHEDULERDB, database FCRASSVR (if ICD is installed) **CRA Release 3.1 and later (CRS server)** • All files in "All versions of CRA" and "CRA Release 3.0 and later" • System DSN dsn_cra_hrdb • If ICD is installed, C:\Program Files\Cisco\Desktop_AudioFiles **CRA Release 3.1 and later (RDB server)** • LMHosts file and Hosts file • Databases - db_cra, db_cra_ccdr • SQL jobs belonging to category 'CRS-RemoteDB Synchronization' **CRA Release 3.1 and later (VOIP and Record server)** • C:\Program Files\Cisco\Desktop_Audio Files • CFG files (*.CFG) from C:\program Files\Cisco\Desktop
CDR Analysis and Reporting (CAR)	The utility backs up the following data: • CAR (ART) database • C:\Ciscowebs\ART\reports\Pregenerated • Registry keys

May I use any backup utility that I want?

Cisco strongly recommends that you use the Cisco IP Telephony Applications Backup Utility to perform backups. If you do not want to use the Cisco IP Telephony Applications Backup Utility, you can uninstall it after the installation or disable it, depending on how your server is set up. Cisco does not support any other backup utility with these Cisco IP telephony applications.

Caution Some application installations require that the utility serve as a mandatory component on the server. For example, the initial upgrade to Cisco CallManager 3.3 requires that the utility remain on the publisher database server after the upgrade; therefore, the utility name does not display in the Add/Remove Programs window, and you cannot uninstall it.

If you want to change the purpose of the publisher database server, for example, you should upgrade to a later version of the utility and configure it appropriately.

To uninstall the utility, perform the following procedure:

Procedure to Uninstall the Utility

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

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

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

If the application requires that the utility serve as a mandatory component on the server, the utility name does not display in the window. You cannot uninstall the utility, so close the window.

Step 4 Click **Remove**.

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

To disable the Cisco IP Telephony Applications Backup service, perform the following procedure:

Procedure to Disable the Cisco IP Telephony Applications Backup Service

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

Step 2 Locate the service named **Cisco IP Telephony Applications Backup**.

Step 3 Right-click the service and choose **Properties**.

Step 4 Click **Stop** to immediately terminate the service.

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

Choosing this option prevents the service from automatically starting after the server reboots.

Step 6 Click **OK**.

Do I need to manually uninstall the backup utility before I upgrade it?

If you run a backup utility that is earlier than 3.5, you must manually uninstall the utility before you upgrade to the latest utility. See the "Procedure to Uninstall the Utility" section on page 13 to remove the utility.

Caution If you want to change the purpose of the publisher database server after a Cisco CallManager 3.3 upgrade, you should upgrade to a later version of the utility and configure it appropriately. You cannot uninstall the version that exists after the initial 3.3 upgrade.

If you installed Cisco CallManager 3.1 or 3.2 in the cluster, you can uninstall Cisco IP Telephony Applications Backup Utility, Version 3.5.44, on any servers where the utility is installed. If you choose to upgrade to Cisco CallManager 3.3, you must install this version of the utility, or a later version, if available, before you can upgrade. Refer to the Cisco CallManager 3.3 upgrade documentation for more information.

If I upgrade my utility, do I need to reconfigure the backup settings?

Each time that you upgrade the utility, you must reconfigure the backup settings.

Where do I obtain the log file?

The backup process creates the log file, stiBack.log, under C:\Program Files\Common Files\Cisco\Logs on the backup server. In the log file, you can search for the words, "failed" or "fatal error," which indicate that the backup did not work properly. To review a list of error messages that could display in the log file, see Table 5.

Caution During the backup, heed warnings about the amount of temporary space that is available on the staging directory. If you do not have enough temporary space, the backup will fail. Do not run a backup if you receive these warnings.

Always verify that the backup completed successfully.

Using the Backup Utility

Determine which of the following tasks you need to perform and see the corresponding section:

- Installing and Upgrading the Utility/Changing the Purpose of the Server, page 15
- Configuring Backup Settings on the Backup Server, page 17
- Starting a Backup Now, page 21
- Viewing the Backup As It Occurs, page 21

Installing and Upgrading the Utility/Changing the Purpose of the Server

Tip If you are upgrading the utility or changing the purpose of the server, Cisco recommends that you uninstall the existing utility before you proceed.

Changing the purpose of the server requires a reinstallation of the backup utility.

Procedure

Step 1 Perform one of the following tasks:

a. If you are currently installing Cisco CallManager and the Backup Utility Setup window automatically displays, go to Step 2.

b. If you have a backup utility disk and the publisher database server is functional and running, insert the disk into the disk drive. Then, go to Step 2.

c. To install the backup utility from the web, click the following URL:

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

Note You must have a Cisco Connection Online (CCO) username and password to obtain the utility from the web.

d. Choose **The Application** (for example, Cisco CallManager) > **Download...Cryptographic Software... > Download Cisco 3DES Cryptographic Software under export licensing controls.**

e. Locate the backup and restore file on the page that displays.

f. Download the backup and restore file to your hard drive.

g. Note the location where you save the downloaded file.

h. Double-click the downloaded file to begin the installation.

Caution You may receive a message that a previous version of the utility was detected. Continue the installation.

Step 2 When the Welcome window displays, click **Next**.

Step 3 Click the appropriate radio button to accept the license agreement. Click **Next**.

Step 4 Perform the following procedure from Table 3, depending on whether you want to install the backup server or backup target.

Table 3 Choosing Backup Server or Backup Target

Backup Server	Backup Target
Click **Backup Server**. The backup server actually performs the backup operation. It stores the backup data in the directory or tape drive destination that you specify. You specify one backup server.	Click **Backup Target**. The backup target(s) designates a server (source) that contains the data that the utility will back up. You can specify more than one backup target; to configure backup settings, you must add all backup targets to the CallManager targets list on the backup server.
Click **Next**.	Enter the computer name for the backup server.
Go to Step 5.	Click **Next**.

Step 5 Enter the BackAdmin Private Password Phrase; enter the phrase again in the Confirm Password field. Click **Next**.

Step 6 Click the version of Cisco CallManager that you have installed in the cluster. Click **Next**.

Step 7 To install the backup utility, click **Install**.

The status bar indicates the progression of the installation.

Click **Cancel**.

Step 8 Click **Yes**.

Step 9 Click **Finish**.

Step 10 Click **Yes** to restart the server.

Tip After the server reboots and the system is running, verify that the backup and restore icon displays in the Windows 2000 system tray.

After the server reboots, you can remove the disk from the disk drive and log in to the server by using the Administrator password.

Step 11 Go to the "Configuring Backup Settings on the Backup Server" section on page 17.

Note You must add CallManager (CallManager, CRA, or CAR) targets to the backup server. You must also configure the destination, which is the location where you plan to store the data, and the schedule, which specifies the days and time when you want to run the utility.

Configuring Backup Settings on the Backup Server

To modify existing or configure new backup settings, perform the following procedure:

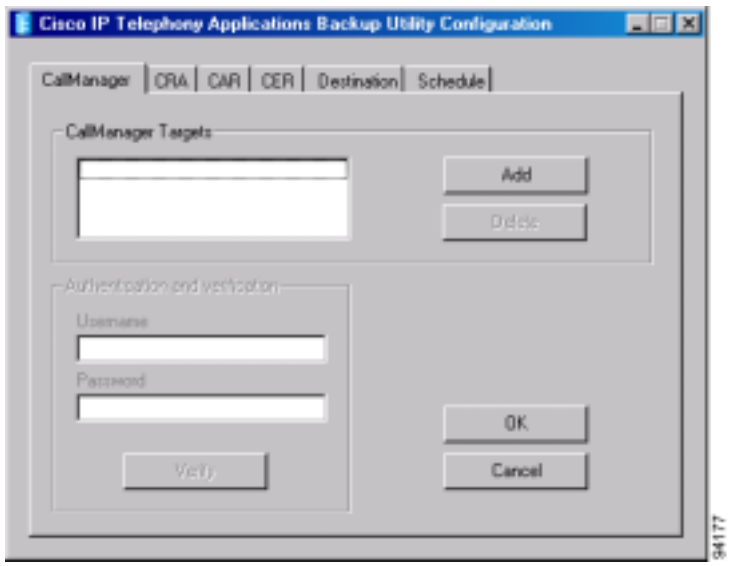
Procedure

Step 1 If the window in Figure 2 does not automatically display on the backup server, perform one of the following actions:

- Right-click the backup icon in the Windows 2000 system tray. Choose **Configure Settings**.
- If the backup icon does not display in the Windows 2000 system tray, choose **Start > Programs > Cisco IP Telephony Applications Backup > Backup Configuration**.

  If the backup is running, an error message states that you should right-click the backup icon in the Window 2000 system tray.

Figure 2 CallManager Tab



Step 2 Verify that the servers that are listed in the CallManager Targets pane are the ones that you want to include. These target servers contain data that you want to back up through the utility.

If you are configuring the backup utility for Cisco CallManager, remember that you must add all backup target servers to the CallManager Targets list. If necessary, perform the following procedure to add a target:

a. Add targets by clicking **Add**.

To add a remote target, you must connect the server to the network before you add it to the target list.

b. In the dialog box that displays, enter the name of the target server.

When you add a target server to the backup server, you must enter the computer name (not the IP address or fully qualified DNS name).

c. If the server is a remote target, enter a username and password with administrator access rights on the remote server and then click **Verify**.

The Backup Utility attempts to connect to the remote server. If the remote server is not found, the authentication fails.

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

e. If you are running Cisco CallManager Release 3.3, you can check the **Include Database** check box for the CDR Database option. This option does not apply for Cisco CallManager Release 3.1 or 3.2.

f. In the lower, right corner of the window, click **OK**.

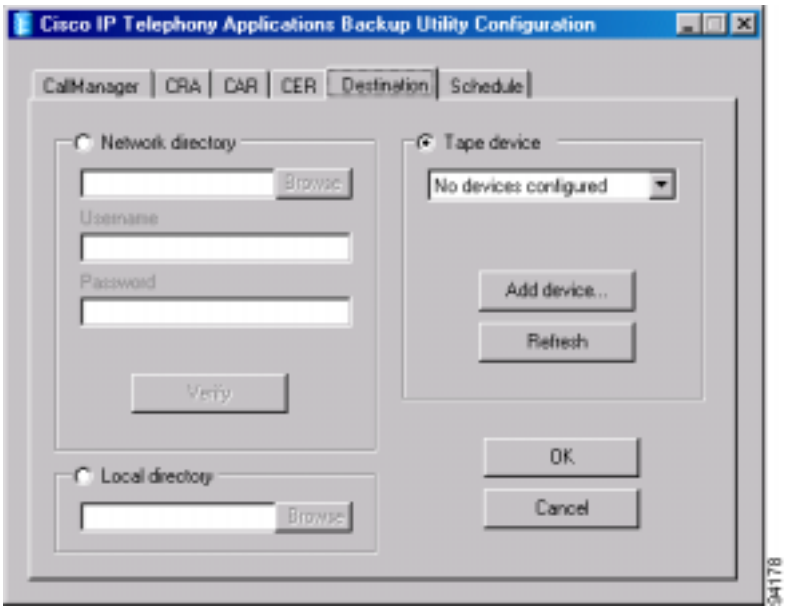
Tip To remove servers from the target list, highlight the server, click **Delete** and then click **OK**.

Step 3 Click the **CRA** (Cisco Customer Response Applications) or **CAR** (Cisco CDR Analysis and Reporting) tab and repeat Step 2 to configure the backup for CRA, or CAR.

Caution This information applies if you are performing a Cisco CallManager 3.3 upgrade from a 3.1 or 3.2 version of Cisco CallManager. If you have installed CAR on the publisher database server, verify that you have added the publisher database server name (not IP address or fully qualified DNS name) to the CallManager and CAR target lists. Use the same naming conventions in each list, so the restore utility can restore CAR database during the Cisco CallManager data restoration.

Figure 3 shows an example of the Destination tab in the Cisco IP Telephony Applications Backup Utility. Cisco allows you to configure only one destination for all applications that use the backup utility.

Figure 3 Destination Tab



Step 4 Click the **Destination** tab. Perform one of the following tasks, depending on the location where you want to store the data:

Choosing a Network directory

Step 5 Click the Network directory radio button.

Step 6 Click the **Browse** button and browse to the location where you want to store the data.

Step 7 Enter a username and password that has administrative privileges on the server and click **Verify**.

Step 8 Click **OK**, and skip to Step 17.

Choosing a Tape device

Step 9 Click the Tape device radio button.

Tip You may click the Tape device radio button only if you have the MCS-7835, MCS-7845-1400, IBM xSeries 340, or xSeries 342 server. The server must have a tape drive.

If you plan to restore data from one server to another server by using a tape drive, make sure that both servers use the same tape format.

Step 10 From the drop-down list box, choose the tape device where you want to store the data.

Step 11 To add or uninstall a tape drive, click the Add device button and follow the prompts in the wizard.

Step 12 To refresh the device list after you add a device, click Refresh.

Step 13 Click **OK** and skip to Step 17.

Choosing the Local directory

Caution Cisco recommends that you choose a network directory or tape device.

Step 14 Click the Local directory radio button.

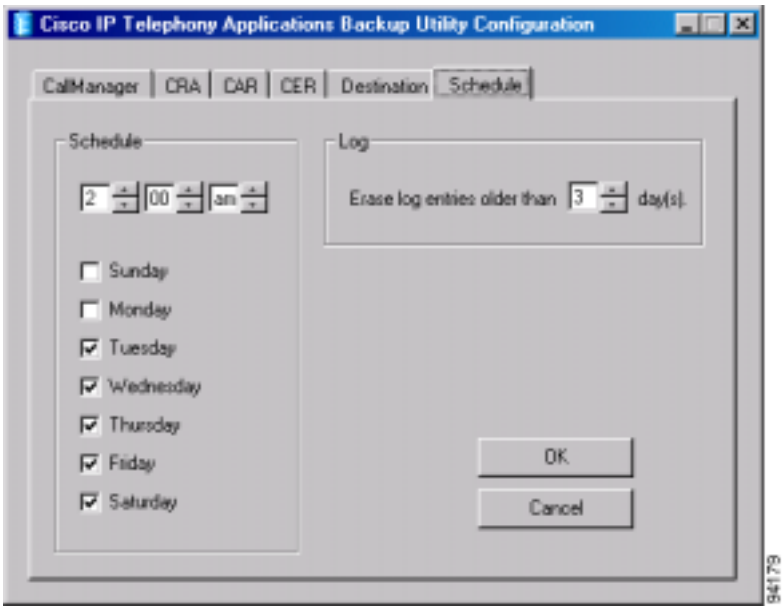
Step 15 Click the Browse button and browse to the location where you want to store the data.

Step 16 Click **OK**.

Figure 4 shows an example of the Schedule tab in the Cisco IP Telephony Applications Backup Utility Configuration window. Cisco only allows you to schedule the same days and time for all applications that use the backup utility. The backup utility backs up all affected applications during the scheduled time.

Caution Schedule Cisco CallManager backups to occur during off-peak hours because CPU utilization is high during the backup process.

Figure 4 Schedule Tab



Step 17 Click the **Schedule** tab. Choose the days and times when you want an automatic backup to occur. The default sets the backup time to 2:00 am Tuesday through Saturday. Click **OK**.

Step 18 From the drop-down list box in the Log pane, choose the number of days that you want to retain log entries.

Step 19 Click **OK** to save the settings.

Step 20 If you did not reboot the server after you installed the utility, you must reboot the server now.

If the disk remains in the disk drive, you can remove the disk from the disk drive after the server reboots; then, you can log in to the server by using the Administrator password.

Starting a Backup Now

Backups occur automatically according to the settings in the Schedule window of the Cisco IP Telephony Applications Backup Utility; if you want to start a backup now, perform the following procedure:

Procedure

Step 1 Verify that the Cisco IP Telephony Applications Backup service is running in the Services window. If this service is not running, the backup fails.

Step 2 Right-click the Cisco IP Telephony Applications Backup Utility icon in the Windows 2000 system tray.

Step 3 Choose **Start backup now**.

Step 4 In the window that displays, click the **Start Backup** button.

Tip After the backup completes, the last line indicates that the backup completed successfully.

Viewing the Backup As It Occurs

Perform the following procedure:

Procedure

Step 1 In the Windows 2000 system tray on the backup server, click the Cisco IP Telephony Applications Backup Utility icon and choose **View status**.

Step 2 If the Cisco IP Telephony Applications Backup Utility icon is not in the Windows 2000 system tray, choose **Start > Programs > Cisco IP Telephony Applications Backup > Backup Viewer**; then, click the Cisco IP Telephony Applications Backup Utility icon in the Windows 2000 system tray and choose **View status**.

Step 3 Verify that the current status is “Waiting until <time> on <date>.” You can keep this log window open to view the progress of the backup utility.

Step 4 Use the information that is generated in the log window to help identify problems. The last line in the log file indicates that the log is closed.

To obtain the log file, see the “Where do I obtain the log file?” section on page 14.

Frequently Asked Questions About the Cisco IP Telephony Applications Restore Utility

Review the following questions and responses before you perform any Cisco CallManager restoration procedures:

How does the Cisco IP Telephony Applications Restore Utility work?

You use the Cisco IP Telephony Applications Restore Utility to restore data to the server of your choice. The restoration takes the system back to the state in which it was when it was backed up. The utility does not restore the application files; therefore, you must install the application before the restoration occurs.

The utility does not provide prompts to restore servers or the entire cluster. You must perform a manual procedure to restore or replace a server.

Note You cannot perform a backup and a restoration at the same time.

Before I perform the restoration, do I need to reinstall the backup utility that created the MCS.sti file?

You can restore the data with the backup utility that currently runs on your system.

If you created the MCS.sti file with a different version of the backup utility and you now need to restore that file, defects from the previous version of the utility may cause errors to display in the current log file.

Complete the restoration and verify that the data restored properly.

How do I restore the data?

Caution If you browse to the network directory, you must manually highlight the MCS.sti file to restore the data.

Caution For a successful recovery, make sure that the version of Cisco CallManager that is running on your system matches the last successful backup. Cisco does not migrate data during the restoration.

The Cisco IP Telephony Application Restore Utility allows you to recover all data, if you chose to back up the data through the backup utility. When you restore, you must provide the following information:

- The location (server) where the archived MCS.sti file is stored
- The data, the MCS.sti file, that you want restored
- The server where you want the restore utility to send the restored data
- Authentication information for remote servers

By default, the MCS.sti file stores all data that was backed up from the target servers in the target list. When you restore data, you can restore only one application on one server at a time. For example, if you need to restore Cisco CallManager and CRA/CRS on a co-resident server, you must perform the procedure twice.

The restore utility copies the data that you want restored to a staging directory and then restores the extracted files to the chosen location. The restore utility also notifies the user when the restoration occurs.

Caution During the restoration, services stop, and call-processing interruptions occur.

Cisco recommends that you use the restore utility during a single maintenance window to minimize call-processing interruptions.

This section provides the procedure for restoring the data. This procedure does not restore the operating system, Cisco CallManager software, or any other software. To restore the data, perform the following steps:

Procedure

Step 1 Perform one of the following tasks. Two options exist for Cisco CallManager Release 3.2 and 3.3.

- For Cisco CallManager Releases 3.1, 3.2, or 3.3—Choose **Start > Programs > Cisco IP Telephony Applications Backup > Restore Utility**.
- For Cisco CallManager Releases 3.2 or 3.3—Right-click the backup icon in the Windows 2000 system tray and choose **Restore server**.

Step 2 When the Restore Utility window displays, choose the location and name of the backup file that you want to restore and then click **Next**.

Caution If you browse to the network directory, you must manually highlight the MCS.sti file to restore the data.

If you are restoring a remote server, you must verify the authentication by providing a username and password for the remote server. When you authenticate successfully, a message displays; click OK.

Step 3 Choose the target server, which is the server where you want the utility to send the data. Click **Next**.

Step 4 The restoration warns that you will overwrite the target server and lose all existing data on that server. Click **Yes**.

Step 5 During the restore process, the Cisco IP Telephony Applications Restore Utility log window displays each event that occurs.

Step 6 You must enter the password for the SA account on the publisher database server. Click **OK**.

Step 7 You must enter the authentication information (administrator password and SA password) for all subscriber servers in the cluster. Click **OK**.

Tip The last line in the window indicates that the restoration completed successfully for the server.

You can use the log window to identify errors, such as the errors that display in the "Where do I obtain the log file for the restoration?" section on page 24.

Step 8 When the restore is complete, click **OK**.

Step 9 Reboot the server.

Step 10 After you log in to the server by using the Administrator password, verify that the restored data is on the server.

Where do I obtain the log file for the restoration?

The restoration process creates the log file, stiRestore, under C:\Program Files\Common Files\Cisco\Logs. To review error messages that could display in the log file, see Table 5.

How do I restore the entire cluster?

Caution All pre-/post-installation tasks that are noted in the Cisco CallManager installation and upgrade documents apply to restoring the cluster. Review the guidelines before you begin any restoration procedures.

If you must restore the entire cluster because of an unforeseen event, consider the following information. As with new installations, always restore the publisher database server first. See Table 4 for information on how to accomplish this task. After you restore the publisher database server, verify that you successfully completed the restoration.

While the publisher database server is functional and running, you can begin the restoration of the subscriber server(s). See "How do I restore subscriber servers?" for more information. Always restore one server at a time, so database replication occurs on the subscriber servers. If you attempt to restore the subscriber servers simultaneously, the servers cannot pull the database replica from the publisher database server.

After you restore the Cisco CallManager servers, you can restore other application servers, such as CRA or Cisco uOne servers.

Caution Cisco strongly recommends that you do not change any passwords when you are restoring/replacing the server or cluster. The restoration process restores the previously backed up passwords, does not acknowledge the new passwords, and causes the system to malfunction.

If you change the Directory Manager password when you are restoring/replacing the server or cluster, the server cannot access the directory.

How do I restore the publisher database server?

Use the following guidelines in Table 4 to restore the publisher database server:

:

Table 4 Restoring the Publisher Database Server

Step	Task	Important Notes
Step 1	Perform a new operating system installation or Same Server Recovery by installing Cisco-provided operating system 2000.2.4 or later.	Refer to *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of the document, see Table 1.
Step 2	Perform a new Cisco CallManager installation from disk. **Caution** If you are installing Cisco CallManager Release 3.2 or 3.1, do not install the backup utility during the installation. Instead, install the utility by downloading the utility that is available on the web.	Refer to the Cisco CallManager installation documentation that matches the version that you plan to install. To obtain this document, see Table 1.
Step 3	The Cisco CallManager version that is running on the publisher database server must match the version of the latest successful backup. If necessary, upgrade Cisco CallManager to the version of the latest successful backup.	Refer to the Cisco CallManager upgrade documentation that matches the version of the latest successful backup.
Step 4	Manually restore the latest successful backup (MCS.sti file) to the publisher database server.	See the "How do I restore the data?" section on page 22.
Step 5	Verify that you successfully restored the data.	You can obtain StiRestore.log by using Windows Explorer to browse to the following file: C:\Program Files\Common Files\Cisco\Logs For a list of error messages that could display, see the "Reviewing Error Messages and Contacting Technical Support" section on page 28.
Step 6	If you backed up CAR, you must install the CAR plugin on the server.	Refer to the *Cisco CallManager Administration Guide*.

How do I restore subscriber servers?

Cisco no longer requires that you remove the subscriber server from the Cisco CallManager database before recovering the server. When the subscriber server authenticates to the publisher database server and pulls the duplicate of the database from the server, the subscriber server automatically adds itself to the database.

Use the following guidelines to restore the subscriber server(s):

1. Perform a new installation of Cisco-provided operating system 2000.2.4 or later.
2. Perform a new installation of Cisco CallManager.

   You do not need to restore the data.
3. Upgrade the server to match the version of Cisco CallManager that is running on the publisher database server.
4. See the "What post-restoration tasks should I perform?" section on page 26.

How do I restore a CRA server?

Use the following guidelines to restore these application servers:

1. Make sure that you have restored the Cisco CallManager servers/data before you restore these application servers.
2. Install the operating system on the server, if it is not already installed.

   Co-resident servers (Cisco CallManager and CRA/CRS installed on the same server) may already have the operating system installed.
3. Install the application as if it were a new installation.
4. Upgrade the application to the version of the backup that you want to restore, if necessary.
5. Restore the backup data to the new server.

   To restore the data, Cisco recommends that you have backup data stored on tape device or on a network directory, not on the local directory of the failed server.
6. Verify that the data was restored to the new server.
7. See the "What post-restoration tasks should I perform?" section on page 26.

What post-restoration tasks should I perform?

Perform the following post-restoration tasks:

- For the restoration to take effect, make sure that you reboot the server after you restore the data.
- Verify that no errors occurred during the restoration.
- If necessary, reinstall the Cisco IP telephony applications/products/plugins/support patches to the version that is compatible with the restored version of Cisco CallManager. Refer to the *Cisco CallManager Compatibility Matrix* for more information. To obtain the most recent version of this document, see Table 1.
- To obtain the locales that were used prior to the restoration, reinstall the Cisco IP Telephony Locale Installer. To obtain locale installer documentation, see Table 1.

How do I replace an existing or a failed publisher database server or co-resident server?

Tip If you are upgrading to Cisco CallManager 3.3(3), you can replace the publisher database server while you upgrade. Refer to *Upgrading Cisco CallManager Release 3.3(3)* for more information. To obtain the most recent version of this document, see Table 1.Cisco does not support replacing co-resident servers during upgrades.

Tip When you perform a server replacement, you must always manually enter the IP information, computer name, and other configuration data exactly as it was on the original server.

Before you begin, locate the configuration information for this server.

To replace an existing or failed server, use the following guidelines:

1. Install the operating system and the software as if it were a new installation.
2. Upgrade the application to the version of the backup that you want to restore.
3. Restore the backup data to the new server.

   To restore the data, you must have backup data stored on tape or on a network directory, not on the local directory of the existing or failed server.
4. Verify that the data was restored to the new server.
5. See the "What post-restoration tasks should I perform?" section on page 26.

Reviewing Error Messages and Contacting Technical Support

Table 5 provides the error messages that could display in the log file or in dialog boxes.

Table 5 Backup and Restore Utility Error Messages

Error Message	Reason	Corrective Action
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.
Fatal Error - Could not authenticate to server_name\C$ as User_Name. Skipping target.	You entered incorrect authentication information during the configuration, or the server is not available at this time	Verify whether the authentication information that you entered during the configuration is correct and whether the target server is available. Repeat the backup.
Could not find the Remote Command service running on server_name.	The remote target does not have the the Remote Command service on the remote target; therefore, the data may not back up correctly.	From the Services window, start the Remote Command service on the remote target. Repeat the backup.
Fatal Error - SQL Server does not appear to be installed on server_name. Skipping backup of SQL Server.	The utility specifies that the SQL Server is not installed or is not available; the utility will not back up the database.	Verify that SQL Server is correctly installed on the backup target. If it is installed correctly, restart the SQL Server on the backup target and repeat the backup.
Fatal Error - Could not find a CallManager database on server_name.	The utility did not back up the Cisco CallManager database.	Verify that the <server_name> is a valid Cisco CallManager machine and that database ccm030x exists. If these items exist, verify the administrator and sa passwords that you provided during the backup utility configuration for this server. Repeat the backup.
Could not verify database backup successfully	The utility identified that the database backup is corrupt.	Repeat the backup.
Failed to copy files from C:\program Files\Cisco\CallDetail\CDR	The utility did not successfully back up the CDR flat files.	Repeat the backup.
Failed to copy files from C:\program Files\Cisco\CallDetail\CMR	The utility did not successfully back up the CDR flat files.	Repeat the backup.

Table 5 Backup and Restore Utility Error Messages (continued)

Error Message	Reason	Corrective Action
Failed to determine the path for CDR flat files. Skipping CDR file backup.	The utility could not determine the value of "Local CDR path," the path where CDR flat files are created.	Verify that SQL Server is running on the backup target. Verify that you configured the enterprise parameter, "Local CDR path." Repeat the backup.
Fatal Error - Could not backup DC Directory database.	The DC Directory backup failed.	Verify whether DC Directory is installed and whether the service "DC Directory server" currently runs on the backup target. Restart the service and repeat the backup.
Fatal Error - No CallManager components were found on server_name. Nothing was backed up.	The utility did not back up the Cisco CallManager database or DC Directory.	Verify that the Cisco CallManager installation has SQL Server and DC Directory installed. In Services window, verify that Cisco services are running; then, repeat the backup.
Failed to back up TFTPPath folder successfully.	You may not have enough space on the backup server.	Verify that space is available on the backup server. Repeat the backup.
Fatal Error - Could not find CAR SQL database on server_name.	You did not provide a valid server_name, or database ART does not exist on the server.	Verify that the <server_name> is a valid CAR machine and that the database ART exists. If these items exist, verify the administrator and sa passwords that you provided during the backup configuration for this server.
SQL Server does not appear to be installed on the server.	SQL Server does not exist on the server, and you cannot back up the database.	Verify that SQL Server installed correctly on the backup target. If it is installed correctly, restart SQL Server on the backup target, and repeat the backup.
Fatal Error - Failed to backup <folder>	The utility detects that the folder does not exist.	Verify that this folder exists. If the folder exists, repeat the backup.
Could not authenticate to server_name\C$ as User_Name. Skipping target.	You entered incorrect authentication information during the configuration, or the server is not available at this time.	Verify whether the authentication information that you entered during the configuration is correct and whether the target server is available. Repeat the process.

Table 5 Backup and Restore Utility Error Messages (continued)

Error Message	Reason	Corrective Action
The Cisco CallManager archive appears to be version 3.0 whereas the Cisco CallManager version being installed is 3.3. This upgrade is not allowed.	You cannot upgrade from Cisco CallManager 3.0 to Cisco CallManager 3.3.	You must upgrade to the latest version of Cisco CallManager Release 3.1 or 3.2 before you upgrade to Cisco CallManager Release 3.3.
Fatal Error - Database db_name on server server_name was not restored.	The utility did not restore the stored database. This catastrophic error indicates that the utility will not recover the data in the SQL Server database.	Repeat the restoration.
Fatal Error - Could not recreate publication on server_name.	The utility could not republish the Cisco CallManager database on the publisher database server.	Repeat the restoration.
Fatal Error - Could not recreate publication. Missing publishing information from archive.	Replication information does not exist in the stored backup file. The backup file appears corrupt.	Repeat the restoration.
Failed to determine the path for CDR flat files. Skipping CDR file restore.	The utility could not determine the value of "Local CDR path," the path where CDR flat files are created.	Verify that SQL Server runs on the backup target. Verify that you configured the enterprise parameter "Local CDR path." Repeat the restoration.
Fatal Error - Failed to restore the SQL database and DC Directory. Please repeat the restore process.	The utility could not restore the SQL Server database or the DC Directory.	Repeat the restoration.
Fatal Error - Failed to restore DC Directory.	The utility could not restore DC Directory.	Repeat the restoration.
CAR/CRA does not appear to be installed on server_name. You need to install CAR/CRA in order to restore data.	These applications do not exist on the server.	Install the application.
Fatal Error - Could not find dump file for CAR/CRA database from server_name.	The utility will not restore this database because the backup utility could not back up the database.	You may have a corrupt backup file. If you retained previous versions of the MCS.sti file, obtain an archived MCS.sti file and perform the restoration again.
Fatal Error - Could not find Version.ini in the staging directory.	The utility does not extract the .ini file from the MCS.sti file.	You may have a corrupt backup. Verify that the MCS.sti file is valid.
Fatal Error - Could not find reg.dmp in the staging directory	You may have a corrupt backup.	You may have a corrupt backup. The utility will not restore the registry information.

Table 5 Backup and Restore Utility Error Messages (continued)

Error Message	Reason	Corrective Action
Fatal Error - Could not connect to the subscribers. Publication may fail.	The login to the subscriber server failed.	Verify the replication status.
Fatal Error - Failed to drop the database from the server.	The utility failed to delete the database. The restoration fails because the utility cannot restore the backed-up database.	Repeat restoration.
Fatal Error - Could not recreate the publication on the server.	The publication failed on the publisher database server.	Repeat restoration.
Fatal Error - Could not recreate the subscription on the subscriber	Subscriptions did not get created. No replication occurred.	Verify that the subscribers are online and that the administrative passwords are synchronized. Repeat the restoration.
Fatal Error - Database cannot be restored on the server	The restoration fails because problems occurred while the utility attempted to restore the backed-up database.	Repeat restoration.
Fatal Error - Could not find <directory> in the staging directory	The utility did not back up the files/directories.	The restore utility will not restore the files.

If you need to contact technical support (your Cisco AVVID partner or the Cisco Technical Assistance Center), be prepared to provide logs that are located within the following directories:

- C:*.log
- C:*.txt
- C:\Winnt\sti*.*
- C:\dcdsrvr\log*.*
- C:\Install\DBInstall*.*
- C:\Program Files\Common Files\Cisco\Logs*.*

In addition to the logs, obtain the version of Cisco CallManager, the backup utility, and all third-party applications that are installed in the cluster.

For more information on obtaining technical assistance, see the "Obtaining Technical Assistance" section on page 33.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

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 Networking Products MarketPlace:

  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, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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, Inc.
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.

- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing 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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

---