

CIPT1

Cisco IP Telephony Part 1

Volume 1

Version 4.1

Student Guide

CLS Production Services: 08.18.05

Copyright Ó 2005, Cisco Systems, Inc. All rights reserved.

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece
Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania
Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland
Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

 Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Volume 1

<i>Course Introduction</i>	1
Overview	1
Learner Skills and Knowledge	1
Course Goal and Objectives	3
Course Flow	4
Additional References	5
Cisco Glossary of Terms	6
Your Training Curriculum	7
<i>Getting Started with Cisco CallManager</i>	1-1
Overview	1-1
Module Objectives	1-1
<i>Introducing Cisco CallManager</i>	1-3
Overview	1-3
Objectives	1-3
Cisco AVVID	1-4
Cisco CallManager Functions	1-5
Example: Basic IP Telephony Call	1-7
Cisco CallManager Operating System, Database, and Supporting Applications	1-8
Cisco CallManager Servers	1-9
Installation CD-ROMs	1-10
Installation Configuration Data	1-11
Example: Configuration Data Worksheet	1-13
Postinstallation Procedures	1-15
Activating Cisco CallManager Services	1-17
Upgrading Prior Cisco CallManager Versions	1-20
Summary	1-21
References	1-22
<i>Identifying Cisco CallManager Cluster and Deployment Options</i>	1-23
Overview	1-23
Objectives	1-23
Microsoft SQL Cluster Relationship	1-25
Intracenter Communication	1-27
Cluster Redundancy Designs	1-28
Call-Processing Deployment Models	1-30
Single-Site Deployment	1-31
Multisite WAN with Centralized Call Processing	1-34
Multisite WAN with Distributed Call Processing	1-36
Clustering over the IP WAN	1-39
Summary	1-41
References	1-42
Module 1 Summary	1-43
Module 1 Self-Check	1-44
Module 1 Self-Check Answer Key	1-46
<i>Establishing an On-Cluster Call</i>	2-1
Overview	2-1
Module Objectives	2-1
<i>Identifying Cisco IP Telephony Endpoints</i>	2-3
Overview	2-3
Objectives	2-3
Cisco IP Phone Overview	2-4
Entry-Level Cisco IP Phones	2-5

Midrange and Upper-End Cisco IP Phones	2-7
Additional Cisco IP Telephony Endpoints	2-9
IP Phone Startup Process	2-11
Cisco IP Phone Codec Support	2-13
Summary	2-14
References	2-15
Configuring Cisco CallManager to Support IP Phones	2-17
Overview	2-17
Objectives	2-17
Server Configuration	2-18
Configuring Device Pools	2-19
Example: Device Pool Configuration	2-20
Example: Cisco CallManager Group Configuration	2-22
Example: Region Configuration	2-24
IP Phone Button Templates	2-26
Example: Naming a Phone Button Template	2-27
Manual IP Phone and Directory Number Configuration	2-28
Configuring IP Phone Auto-Registration	2-30
Summary	2-33
References	2-33
Configuring Cisco Catalyst Switches	2-35
Overview	2-35
Objectives	2-35
Catalyst Switch Role in IP Telephony	2-36
Powering the Cisco IP Phone	2-37
Types of PoE Delivery	2-38
Catalyst Family of PoE Switches	2-41
Configuring PoE	2-43
Configuring Dual VLANs	2-45
Configuring Class of Service	2-50
Summary	2-52
References	2-53
Configuring Cisco IP Communicator	2-55
Overview	2-55
Objectives	2-55
Cisco IP Communicator Overview	2-56
Cisco IP Communicator Installation and Configuration Overview	2-59
Configuring Cisco CallManager for Cisco IP Communicator	2-60
Deploying and Updating Cisco IP Communicator	2-61
Postinstallation Configuration Tasks	2-64
Summary	2-65
References	2-66
Using the Bulk Administration Tool	2-67
Overview	2-67
Objectives	2-67
Introducing the Bulk Administration Tool	2-68
Installing BAT	2-72
Using the BAT Wizard	2-74
Configuring BAT Templates	2-78
Creating CSV Files	2-81
Validating Data Input Files	2-85
Inserting IP Phones into Cisco CallManager	2-86
Updating IP Phones with BAT	2-87
Using the Tool for Auto-Registered Phone Support	2-89
Summary	2-93
References	2-94
Module 2 Summary	2-95
Module 2 Self-Check	2-96
Module 2 Self-Check Answer Key	2-100

Course Introduction

Overview

Cisco IP Telephony Part 1 (CIPT1) v4.1 prepares you for installing, configuring, and maintaining a Cisco IP telephony solution. This course focuses primarily on Cisco CallManager, the call routing and signaling component for the Cisco IP telephony solution. This course includes lab activities in which you will perform postinstallation tasks and configure Cisco CallManager; configure gateways, gatekeepers, and switches; and build route plans to place intra- and intercluster Cisco IP Phone calls. You will also configure telephony class of service (calling restrictions) and numerous user telephone features, services, media resources, and applications.

Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should complete to benefit fully from this course.

Learner Skills and Knowledge

Cisco.com

Skill or Knowledge	Cisco Learning Offering
Working knowledge of fundamental terms and concepts of computer networking, to include LANs, WANs, and IP switching and routing	<i>Interconnecting Cisco Network Devices (ICND)</i> Cisco CCNA® certification recommended prerequisite
Ability to configure and operate Cisco routers and switches and to enable VLANs and DHCP	<i>Building Cisco Multilayer Switched Networks (BCMSN)</i>
Fundamental knowledge of converged voice and data networks Ability to configure voice interfaces on Cisco voice-enabled equipment for connection to traditional, nonpacketized telephony equipment and to configure the call flows for POTS and VoIP dial peers	<i>Cisco Voice over IP (CVOICE)</i>

Course Goal and Objectives

This topic describes the course goal and objectives.

Course Goal

Cisco.com

“To prepare learners to install, configure, and maintain a Cisco IP telephony solution. The course focuses on the Cisco CallManager, which is the call routing and signaling component for the Cisco IP telephony solution.”

Cisco IP Telephony Part 1

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1—4

Upon completing this course, you will be able to meet these objectives:

- n Deploy a Cisco CallManager server in a cluster by using a supported IP telephony deployment model
- n Configure Cisco CallManager and the Cisco Catalyst switch to enable on-cluster calls and add users, phones, and Cisco IP Communicator to the Cisco CallManager database using manual configuration, auto-registration, or BAT
- n Configure Cisco gateways and intercluster trunks, create hunt groups, and create a route plan in Cisco CallManager to enable calling to remote clusters so that the WAN is not oversubscribed, calls are preserved if the WAN fails, and user calling restrictions are in place
- n Configure Cisco CallManager to enable features and services, including conferencing, music on hold (MOH), speed dials, Call Park, Call Pickup, Cisco Call Back, Barge, Privacy, Cisco IP Phone Services, Cisco CallManager Extension Mobility, Cisco CallManager Attendant Console, and Cisco IP Manager Assistant (IPMA) and also use these features on Cisco IP Phones
- n Configure Cisco CallManager and the client PC to enable Cisco CallManager Attendant Console and Cisco IPMA

Course Flow

This topic presents the suggested flow of the course materials.

		Course Flow				
		Cisco.com				
		Day 1	Day 2	Day 3	Day 4	Day 5
A	M	Course Introduction	Establishing an On-Cluster Call	Establishing an Off-Cluster Call	Establishing an Off-Cluster Call	Enabling Features and Services
		Getting Started with Cisco CallManager			Enabling Features and Services	Configuring Cisco CallManager Applications
Lunch						
P	M	Establishing an On-Cluster Call	Establishing an On-Cluster Call	Establishing an Off-Cluster Call	Enabling Features and Services	Configuring Cisco CallManager Applications
			Establishing an Off-Cluster Call			Wrap-Up

© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1-5

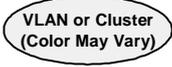
The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

This topic presents the Cisco icons and symbols used in this course, as well as information on where to find additional technical references.

Course Icons and Symbols

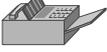
Cisco.com

	Router		Cisco CallManager		File Server
	Voice Router		Traditional PBX		LDAP Directory Server
	SRST-Enabled Router		Phone		Relational Database
	Switch Router		IP Phone		Digital Signal Processor
	Switch		Gateway		VLAN or Cluster (Color May Vary)
	Voice Multilayer Switch		PSTN CO Switch		

© 2005 Cisco Systems, Inc. All rights reserved.
CIPT1 v4.1-6

Course Icons and Symbols (Cont.)

Cisco.com

	PC		WAN		Camera PC/Video
	Printer		Telecommuter		Digital Certificate
	Fax		Mobile User		
	Laptop		Building		
	Videoconference		Building		
	Video Camera				

© 2005 Cisco Systems, Inc. All rights reserved.
CIPT1 v4.1-7

Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>.

Your Training Curriculum

This topic presents the training curriculum of this course.

Cisco Voice Career Certifications

Cisco.com

**Expand Your Professional Options
and Advance Your Career**

Cisco Voice Career Certifications

Professional-level recognition in Cisco Voice Career Certifications



Required Exam	Recommended Training Through Cisco Learning Partners
Gateway Gatekeeper	Implementing Cisco Voice Gateways and Gatekeepers
IPTT 642-425	IP Telephony Troubleshooting (IPTT)
QOS 642-642	Implementing Cisco Quality of Service (QoS)
GIPT 642-444	Cisco IP Telephony Part 1 Cisco IP Telephony Part 2
CVOICE 642-432	Cisco Voice Over IP

© 2005 Cisco Systems, Inc. All rights reserved. <http://www.cisco.com/go/certifications> 12 v4.1-1

You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE[®], CCNA[®], CCDA[®], CCNP[®], CCDP[®], CCIP[®], CCVP[™], or CCSP[™]). It provides a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit www.cisco.com/go/certifications.

Module 1

Getting Started with Cisco CallManager

Overview

Cisco CallManager is the software-based, call-processing component of the Cisco IP telephony solution. This module discusses the servers that Cisco CallManager supports, explores the available deployment models for using Cisco CallManager in a Cisco IP telephony solution, and reviews the Cisco CallManager server installation process.

Module Objectives

Upon completing this module, you will be able to deploy a Cisco CallManager server in a cluster using a supported IP telephony deployment model. This ability includes being able to meet these objectives:

- n Identify the functions that Cisco CallManager provides in the overall Cisco AVVID strategy and identify the hardware, software, and tasks required for a Cisco CallManager installation
- n Determine the optimum Cisco CallManager cluster option and IP telephony deployment model for your enterprise

Lesson 1-1

Introducing Cisco CallManager

Overview

A Cisco IP telephony deployment relies on Cisco CallManager for its call-processing and call-routing functions. Understanding the role that Cisco CallManager plays in a converged network from a system, software, and hardware perspective is necessary to successfully install and configure Cisco CallManager.

This lesson discusses the Cisco Architecture for Voice, Video and Integrated Data (AVVID) and Cisco CallManager functions, hardware requirements, software requirements, and installation and upgrade information.

Objectives

Upon completing this lesson, you will be able to identify the functions that Cisco CallManager provides in the overall Cisco AVVID strategy and identify the hardware, software, and tasks required for a Cisco CallManager installation.

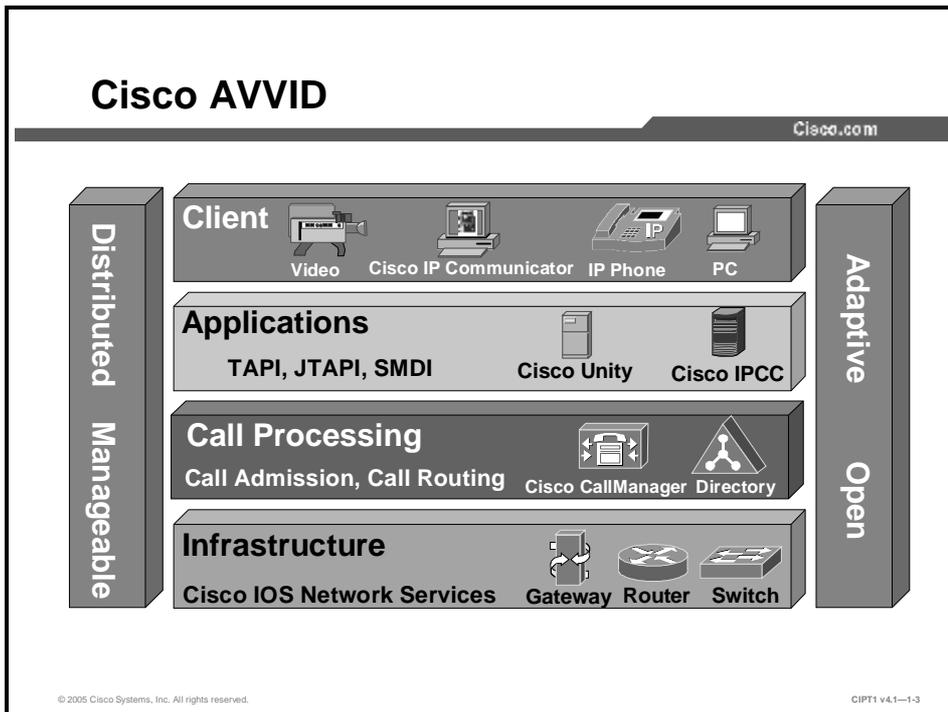
This ability includes being able to meet these objectives:

- n Describe the purpose and key components of each Cisco AVVID layer
- n Identify the primary Cisco CallManager functions
- n Identify the software that Cisco CallManager depends upon for its operating system, database, directory, and backup
- n Identify the major features of each base platform on which Cisco CallManager Release 4.1 is supported
- n Identify the Cisco CallManager CDs that are required for installation
- n Identify all configuration data that is required to install Cisco CallManager software
- n Perform postinstallation procedures to help secure the server and optimize server resources

- n Activate Cisco CallManager services
- n Identify the supported versions of Cisco CallManager required to upgrade to release 4.1

Cisco AVVID

This topic describes the purpose and key components of each Cisco AVVID layer.



Cisco AVVID provides the foundation for converged networks. The Cisco AVVID strategy encompasses voice, video, and data traffic within a single network infrastructure. Cisco AVVID equipment is capable of managing all three traffic types and interfacing with all standards-based network protocols in each network class.

This figure shows the four standard layers of the Cisco AVVID voice infrastructure model: the infrastructure layer, which lays the foundation for network components; the call-processing layer, which maintains PBX-like functions; the applications layer, where applications that provide additional network functionality reside; and the client layer, where end-user devices reside. The key points about the four standard layers are as follows:

- n **Infrastructure layer:** The infrastructure carries data between all network devices and applications and consists of routers, switches, and voice gateways.
- n **Call-processing layer:** Call processing is physically independent of the infrastructure. Thus, a Cisco CallManager in Chicago can process call control for a bearer channel in Phoenix.
- n **Applications layer:** Applications are physically independent of call-processing functions and the physical voice-processing infrastructure; that is, they may reside anywhere within the network.
- n **Client layer:** The client layer brings applications to the user, whether the end device is a Cisco IP Phone, a PC using a Cisco IP Communicator, or a PC delivering converged messaging.

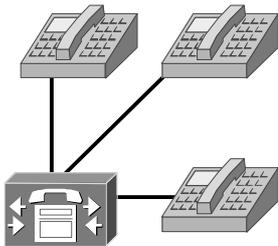
Cisco CallManager Functions

This topic describes the primary Cisco CallManager functions within the Cisco IP telephony solution.

Cisco CallManager Functions

Cisco.com

- **Call processing**
- **Signaling and device control**
- **Dial plan administration**
- **Phone feature administration**
- **Directory services**
- **Programming interface to external applications**



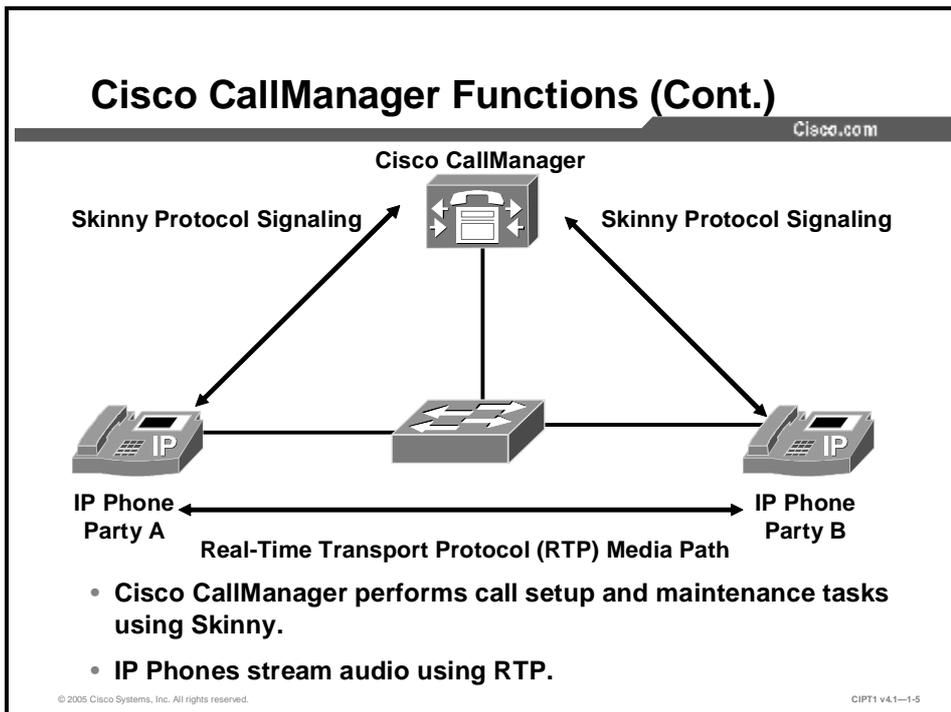
© 2004 Cisco Systems, Inc. All rights reserved. Course acronym vx.x--#-6

Cisco CallManager extends enterprise telephony features and functions to packet telephony network devices. These network devices include Cisco IP Phones, media-processing devices, voice over IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as converged messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact with the IP telephony solution through the Cisco CallManager application programming interface (API).

Cisco CallManager provides the following functions:

- n **Call processing:** Call processing refers to the complete process of routing, originating, and terminating calls, including any billing and statistical collection processes.
- n **Signaling and device control:** Cisco CallManager sets up all of the signaling connections between call endpoints and directs devices such as phones, gateways, and conference bridges to establish and tear down streaming connections.
- n **Dial plan administration:** The dial plan is a set of configurable lists that Cisco CallManager uses to determine call routing. Cisco CallManager provides the ability to create secure dial plans for users.
- n **Phone feature administration:** Cisco CallManager extends services such as hold, transfer, forward, conference, speed dial, last-number redial, Call Park, and other features to IP Phones and gateways.

- n **Directory services:** Cisco CallManager uses DC-Directory as an embedded Lightweight Directory Access Protocol (LDAP) directory. This directory stores authentication and authorization information about users and is a standard feature of Cisco CallManager (it does not require any special configuration or installation). However, Cisco CallManager can also be integrated with a corporate LDAP directory.
- n **Programming interface to external applications:** Cisco CallManager provides a programming interface to external applications such as Cisco IP SoftPhone, Cisco IP Interactive Voice Response (IVR), Cisco Personal Assistant, and Cisco CallManager Attendant Console.



Cisco CallManager use the Skinny Client Control Protocol (SCCP, or Skinny) signaling protocol over IP to communicate with Cisco IP Phones for call setup and maintenance tasks. When the call is set up, Cisco IP Phones communicate directly using Real-Time Transport Protocol (RTP) to carry the audio.

You can better understand how Cisco CallManager performs key functions by tracking a basic IP telephony call.

Example: Basic IP Telephony Call

In the figure shown, Party A (left telephone) wants to call Party B (right telephone). Party A picks up the handset and dials the number of Party B. In this environment, dialed digits are sent to Cisco CallManager, the call-processing engine. Cisco CallManager finds the address and determines where to route the call.

Using the Skinny protocol, Cisco CallManager signals the calling party over IP to initiate a ring back, and Party A hears ringing. Cisco CallManager also signals the destination phone to initiate ringing.

When Party B picks up the telephone, the RTP media path opens between the two stations. Party A or Party B may now initiate a conversation.

The IP Phones require no further communication with Cisco CallManager until either Party A or Party B invokes a feature, such as call transfer, call conferencing, or call termination.

Cisco CallManager Operating System, Database, and Supporting Applications

This topic identifies key software on which Cisco CallManager depends.

Operating System, Database, and Applications

Cisco.com

- **Windows 2000 Server**
- **Microsoft SQL Server 2000**
- **DC-Directory**
- **Cisco IP Telephony Backup and Restore System**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1-1-6

Cisco CallManager server relies on Microsoft Windows 2000 for its operating system and Microsoft Structured Query Language (SQL) Server 2000 for its database (both provided by Cisco Systems). The operating system version that Cisco provides is called the Cisco IP Telephony Operating System. Cisco CallManager 4.1(2) requires Cisco IP Telephony Operating System Version 2000.2.6 (or later) and the latest Cisco IP Telephony Server Operating System service release (2000-2-6 sr3 or later). Cisco CallManager 4.1(3) requires Cisco IP Telephony Operating System Version 2000.2.7 (or later) and the latest service release (2000-2-7 sr2 or later).

Cisco CallManager uses DC-Directory as an embedded LDAP directory. This directory stores authentication and authorization information about users and is standard with Cisco CallManager (it does not require any special configuration or installation). Authentication establishes the right of the user to access the system, while authorization identifies the telephony resources that a user is permitted to use, such as a specific telephone extension.

The Cisco Customer Directory Plugin allows you to integrate Cisco CallManager with one of the following enterprise directories:

- n Microsoft Active Directory, available with Microsoft Windows 2000
- n Microsoft Active Directory, available with Microsoft Windows 2003
- n Netscape Directory Server, Versions 4.1 and 4.2,
- n Sun ONE Directory Server 5.x

The Cisco IP Telephony Backup and Restore System (BARS) can be used to back up Cisco CallManager. Cisco BARS is installed separately from Cisco CallManager.

Cisco CallManager Servers

This topic describes the major features of the supported server hardware platforms for Cisco CallManager Release 4.1.

Cisco 7800 Series MCS					
Cisco.com					
Platform	Space	Processor	CPU Equipped	CPU Max.	Max. Phones Per Cluster
MCS 7815-H1	Tower	Pentium 4 3060 MHz	1	1	300
MCS 7825-H1	1U Rack Mount	Pentium 4 3400 MHz	1	1	1000
MCS 7835-H1	2U Rack Mount	Nocona Xeon 3400 MHz	1	2	2500
MCS 7845-H1	2U Rack Mount	Nocona Xeon 3400 MHz	2	2	7500
MCS 7825-H1	1U Rack Mount	Pentium 4 3400 MHz	1	1	1000
MCS 7835-H1	2U Rack Mount	Nocona Xeon 3400 MHz	1	2	2500
MCS 7845-H1	2U Rack Mount	Nocona Xeon 3400 MHz	2	2	7500



© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1-1-7

Because voice networks should maintain an uptime of 99.999 percent, you must install Cisco CallManager on a server that meets Cisco configuration standards. For this reason, Cisco has collaborated with two server hardware manufacturers, Hewlett-Packard and IBM, to create Cisco Media Convergence Servers (MCSs). Hewlett-Packard and IBM designed these server hardware platforms specifically for Cisco voice applications.

All of these servers are rack-mountable and do not include a monitor, mouse, or keyboard. Cisco designed the Cisco MCS for local setup, rack mounting, and remote administration.

For a list of servers on which Cisco CallManager 4.1 is supported, refer to the Cisco CallManager 4.1 data sheet at:

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_data_sheet0900aecd801979f0.html.

Installation CD-ROMs

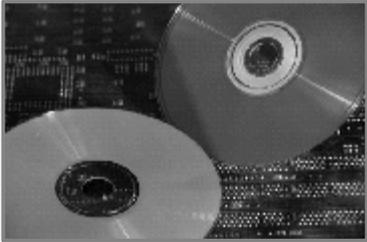
This topic identifies the CD-ROMs that you must use to install a Cisco CallManager server.

Installation Disks

Cisco.com

Disks essential for new Cisco CallManager 4.1 installation:

- **Hardware Detection**
- **Cisco CallManager Installation, Upgrade, and Recovery**
- **Cisco CallManager 4.1 Software**



Cisco CallManager 4.1 upgrade software can be downloaded from Cisco.com or ordered on DVD/CD (includes Cisco CallManager software only, does not include operating system)

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1—1-8

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

- n **Cisco IP Telephony Server Operating System Hardware Detection Disk:** Checks the server and displays an error message if it detects an unsupported server. After you boot the server using the Hardware Detection CD-ROM, the automated installation process prompts for the correct CD-ROMs to use.
- n **Cisco IP Telephony Server Operating System Installation and Recovery Disk:** Installs the operating system. Use only one of the server-specific Cisco IP Telephony Server Operating System Installation and Recovery disks that come in your software kit. During the operating system installation, a prompt instructs you to insert the appropriate disk into the drive.
- n **Cisco CallManager 4.1 Software Disk:** This disk installs the Cisco CallManager application on the server.

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

Installation Configuration Data

This topic describes the configuration data that you will need when installing a Cisco CallManager server.

Configuration Information

Cisco.com

- **New installation or server replacement**
- **Cisco product key**
- **Username and organization name**
- **Computer name**
- **Workgroup**
- **Domain suffix**
- **TCP/IP properties**
- **Domain Name System**
- **SNMP community string**
- **Database server**
- **Password for system administrator**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1-1-9

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

The process erases all data on the server hard disk. During the installation, you are prompted for the following items:

- n **New installation or server replacement:** Choose this option if you are installing the Cisco IP telephony application for the first time, overwriting an existing installation, or replacing a server. To replace the server, you must store the data to a network directory or tape device before the operating system installation. Choosing this setting erases all existing drives.
- n **Cisco product key:** Cisco supplies a product key when you purchase a Cisco IP telephony product. The product key is based on a file encryption system that allows you to install only the components that you have purchased. It also prevents you from installing other supplied software for general use. The product key consists of alphabetical characters only.
- n **Username and organization name:** The system will prompt you for a username and an organization name to register the software product that you are installing. Do not leave the field blank. You can enter letters, numbers, hyphens (-), and underscores (_).

- n **Computer name:** The system will prompt you to assign a unique computer name, using 15 characters or fewer, to each Cisco CallManager server. The computer name may contain alphabetic and numeric characters, hyphens, and underscores, but it must begin with a letter of the alphabet. Follow your local naming conventions, if possible. If you want to change the computer name after the application installation, you must completely reinstall the operating system and the application.
- n **Workgroup:** The system will also prompt you for a workgroup name. A workgroup consists of a collection of computers that share the same workgroup name. Computers in the same workgroup can more easily communicate with each other across the network. Ensure that this entry, which must also be 15 characters or fewer, follows the same naming conventions as the computer name.
- n **Domain suffix:** When prompted, you must enter the Domain Name System (DNS) suffix in the format “mydomain.com” or “mycompany.mydomain.com.” If you are not using DNS, use a fictitious domain suffix, such as fictitioussite.com.
- n **TCP/IP properties:** You must assign an IP address, subnet mask, and default gateway when installing a Cisco CallManager server. You should not change the IP addresses after installation because they are permanent properties.

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

- n **DNS:** You must identify a primary DNS server for this optional field. By default, the telephones will attempt to connect to Cisco CallManager using DNS. Therefore, you must verify that the DNS server contains a mapping of the IP address and the fully qualified domain name (FQDN) of the Cisco CallManager server. If you do not use DNS, use the server IP address, instead of a server name, to register the telephones with Cisco CallManager. Refer to the *Cisco CallManager Administration Guide*, or the online help in the Cisco CallManager application, for information about changing the server name.

Note Before you begin installing multiple servers in a cluster, you must have a name resolution method in place, such as DNS, Windows Internet Naming Service (WINS), or local name resolution using a configured LMHOSTS file.

If you use DNS, you must verify that the DNS server contains a mapping of the IP address and the hostname of the server that you are installing. This verification must take place before you begin the installation.

If you use local name resolution, ensure that the LMHOSTS file is updated on the existing servers in the cluster before you begin the installation on the new subscriber server. You must add the same information to the LMHOSTS file on the new server during installation.

- n **SNMP community string:** The Windows 2000 Simple Network Management Protocol (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.
- n **Database server:** You must determine whether you will configure this server as a publisher database server or as a subscriber database server. This selection is permanent. You must

reinstall the Cisco CallManager server if you want to reassign the database server type at a later date.

Note You must install a Cisco CallManager publisher server before you can install any subscriber servers.

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

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

Note For Cisco CallManager database replication, you must enter the same replication account password for the publisher and all of the subscribers in the cluster.

Example: Configuration Data Worksheet

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

Configuration Data for Cisco MCS

Configuration	Data
Cisco product key	
Username	
Name of your organization	
Computer name	
Workgroup	
Microsoft NT domain (optional)	
DNS domain suffix	
Current time zone, date, and time	
DHCP parameters	It is recommended that you program a fixed IP address in TCP/IP properties for the server instead of using DHCP.
TCP/IP properties (required if DHCP is not used): <ul style="list-style-type: none"> n IP address n Subnet mask n Default gateway 	
DNS servers (optional): <ul style="list-style-type: none"> n Primary n Secondary WINS servers (optional): <ul style="list-style-type: none"> n Primary n Secondary LMHOSTS file (optional)	
Database server (choose one): <ul style="list-style-type: none"> n Publisher n Subscriber If you are configuring a subscriber server, supply the username and password of the publishing database server: <ul style="list-style-type: none"> — Publisher username — Publisher password 	
Backup (choose one or both): <ul style="list-style-type: none"> n Server n Target 	
New Windows 2000 administrator password	

Postinstallation Procedures

This topic examines the tasks that Cisco recommends that you perform after installing Cisco CallManager.

Postinstallation Procedures

Cisco.com

Change passwords:

- During upgrades, password resets to default.
- Change passwords on all servers in a cluster.

Stop unnecessary services:

- **Publisher and subscribers:**
 - DHCP Client, Fax Service, FTP Publishing Service, Smart Card, Smart Card Helper, Computer Browser, Distributed File System, License Logging Service
- **Subscribers:**
 - IIS Admin Service, World Wide Web Publishing Service
- **Activate services**
- **Install backup utility and configure the backup settings.**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1—1-10

You should perform postinstallation tasks to ensure the optimal operation of Cisco CallManager. Perform the following tasks for each server that you have installed:

- n **Change passwords:** During installation, all accounts are set to a default password. The server will prompt you to change the passwords for the Cisco CallManager accounts after installation is complete. These passwords must be the same for each of the Cisco CallManager servers in the cluster.
- n **Stop unnecessary services:** The Windows 2000 operating system may have services running that are not necessary. When you stop unnecessary services, you gain additional resources that you can allocate to mission-critical Cisco CallManager processes. You should stop all of the following services and set them to manual-start status unless they are otherwise needed on the system:
 - n DHCP Client
 - n Fax service (Cisco CallManager 3.2 and earlier)
 - n FTP Publishing Service
 - n Smart Card (Cisco CallManager 3.2 and earlier)
 - n Smart Card Helper (Cisco CallManager 3.2 and earlier)
 - n Computer browser (Cisco CallManager 3.2 and earlier)
 - n Distributed File System
 - n License Logging Service

In addition to the services listed here, you should stop and set the following services to *manual* on the subscriber servers:

- n **Microsoft Internet Information Server (IIS) Admin Service:** You can provide an additional level of security by turning off IIS on Cisco CallManager servers that do not need web access, such as subscriber servers. Turning off IIS protects unauthorized users from accessing Cisco CallManager in a distributed architecture.

- n **World Wide Web Publishing Service**

Both the FTP Publishing Service and the World Wide Web Publishing Service depend on the IIS Admin Service. When the IIS Admin Service stops, the FTP Publishing Service and World Wide Web Publishing Service also stop. You must set the FTP Publishing Service and the World Wide Web Publishing Service to manual.

To open services, choose **Start > Programs > Administrative Tools > Services**. Right-click each service and choose **Properties**. Then choose the startup type, stop the service, and click **Apply**.

- n **Activate services:** Activate Cisco CallManager services that you want to run on each server in the cluster.
- n **Install the backup utility:** Install Cisco BARS and configure the backup settings that determine when the Cisco CallManager data is backed up and to what device.

Activating Cisco CallManager Services

This topic explains the process of selecting and activating Cisco CallManager services after installation.

Cisco CallManager Service Selection

Cisco.com

- Cisco CallManager Service
- Cisco TFTP
- Cisco Messaging Interface
- Cisco IP Voice Media Streaming Application
- Cisco CTIManager
- Cisco Telephony Call Dispatcher
- Cisco MOH Audio Translator
- Cisco RIS Data Collector
- Cisco Database Layer Monitor
- Cisco CDR Insert
- Cisco CTL Provider
- Cisco Extended Functions
- Cisco Serviceability Reporter
- Cisco WebDialer
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco CTL Provider
- Cisco Certificate Authority Proxy Function (CAPF)

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1—1-12

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

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

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

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

The following information briefly describes each available Cisco CallManager service:

- n **Cisco CallManager Service:** Allows the server to actively participate in telephone registration, call processing, and other Cisco CallManager functions. Cisco CallManager Service is the core service of the Cisco CallManager platform.
- n **Cisco TFTP:** Activates a TFTP server on Cisco CallManager. The TFTP service delivers Cisco IP Phone configuration files to IP Phones, along with streamed media files, such as music on hold (MOH) and ring files.
- n **Cisco Messaging Interface:** Allows Cisco CallManager to interface with a Simplified Message Desk Interface (SMDI)-compliant, external voice-mail system.

- n **Cisco IP Voice Media Streaming Application:** Allows Cisco CallManager to act as an Media Termination Point (MTP), a conference bridge, a music on hold (MOH) server, and an annunciator.
- n **Cisco CTIManager:** Allows Cisco CallManager to support computer telephony integration (CTI) services and provides Telephony Application Programming Interface (TAPI) or Java Telephony Application Programming Interface (JTAPI) client support. Cisco CTIManager allows you to use applications such as Cisco IP SoftPhone.
- n **Cisco Telephony Call Dispatcher:** Distributes calls to multiple telephone numbers (hunt groups). Cisco WebAttendant and Auto Attendant require Cisco Telephony Call Dispatcher (TCD).
- n **Cisco MOH Audio Translator:** Allows Cisco CallManager to convert MP3 or WAV audio files into the MOH format.
- n **Cisco Real-Time Information Server (RIS) Data Collector:** Allows Cisco CallManager to write trace and alarm file information to a database or alert an SNMP server.
- n **Cisco Database Layer Monitor:** Monitors aspects of the Microsoft SQL 2000 database, as well as call detail records (CDRs).
- n **Cisco CDR Insert:** Allows Cisco CallManager to write CDRs to the local database and replicates CDR files to the Microsoft SQL publisher at a configured interval.
- n **Cisco CTL Provider:** Works with the Cisco Certificate Trust List (CTL) client to change the security mode for the cluster from nonsecure to secure.
- n **Cisco Extended Functions:** Provides support for some Cisco CallManager features, including Cisco Call Back and Quality Report Tool (QRT).
- n **Cisco Serviceability Reporter:** Generates the following daily reports: Device Statistics, Server Statistics, Service Statistics, Call Activities, and Alert.
- n **Cisco WebDialer:** Provides click-to-dial functionality by using a web page or a desktop application.
- n **Cisco IP Manager Assistant:** Allows Cisco CallManager to support the Cisco IP Manager Assistant (IPMA).
- n **Cisco CallManager Extension Mobility:** Allows Cisco CallManager to support extension mobility functions for roaming users.
- n **Cisco Certificate Authority Proxy Function:** Working in conjunction with the Cisco Certificate Authority Proxy Function (CAPF) application, the Cisco CAPF service can perform the following tasks, depending on your configuration:
 - Issue locally significant certificates to supported Cisco IP Phone models
 - Request certificates from third-party certificate authorities on behalf of supported Cisco IP Phone models
 - Upgrade existing certificates on the phones
 - Retrieve phone certificates for troubleshooting
 - Delete locally significant certificates on the phone

Cisco CallManager Service Activation

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1-1-13

The Service Activation tool activates services in automatic mode. It also checks for service dependencies based on a single-server configuration. When you click the **Set Default** button, the Service Activation tool chooses the services that are required to run Cisco CallManager based on a single-server configuration. For example, if you choose one service, you will be prompted to choose whether you want all the other services that depend on that service to run Cisco CallManager based on a single-server configuration.

You can activate the Cisco CallManager services in the Service Activation window. To activate these services, complete the following steps:

- Step 1** Open Internet Explorer, and go to http://<CallManager_IP_Address>/ccmadmin. The <CallManager_IP_Address> is the IP address of the Cisco CallManager server. Enter the administrative username and password information.
- Step 2** From the Application menu, choose **Cisco CallManager Serviceability**. The CallManager Serviceability interface appears.
- Step 3** From the Tools menu, choose **Service Activation**. A window similar to the window shown here appears.
- Step 4** Click the server that you would like to configure from the Servers column. Next, click the services that you would like to activate, and click the **Update** button. (You will experience a slight delay.) The Service Activation window will refresh when the process is complete.

Caution You should activate the Cisco CallManager services from the Service Activation window. If you manually start the services through the Windows 2000 Services administrative tool, unpredictable results may occur.

Upgrading Prior Cisco CallManager Versions

This topic identifies the supported versions of Cisco CallManager required to upgrade to Release 4.1.

Upgrading to Cisco CallManager 4.1

Cisco.com

Direct upgrades from:

- 3.3(4)
- 3.3(5)
- 4.0(1)
- 4.0(2a)

—————→

4.1

Other upgrades must go through one of the releases above.

© 2005 Cisco Systems, Inc. All rights reserved. CIP1 v4.1—1-11

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

If your server runs a version of Cisco CallManager Release 3.2 or earlier, you must first upgrade every server in the cluster to the latest version of Cisco CallManager Release 3.3 before you can upgrade to a version of Cisco CallManager Release 4.1.

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

Cisco requires that you install Cisco IP Telephony Server Operating System Version 2000.2.6 (or 2000.2.4 with upgrade to 2000.2.6) before you upgrade to Cisco CallManager Release 4.1.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The Cisco AVVID strategy provides the foundation for converged networks and includes the infrastructure, call-processing, applications, and client layers.**
- **Cisco CallManager functions include call processing, signaling and device control, dial plan administration, phone feature administration, directory services, and a programming interface.**
- **Cisco CallManager server requirements are Windows 2000 and Microsoft SQL Server 2000. DC-Directory is an embedded LDAP directory, and BARS can be used for backups.**
- **Cisco CallManager hardware requirements include Cisco MCSs, which have been designed specifically for Cisco voice applications by HP and IBM.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—1-14

Summary (Cont.)

Cisco.com

- **Installing the operating system and Cisco CallManager IP telephony application for a new installation requires several disks. Upgrades can be downloaded from Cisco.com (with required privileges) or ordered on disks.**
- **Gather configuration data before installing a Cisco CallManager server.**
- **Postinstallation procedures include changing passwords, stopping unnecessary services, activating services, and backing up the system.**
- **You must activate required services for a new installation. If you are upgrading, those services that you have already started on your system will start after the upgrade.**
- **Direct upgrades to Cisco CallManager 4.1 can be made from versions 3.3(4), 3.3(5), 4.0(1), or 4.0(2a).**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—1-15

References

For additional information, refer to these resources:

- n Cisco Systems, Inc. Cisco CallManager documentation.
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
- n Cisco Systems, Inc. Cisco 7800 Series Media Convergence Servers overview.
<http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/index.html>.

Identifying Cisco CallManager Cluster and Deployment Options

Overview

To ensure the same service availability that the traditional voice network provides, it is critical to build redundancy and failover capabilities into the IP telephony network design. The primary ways to achieve these capabilities are to cluster Cisco CallManager servers and to follow recommended design and deployment practices.

This lesson discusses the Microsoft SQL cluster relationship and its impact on the Cisco CallManager cluster and options that are available to enterprises to deploy a highly available IP telephony network.

Objectives

Upon completing this lesson, you will be able to determine the optimum Cisco CallManager cluster option and IP telephony deployment model for your enterprise. This ability includes being able to meet these objectives:

- n Describe how the Microsoft SQL cluster relationship provides publisher database redundancy and server failover capability
- n Describe the two types of communication that are used to ensure database replication and synchronization throughout the cluster
- n Describe the advantages and disadvantages of two design schemes that provide call-processing redundancy within the cluster
- n Identify the four supported IP telephony call-processing deployment models

- n Identify the major characteristics and design guidelines of a single-site IP telephony deployment model

- n Identify the major characteristics and design guidelines of a multiple-site centralized call-processing deployment model
- n Identify the major characteristics and design guidelines of a multiple-site distributed cluster call-processing deployment model
- n Identify the characteristics, limitations, and advantages of clustering over the IP WAN

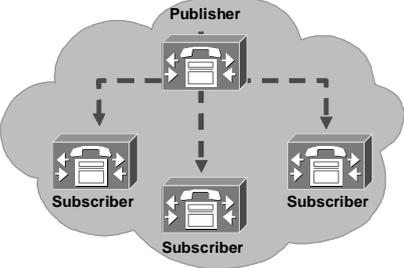
Microsoft SQL Cluster Relationship

This topic describes how the Microsoft SQL cluster relationship provides database redundancy and failover capability.

Microsoft SQL Cluster Relationship

Cisco.com

- **Two or more servers share a database and support a common group of IP devices.**
- **Clustering provides redundancy for the SQL database.**
- **A cluster has one publisher server and up to eight subscriber servers.**
- **One database on the publisher replicates to subscribers.**



© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1-1-3

The voice network is one of the most reliable business networks because PBX vendors design their systems to provide 99.999 percent uptime. To provide the same level of voice network reliability for IP telephony service, you must cluster Cisco CallManager servers. A Cisco CallManager cluster is two or more servers that share the same database and work together to support a common group of IP telephony devices.

Clustering servers provides two important functions: It eliminates a single-server point of failure and allows multiple devices to work together in one call-processing entity. The database replication capability provided by Microsoft SQL Server makes clustering possible by allowing the same database to be on multiple machines. Database replication makes it appear as if a single machine is handling call processing and other functions and ensures that standby processors can seamlessly step in and fulfill the functions if the primary processor fails.

You must have at least two Cisco CallManager servers to obtain this redundancy, and one of these servers must be a publisher database server. The publisher database server manages the only writable copy of the Microsoft SQL Server 2000 database. The subscriber database servers maintain read-only copies of the database. You can have only one publisher server and up to eight subscriber servers per cluster (a Microsoft SQL restriction).

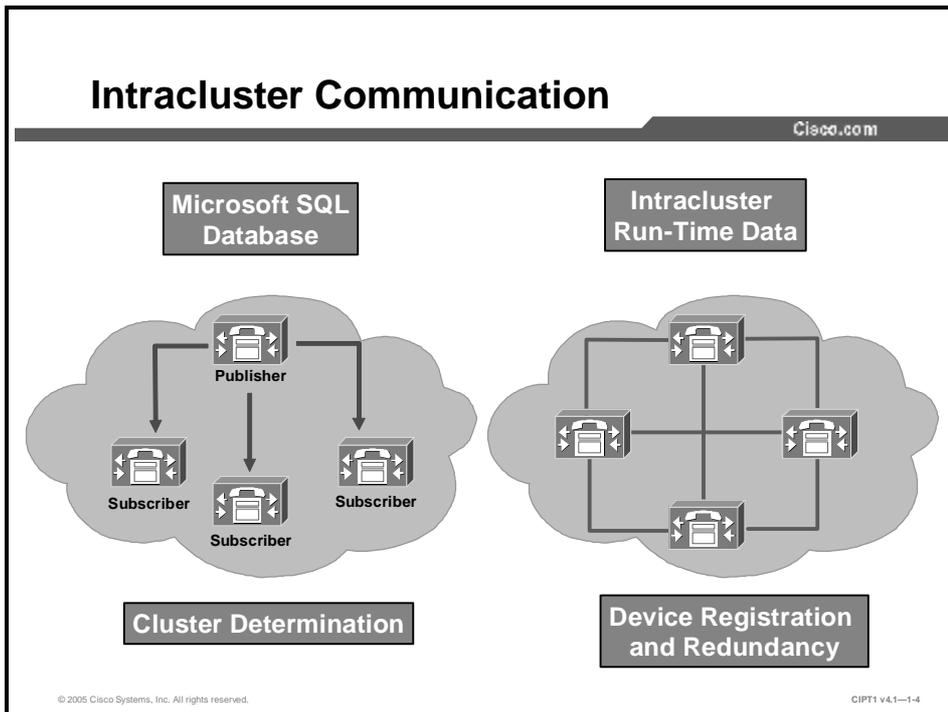
When you make changes to the Cisco CallManager configuration, these changes are written directly to the publisher server. The publisher then replicates these changes to the subscriber servers. When the publisher server is offline, the Microsoft SQL Server 2000 database automatically locks, and thus prevents further database changes. The IP telephony network continues to operate, but you will not be able to add or configure any devices that are managed by Cisco CallManager.

When the publisher is down, the subscribers store Call Detail Records (CDRs) until the publisher comes back online, and then the subscribers update the publisher with the CDRs.

In Cisco CallManager Release 3.3 and later, a cluster is capable of handling approximately 30,000 Cisco IP Phones. This cluster limitation does not restrict the size of the voice over IP (VoIP) network. By creating additional clusters, you can increase the network size. Intercluster trunks allow devices to communicate between cluster boundaries.

Intracuster Communication

This topic examines the two types of intracuster communication.

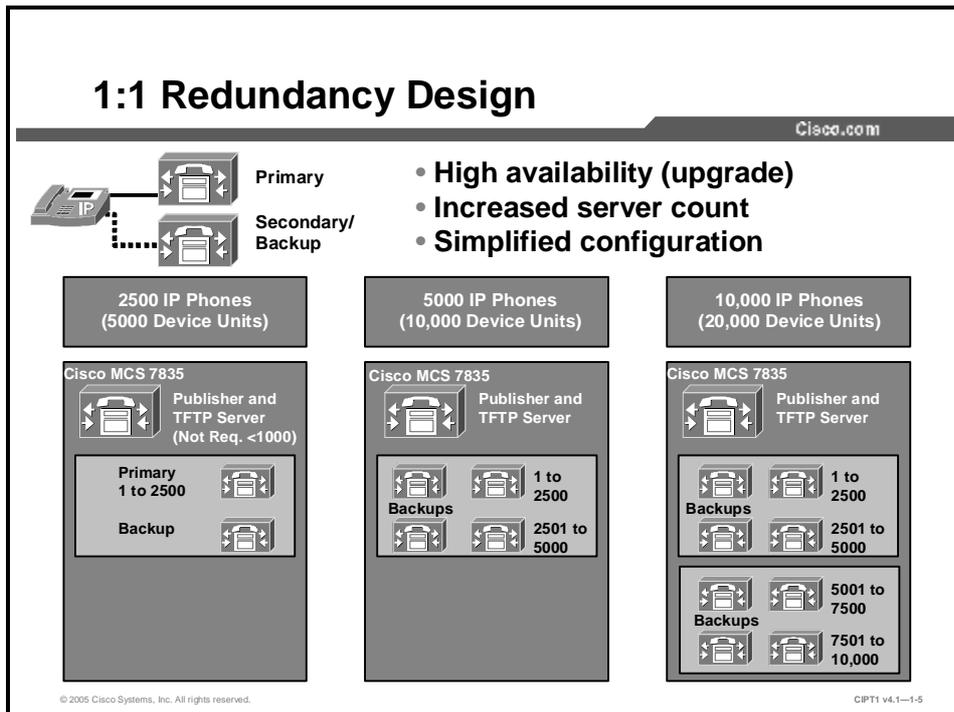


This figure illustrates the two types of intracuster communication: Microsoft SQL Server 2000 database replication and Cisco CallManager run-time data.

- n **Database replication:** During normal operation, all of the Cisco CallManager servers in a cluster read data from and write data to the publisher database. Periodically, the publisher automatically updates the backup copies of the database. If the publisher database becomes unavailable, the various Cisco CallManager servers in the cluster continue to operate from their local backup copies of the database. All data entry to the publisher database is denied if the link to the publisher, or the publisher itself, is down. When the publisher database is restored, normal operations resume.
- n **Run-time data:** The second type of intracuster communication is run-time data, which is used for registration of Cisco IP Phones, gateways, and digital signal processor (DSP) resources. Run-time data is shared with all of the members of the cluster and ensures the optimum routing of calls between members of the cluster and the associated gateways. When a device (such as a Cisco IP Phone) registers with its primary Cisco CallManager server, the primary updates all of the other Cisco CallManager servers in the cluster. After registration, the device sends a TCP keepalive message to the primary server every 30 seconds and sends a TCP connect message to its secondary Cisco CallManager server. When the Cisco IP Phone detects the failure of its TCP keepalive message with the primary Cisco CallManager server, the device attempts to register with its secondary Cisco CallManager server. The secondary CallManager server accepts the registration from the device and announces the new registration (through intracuster run-time communication) to all of the Cisco CallManager servers in the cluster. The device initiates a TCP keepalive message to the secondary Cisco CallManager server (the new primary of the device) and sends a TCP connect message to a tertiary Cisco CallManager server (the new secondary of the device).

Cluster Redundancy Designs

This topic examines two cluster designs that provide call-processing redundancy.



In a 1:1 Cisco CallManager redundancy deployment design, you can have a dedicated backup server for each primary server. This design guarantees that Cisco IP Phone registrations will never overwhelm the backup servers, even if multiple primary servers fail. However, the 1:1 redundancy design considerably limits the maximum cluster size and is not cost-effective.

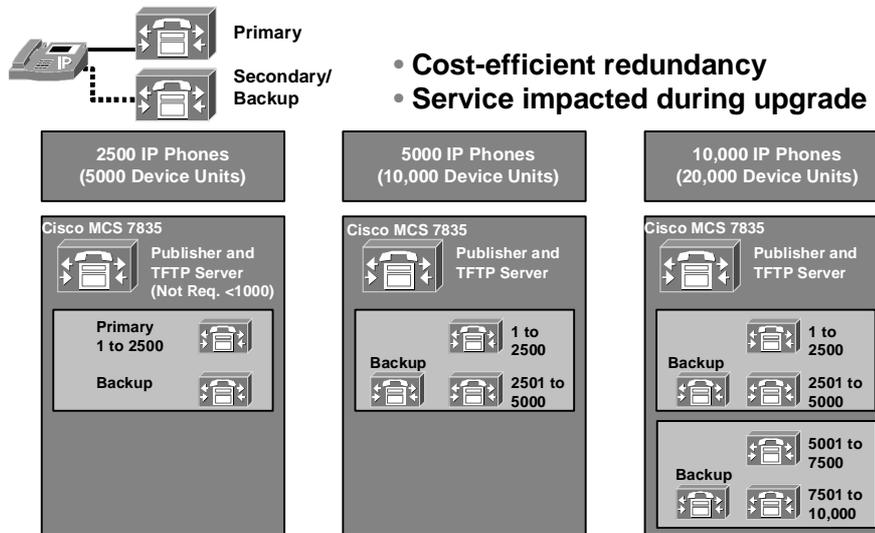
Each cluster must also have a designated TFTP server. Depending on the number of devices that a server is supporting, you can combine this TFTP server functionality with the publisher or subscriber Cisco CallManager servers, or you can deploy the TFTP functionality on a separate, standalone server. The TFTP server is responsible for delivering IP Phone configuration files to each telephone, along with streamed media files, such as music on hold (MOH) and ring files; therefore, the TFTP server can experience a considerable network and processor load.

In this example, a Cisco 7835 Media Convergence Server (MCS) is used because each Cisco CallManager server installed on that platform supports a maximum of 2500 Cisco IP Phones. A single Cisco CallManager is the primary server, with a secondary server acting as a dedicated backup. The primary or backup server can also serve as the Microsoft SQL publisher and the TFTP server in smaller IP telephony deployments (fewer than 1000 IP Phones).

When you increase the number of IP Phones, you must increase the number of Cisco CallManager servers that are required to support the telephones. Some network engineers may consider the 1:1 redundancy design excessive, because a well-designed network is unlikely to lose more than one primary server at a time. With the low possibility of server loss and the increased server cost, many network engineers elect to use a 2:1 redundancy design.

2:1 Redundancy Design

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1-1-6

In a 2:1 Cisco CallManager redundancy deployment design, you have a dedicated backup server for every two primary servers. Although this design offers some redundancy, there is the risk of overwhelming the backup server if multiple primary servers fail. In addition, upgrading the Cisco CallManager servers can cause a temporary loss of service because you must reboot the Cisco CallManager servers after the upgrade is complete.

Network administrators use this 2:1 redundancy model in most IP telephony deployments because of the reduced server costs. If you are using a Cisco MCS 7835 (shown in the figure), that server is equipped with redundant, hot-swappable power supplies and hard drives. When you properly connect and configure these servers, it is unlikely that multiple primary servers will fail at the same time, which makes the 2:1 redundancy model a viable option for most businesses.

Call-Processing Deployment Models

This topic lists the call-processing deployment models that Cisco IP telephony supports.

Deployment Models

Cisco.com

- **Supported IP telephony deployment models:**
 - **Single-site deployment**
 - **Multisite WAN with centralized call processing**
 - **Multisite WAN with distributed call processing**
 - **Clustering over the IP WAN**
- **Defining characteristics of each:**
 - **Type of traffic that is carried over the WAN (data only or data and voice)**
 - **Location of call-processing agent**
 - **Size of the deployment**

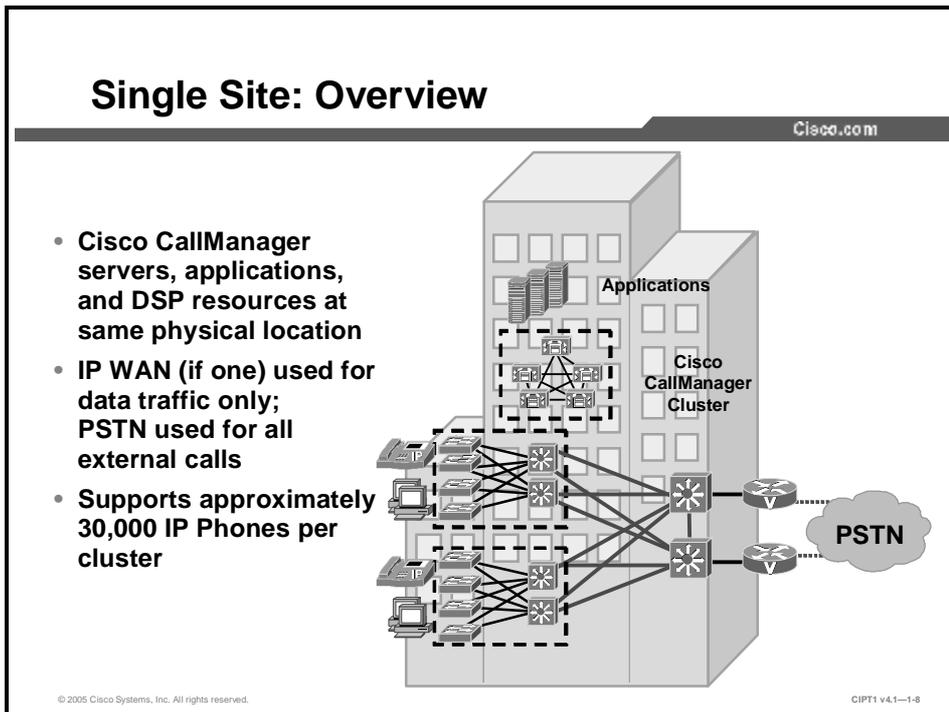
© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1--1-7

This figure illustrates the types of deployment models that Cisco Systems supports. Each model differs in three areas: type of traffic that is carried over the WAN, location of the call-processing agent, and size of the deployment. Cisco IP telephony supports these deployment models:

- n Single-site
- n Multisite with centralized call processing
- n Multisite with distributed call processing
- n Clustering over the IP WAN

Single-Site Deployment

This topic describes the single-site deployment model.



In a single-site deployment model, all Cisco CallManager servers applications, and DSP resources are in the same physical location. You can implement multiple clusters and interconnect them through intercluster trunks if you need to deploy more IP Phones in a single-site configuration. Gateway trunks that connect directly to the Public Switched Telephone Network (PSTN) handle external calls. If an IP WAN exists between sites, it is used to carry data traffic only; no telephony services are provided over the WAN.

Use this model for a single campus or site with fewer than 30,000 lines.

Single Site: Design Guidelines

Cisco.com

- **Understand the current calling patterns within the enterprise.**
- **Use the G.711 codec; DSP resources can be allocated to other functions, such as conferencing and MTP.**
- **Off-net calls should be diverted to the PSTN or sent to the legacy PBX.**
- **Choose a uniform gateway for PSTN use.**
- **Deploy the recommended network infrastructure.**
- **Do not oversubscribe the Cisco CallManager and clustering capability.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--1-9

Single-site deployment is a subset of the distributed and centralized call-processing model. This deployment requires that you adhere to the recommended best practices specific to this model for future scalability. When you develop a stable, single-site infrastructure that is based on a common infrastructure philosophy, you can easily expand the IP telephony system applications, such as video streaming and videoconferencing, to remote sites.

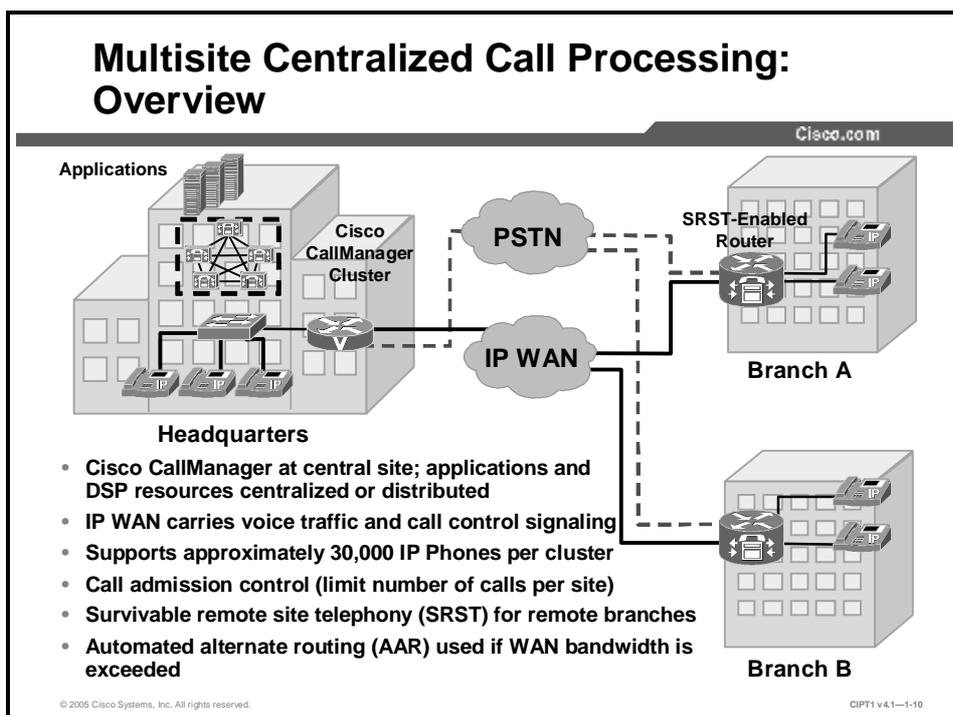
These are the guidelines for single-site deployments:

- n You must understand the current calling patterns within the enterprise. How and where are users making calls? How many calls are intersite or interbranch versus intrasite? If calling patterns dictate that most calls are intrasite, use the single-site model to deploy IP telephony and make use of the relatively inexpensive PSTN. This design also simplifies the dial plans and avoids provisioning dedicated bandwidth for voice in the IP WAN.
- n The G.711 coder-decoder (codec) should be used. The call will stay in the LAN, and G.711 is a simple mechanism for deployment. It does not require dedicated DSP resources for transcoding (which means converting between codec types, such as between G.711 and G.729), and older voice-mail systems may support only G.711. You can allocate these DSP resources to other functions, such as conferencing and Media Termination Point (MTP). Although the 64 kpbs per-call bandwidth that G.711 consumes is higher than that of all other codecs, it is not a concern in this design because the call is not traversing the WAN, where bandwidth is generally limited.
- n All off-net calls will be diverted to the PSTN or sent to the legacy PBX for call routing if the PSTN resources are being shared during migratory deployments.
- n Use Media Gateway Control Protocol (MGCP) gateways for the PSTN if H.323 functionality is not required. Centralize the gateway functions using H.323 gatekeepers when deploying multiple clusters, rather than using MGCP gateways.
- n Deploy the recommended network infrastructure for high-availability connectivity options for telephones (inline power), quality of service (QoS) mechanisms, and other services.
- n Do not oversubscribe Cisco CallManager to scale larger installations. In prior software releases, Cisco used various schemes to allow the capacity of a system to be calculated using device weights, busy hour call attempt (BHCA) multipliers, and dial plan weights. With

Cisco CallManager Release 4.0, this scheme has been replaced by a capacity tool to allow for more accurate planning of the system. The capacity planning tool is currently available only to Cisco employees. If your system does not meet the guidelines found in the *Cisco IP Telephony Solution Network Reference Design*, or if you consider the system to be more complex and would like to verify the capacity, please contact your Cisco Systems engineer. The *Cisco IP Telephony Solution Reference Network Design (SRND)* is found at: <http://www.cisco.com/univercd/cc/td/doc/solution/esm/>.

Multisite WAN with Centralized Call Processing

This topic examines the multisite WAN with centralized call-processing deployment model.



The figure illustrates the multisite centralized call-processing deployment model with a Cisco CallManager cluster at a central site and a connection to several remote sites through a QoS-enabled IP WAN. The remote sites rely on the centralized Cisco CallManager cluster to handle call processing. Applications such as voice mail and interactive voice response (IVR) systems usually reside at the central site, thus reducing the overall cost of ownership and centralizing administration and maintenance. However, this design is not a requirement.

The WAN connectivity options include the following:

- n Leased lines
- n Frame Relay
- n ATM
- n ATM to Frame Relay Service InterWorking (SIW)

Routers that reside at WAN edges require QoS mechanisms, such as priority queuing and traffic shaping, to protect voice traffic from data traffic across the WAN (where bandwidth is typically scarce).

To avoid oversubscribing the WAN links with voice traffic (thus causing deterioration of the quality of established calls), the network may need a call admission control scheme. With the introduction of Cisco CallManager Release 3.3, centralized call-processing models can take advantage of automated alternate routing (AAR) features. AAR allows Cisco CallManager to dynamically reroute a call over the PSTN if the call exceeds the WAN bandwidth.

You can provide PSTN access for the voice network through a variety of Cisco gateways. When the IP WAN is down, the users at remote branches can dial an access code and place their calls through the

PSTN, or the Cisco Survivable Remote Site Telephony (SRST) feature that is available for Cisco IOS gateways can provide call processing during the outage.

ISDN can also provide backup data connectivity during WAN failures; however, voice traffic should not use the ISDN links because these interfaces do not support the required QoS features.

Multisite Centralized Call Processing: Design Guidelines

Cisco.com

- **Installations adopting the centralized call-processing deployment model are limited to hub-and-spoke topologies.**
- **SRST on the branch router limits remote offices to a maximum of 480 IP Phones when using a Cisco 7200 Series router.**

© 2005 Cisco Systems, Inc. All rights reserved.

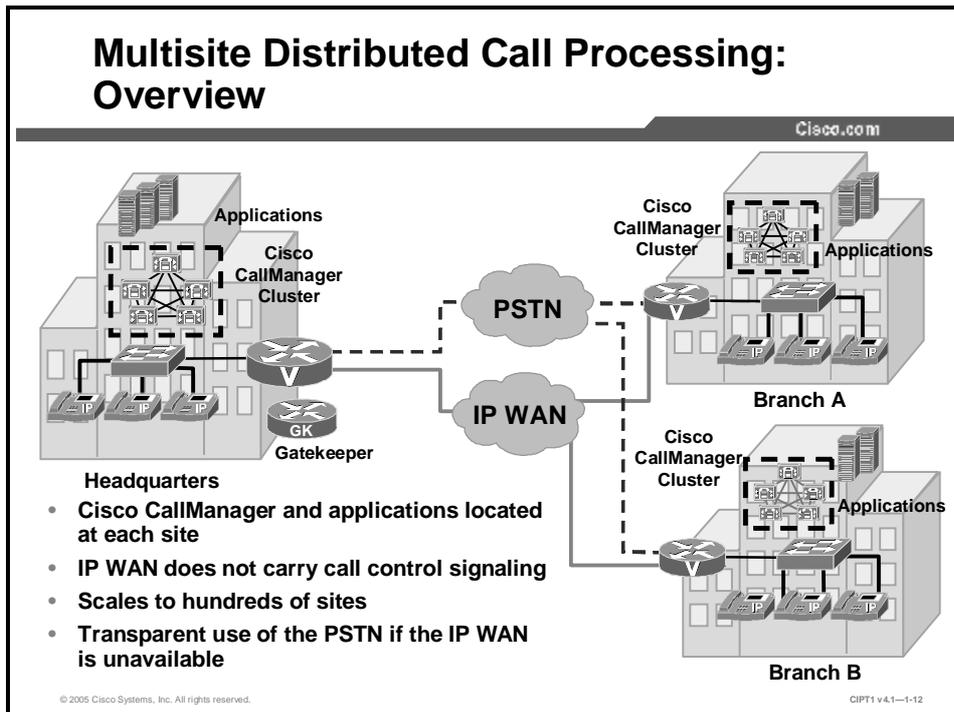
CIPT1 v4.1-1-11

Follow these best-practice guidelines when deploying a centralized call-processing model:

- n Installations adopting the centralized call-processing deployment model are limited to hub-and-spoke topologies because the locations-based call admission control mechanism used in centralized call processing deployments records only the available bandwidth in and out of each location.
- n There is no limit to the number of IP Phones at each individual remote branch. However, the capability that is provided by the SRST feature in the branch router limits remote branches to 480 Cisco IP Phones on a Cisco 7200 Series router during failover. Smaller platforms have lower limits.

Multisite WAN with Distributed Call Processing

This topic examines distributed multisite call-processing design.



A multisite distributed call-processing deployment has one or more call-processing agents at each site, and each site has its own Cisco CallManager cluster. You can trunk these sites together through an IP WAN.

Depending on your network design, a distributed call-processing site may consist of the following:

- n A single site with its own call-processing agent, which may be a Cisco CallManager or a third-party call agent
- n A centralized call-processing site (and all of its remote sites) that the network views as a single site for distributed call processing
- n A legacy PBX with a VoIP gateway or a legacy PBX that is attached using a time-division multiplexing (TDM) interface to a VoIP gateway

You can interconnect all distributed call-processing sites through an IP WAN. Cisco considers a site that is connected only through the PSTN to be a standalone site.

The WAN connectivity options include the following:

- n Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)
- n Voice and Video Enabled IPsec VPN (V3PN)
- n Leased lines
- n Frame Relay
- n ATM
- n ATM to Frame Relay SIW

Multisite distributed call processing allows each site to be completely self-contained. In the event of an IP WAN failure or insufficient bandwidth, the site does not lose call-processing service or functionality. Cisco CallManager simply sends all calls between the sites across the PSTN.

In summary, the main benefits of this deployment model are as follows:

- n Cost savings when you are using the IP WAN for intersite calls
- n Toll-bypass savings when you are using remote gateways to drop off into the PSTN (known as “tail end hop off,” or TEHO)
- n No loss of functionality during an IP WAN failure
- n Scalability to hundreds of sites

Multisite Distributed Call Processing: Design Guidelines

Cisco.com

- **Use of Hot Standby Router Protocol (HSRP) gatekeeper pairs is currently recommended.**
- **Use of a single WAN codec is currently recommended.**
- **Use a logical hub-and-spoke topology for the gatekeeper.**
- **Gatekeeper networks scale to hundreds of sites.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—1-13

The multisite WAN with distributed call-processing deployment model is a superset of the single-site and multisite WAN with centralized call-processing models. You should follow the best practices guidelines for single-site and multisite deployments in addition to those listed here, which are specific to this deployment model.

The gatekeeper or Session Initiation Protocol (SIP) proxy servers are among the key elements in the multisite WAN with distributed call processing. Both provide dial plan resolution, with the gatekeeper also providing call admission control.

A gatekeeper is an H.323 device that provides call admission control and E.164 dial plan resolution.

Additional gatekeeper guidelines include the following:

- n It is recommended that you use alternate gatekeeper support to provide a gatekeeper solution with high availability. It is also recommended that you use multiple gatekeepers to provide spatial redundancy within the network.
- n It is recommended that you use a single WAN codec. This design makes capacity planning easy and does not require you to overprovision the IP WAN to allow for worst-case scenarios.
- n Use a logical hub-and-spoke topology for the gatekeeper. A gatekeeper can manage the bandwidth into and out of a site or between zones within a site, but it is not aware of the topology.
- n Gatekeeper networks can scale to hundreds of sites, and the design is limited only by the hub-and-spoke topology.
- n Also include information on SIP proxy servers.

SIP devices provide resolution of E.164 numbers as well as SIP uniform resource identifiers (URIs) to enable endpoints to place calls to each other. Cisco CallManager supports the use of E.164 numbers only.

The following best practices apply to the use of SIP proxies:

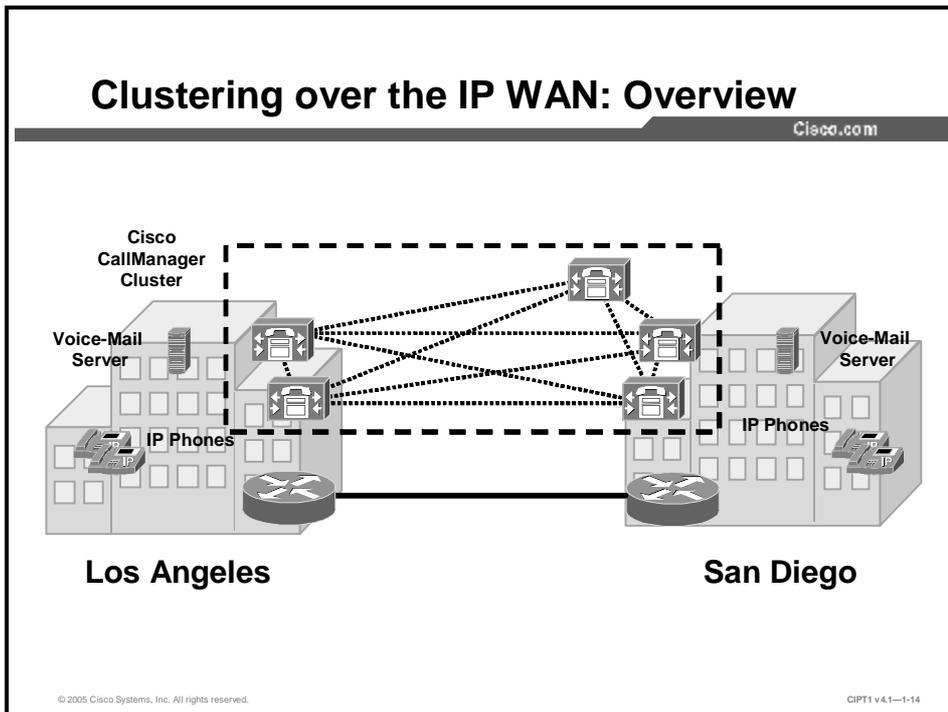
- n Provide adequate redundancy for the SIP proxies.
- n Ensure that the SIP proxies have the capacity for the call rate and number of calls required in the network.

For more detail on bandwidth capacity planning and call admission control for each deployment model, refer to the *Cisco IP Telephony Solution Reference Network Design (SRND)* for Cisco CallManager 4.0 at:

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a00802c370c.html.

Clustering over the IP WAN

This topic examines clustering over the IP WAN.



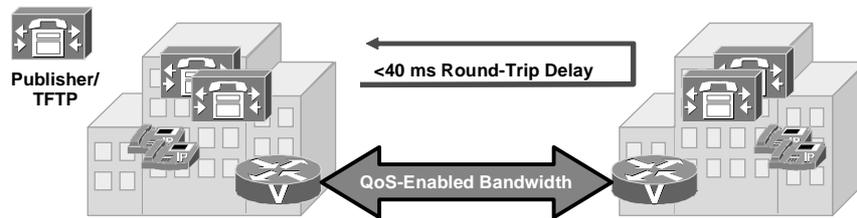
Cisco supports Cisco CallManager clusters over a WAN. Although there are stringent requirements, this design offers these advantages:

- n Single point of administration for users for all sites within the cluster
- n Feature transparency
- n Shared line appearances
- n Extension mobility within the cluster

This design is useful for customers that require more functionality than the limited feature set that is offered by SRST. This network design also allows remote offices to support more Cisco IP Phones than SRST in the event that the connection to the primary Cisco CallManager is lost.

Clustering over the IP WAN: Design Guidelines

Cisco.com



- **40-ms round-trip delay between *any* two Cisco CallManager servers in the cluster**
- **900 kbps for every 10,000 BHCAs within the cluster**
- **Up to eight small sites using the remote failover deployment model**
- **Failover across WAN supported (more bandwidth)**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—1-15

Although the distributed single-cluster call-processing model offers some significant advantages, it must adhere to these strict design guidelines:

- n Two Cisco CallManager servers in a cluster must have a maximum round-trip delay of 40 ms between them. In comparison, high-quality voice guidelines dictate that one-way end-to-end delay should not exceed 150 ms. Because of this strict guideline, you can use this design only between closely connected, high-speed locations.
- n For every 10,000 BHCAs within the cluster, you must support an additional 900 kbps of WAN bandwidth for intracenter run-time communication. The BHCA represents the number of call attempts made during the busiest hour of the day.
- n Up to eight small sites are supported using the remote failover deployment model. Remote failover allows you to deploy the backup servers over the WAN. Using this deployment model, you may have up to eight sites with Cisco CallManager subscribers being backed up by Cisco CallManager subscribers at another site.
- n SRST can function in this model but is not necessary. The telephones can fail over across the WAN to other Cisco CallManager servers. This design may require significant additional bandwidth, depending on the number of telephones at each location.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Clusters provide database redundancy. One publisher maintains the only writable database. Up to eight subscribers maintain read-only copies.**
- **There are two types of intracluster communications: database replication and run-time data.**
- **There are two different failover models: the 1:1 model and the 2:1 model.**
- **Supported Cisco IP telephony deployment models are single-site, multisite with centralized call processing, multisite with distributed call processing, and clustering over the IP WAN.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—1-16

Summary (Cont.)

Cisco.com

- **In the single-site deployment model, the Cisco CallManager applications and the DSP resources are at the same physical location; the PSTN handles all external calls.**
- **The multisite centralized model has a single call-processing agent; applications and DSP resources are centralized or distributed; and the IP WAN carries voice traffic and call control signaling between sites.**
- **The multisite distributed model has multiple independent sites each with a call-processing agent, and the IP WAN carries voice traffic between sites but not call control signaling.**
- **The benefits of clustering over an IP WAN include a unified dial plan, feature extension to all offices, the ability to handle more phones at a remote site during failover (and the server is local), and central administration.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—1-17

References

For additional information, refer to these resources:

- n Cisco Systems, Inc. Cisco CallManager documentation.
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
- n Cisco Systems, Inc. *Cisco IP Telephony Solution Reference Network Design (SRND) for Cisco CallManager 4.1*.
http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/voice/c_callmg/4_1/srnd4_1/index.htm

Module 1 Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **Deploying Cisco CallManager in an Cisco IP telephony solution entails selecting the Cisco MCS hardware platform, installing the Cisco CallManager software, and performing postinstallation procedures.**
- **The primary redundancy designs for the cluster are 1:1 (one backup for every primary) and 2:1. Cost is a primary driver impacting your selection. There are four call-processing deployment models. These models differ based on whether call processing is centralized or distributed and whether the cluster is located within a single site or dispersed across multiple sites.**

© 2005 Cisco Systems, Inc. All rights reserved.CIP11 v4.1--1-1

This module covered the key factors to be considered when you are initially using a Cisco CallManager server in an IP telephony deployment. This module presented the role that Cisco CallManager plays in the overall Cisco AVVID strategy, the Cisco CallManager hardware and software requirements, the Cisco CallManager installation and upgrade process, and postinstallation procedures. The module then covered how the Microsoft SQL relationship provides redundancy and failover and the requirements, advantages, and disadvantages of deploying a 1:1 server redundancy design versus a 2:1 redundancy design. The module ended with a discussion of the four call-processing deployment models.

Module 1 Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module 1 Self-Check Answer Key.

- Q1) Which four of the following are IP telephony deployment models that are supported by Cisco? (Choose four.) (Source: Lesson 1-2, Identifying Cisco CallManager Cluster and Deployment Options)
- A) a single site with one call-processing agent
 - B) multiple sites with centralized call processing
 - C) multiple sites each with its own call-processing agent
 - D) a single cluster with distributed call processing
 - E) multiple clusters with no call-processing agent
- Q2) A 1:1 redundancy design offers _____. (Source: Lesson 1-2, Identifying Cisco CallManager Cluster and Deployment Options)
- A) increased redundancy; however, the increased server cost is often prohibitive
 - B) some redundancy; however, a server reboot is required after an upgrade
 - C) maximum uptime; however, no more than a 20-ms round-trip delay can exist between servers
 - D) high availability; however, you may overwhelm the backup servers
- Q3) A single cluster that spans multiple sites can have which two benefits compared to a branch office in a multisite WAN with a centralized call-processing deployment? (Choose two.) (Source: Lesson 1-2, Identifying Cisco CallManager Cluster and Deployment Options)
- A) completely self-contained individual sites
 - B) WAN bandwidth cost savings
 - C) a common dial plan across all sites
 - D) more IP Phone features during failover
 - E) scalability to hundreds of sites
- Q4) Which two of the following enable the cluster to achieve redundancy? (Choose two.) (Source: Lesson 1-2, Identifying Cisco CallManager Cluster and Deployment Options)
- A) local failover
 - B) database replication
 - C) at least two servers
 - D) directory access
- Q5) Which two of these are NOT functions of Cisco CallManager? (Choose two.) (Source: Lesson 1-1, Introducing Cisco CallManager)
- A) interactive voice response
 - B) signaling control
 - C) device control
 - D) dial plan
 - E) voice messaging

- Q6) Which layer of Cisco AVVID contains Cisco CallManager? (Source: Lesson 1-1, Introducing Cisco CallManager)
- A) client
 - B) applications
 - C) call-processing
 - D) infrastructure
- Q7) Cisco CallManager uses which of these operating systems? (Source: Lesson 1-1, Introducing Cisco CallManager)
- A) Linux
 - B) Windows 95
 - C) Windows NT
 - D) Windows 2000
- Q8) Why is it recommended that you stop IIS on the subscriber servers if it is not needed? (Source: Lesson 1-1, Introducing Cisco CallManager)
- A) enhances server call processing and redundancy
 - B) maximizes the number of devices in a cluster
 - C) disables the use of remote terminal services
 - D) helps prevent unauthorized access to the server
- Q9) When you first install Cisco CallManager software, which CD-ROM should you use to boot the server to determine the correct CD-ROM to insert next? (Source: Lesson 1-1, Introducing Cisco CallManager)
- A) Cisco CallManager 4.0 Software Disk
 - B) Cisco IP Telephony Server Operating System Hardware Detection Disk
 - C) Cisco CallManager Installation, Upgrade, and Recovery Disk
 - D) Cisco IP Telephony Server Backup and Restore Disk
 - E) Cisco Extended Services and Locales Disk
- Q10) If you are not using DNS, what must you configure to resolve server names? (Source: Lesson 1-1, Introducing Cisco CallManager)
- A) DHCP
 - B) backup server
 - C) LMHOSTS file
 - D) DNS reverse lookup

Module 1 Self-Check Answer Key

Q1) A, B, C, D

Q2) A

Q3) C, D

Q4) B, C

Q5) A, E

Q6) C

Q7) D

Q8) D

Q9) B

Q10) C

Establishing an On-Cluster Call

Overview

Numerous components and considerations are involved before you can place Cisco IP Phone calls within the same cluster. This module discusses the various Cisco IP Phone models that you may encounter when administering a Cisco IP telephony network and how to configure the Cisco Catalyst switch to power Cisco IP Phones and support voice traffic. This module also discusses how to configure Cisco CallManager to support IP Phones and users, how to make PC-based IP phone calls, and how to use Cisco CallManager tools to bulk-add users and devices.

Module Objectives

Upon completing this module, you will be able to configure Cisco CallManager and the Cisco Catalyst switch to enable on-cluster calls. You will also be able to add users and phones to the Cisco CallManager database using manual configuration, auto-registration, and BAT. This ability includes being able to meet these objectives:

- n Distinguish among the various Cisco IP endpoints, including IP Phones, conference stations, and PC-based phones, and describe how they work within a Cisco IP telephony solution
- n Configure Cisco CallManager system settings and use auto-registration and manual configuration to add Cisco IP Phones to the Cisco CallManager database and assign a directory number
- n Implement a Cisco Catalyst switch in an IP telephony network to provide inline power to the IP Phones, prioritize voice traffic, and create a separate voice VLAN for IP Phones
- n Install and configure Cisco IP Communicator and make IP Phone calls from the PC
- n Use BAT and TAPS to add and auto-register Cisco IP Phones, users, and ports in bulk in an IP telephony network

Lesson 2-1

Identifying Cisco IP Telephony Endpoints

Overview

An important task of implementing and supporting an IP telephony deployment is managing the end-user devices, or endpoints. You should be able to distinguish between the various Cisco IP telephony end-user devices that you may encounter during the course of deploying and administering a Cisco IP telephony network. In addition, understanding the boot and registration communication between a Cisco IP Phone and Cisco CallManager is important for understanding normal voice network operations and for troubleshooting purposes.

This lesson will explain the various models of Cisco IP Phones and how they work within a Cisco IP telephony solution. You will learn the basic features of Cisco IP Phones, analog adapters, and conference stations; the IP Phone power-up and registration process; and the audio coders-decoders (codecs) that are supported by Cisco IP Phones.

Objectives

Upon completing this lesson, you will be able to distinguish among the various Cisco IP telephony endpoints and describe how Cisco IP Phones work within a Cisco IP telephony solution. This ability includes being able to meet these objectives:

- n Describe the basic features of Cisco IP Phones
- n List the entry-level Cisco IP Phones and their features
- n List the midrange and upper-end Cisco IP Phones and their features
- n Describe the features and functions of additional Cisco IP telephony endpoints, including video endpoints, conference stations, expansion modules for Cisco IP Phones, PC-based Cisco IP Phones, and analog adapters
- n Identify the six steps of the Cisco IP Phone startup process in the correct order

n Identify the two audio codecs that are supported by Cisco IP Phones

Cisco IP Phone Overview

This topic provides an overview of Cisco IP Phones and the features that are common to the majority of Cisco IP telephony endpoints.

Cisco IP Phone Overview

Cisco.com

Cisco IP Phones have the following enhancements:

- **Display-based**
- **User customization**
- **Inline PoE.**
- **Support of the G.711 and G.729 audio codecs**



© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1--2-3

To the user, the telephone is the most visible component of the voice communications network. Cisco IP Phones are next-generation, intelligent communication devices that deliver essential business communications. Fully programmable, the growing family of Cisco IP Phones provides the most frequently used business features.

The majority of Cisco IP Phones provide the following enhancements:

- n Display-based user interface
- n Straightforward user customization
- n Inline power over Ethernet (PoE)
- n Support for the G.711 and G.729 audio codecs

Each Cisco IP Phone provides toll-quality audio and does not require a companion PC. Because it is an IP-based phone, you can install it in any location on a corporate local or wide-area IP network.

Entry-Level Cisco IP Phones

This topic describes the entry-level Cisco IP Phones that are available and provides a brief overview of their features.

Entry-Level Cisco IP Phones

Cisco.com

<small>Cisco IP Phone 7902G</small>	<small>Cisco IP Phone 7905G</small>	<small>Cisco IP Phone 7910G+SW</small>	<small>Cisco IP Phone 7912G</small>
			

- **Basic-featured IP Phones for low-to-medium telephone use**
- **Single line/DN**
- **Display-based (except Cisco 7902G)**
- **Message waiting indicator**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1—2.4

Cisco has produced a number of entry-level IP Phones for a variety of business functions. Depending on user requirements, these IP Phones may function well for employees or for use only in public areas, such as lobbies or break rooms.

Entry-level Cisco phones provide the following common features:

- n Display-based user interface (except Cisco IP Phone 7902G)
- n G.711 and G.729 codec
- n Single line (directory number [DN])
- n Cisco inline power, powered patch panel, or local power option support via a power cube (the same power supply as the Cisco IP Phone 7910, 7940, or 7960)
- n Visual message waiting indicator (MWI)
- n No speakerphone or headset port

Here is a brief description of the major features of each entry-level Cisco IP Phone:

- n **Cisco IP Phone 7902G:** The Cisco IP Phone 7902G is a single-line, entry-level, no-display business phone with fixed feature keys that provide one-touch access to the redial, transfer, conference, and voice-mail access features. Here is a brief description of the major features of the Cisco IP Phone 7902G:
 - Ability to handle low telephone traffic
 - Fixed features: redial, transfer, conference, messages
 - Hard Hold key
 - Single RJ-45 connection (no internal Ethernet switch)

- n **Cisco IP Phone 7905G and Cisco IP Phone 7912G:** The Cisco IP Phone 7905G provides single-line access and four interactive softkeys that guide a user through call features and functions via the pixel-based liquid crystal display (LCD). Use this IP Phone for employees who do not need a full-featured phone or for a common area such as a hallway, manufacturing floor, break room, reception space, or office cubicle. The Cisco IP Phone 7912G includes an integrated Ethernet switch that provides LAN connectivity to a colocated PC. Here is a brief description of the major features of the Cisco IP Phone 7905G and Cisco 7912G:
 - Ability to handle low-to-medium telephone usage
 - Pixel-based display (approximately five lines plus softkeys and date, time, and menu title)
 - Hard Hold key
 - Access to all standard IP Phone features through four on-screen softkeys
 - Support for limited Extensible Markup Language (XML) script processing
 - Support for Cisco Skinny Client Control Protocol (SCCP), H.323 version 2 (Cisco 7905G only), and Session Initiation Protocol (SIP; compliant with RFC 2543)

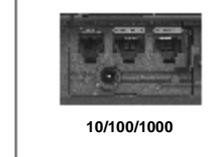
- n **Cisco IP Phone 7910G+SW:** The Cisco IP Phone 7910G+SW is for common-use areas that require only basic features, such as dialing out, accessing 911, and intercom calls. Locations that might benefit from these limited features include lobbies, break rooms, and hallways. The Cisco IP Phone 7910G+SW includes a two-port switch for use in applications where you require basic IP Phone functionality and a colocated PC. The following is a brief description of the major features of the Cisco 7910G+SW:
 - Ability to handle low-to-medium telephone usage
 - Single line with call waiting
 - Display area of 2 x 24 inches (5.08 x 60.96 cm)
 - Cisco 10BASE-T/100BASE-T, two-port Ethernet switch
 - Basic features: line, hold, transfer, settings, messages, conference, forward, speed dial, redial
 - Adjustable foot stand (flat to 60 degrees)
 - Basic and optional wall mounting

Midrange and Upper-End Cisco IP Phones

This topic describes the midrange and upper-end Cisco IP Phones and their features.

Midrange and Upper-End Cisco IP Phones

Cisco.com

Cisco IP Phone 7940G	Cisco IP Phone 7960G	Cisco IP Phone 7970G	Cisco IP Phone 7970G
			 10/100/1000

- **Full-featured IP Phones for medium-to-high telephone use**
- **Multiline**
- **Large pixel-based displays**
- **Integral switch**
- **Built-in headset and high-quality speakerphone**
- **Multiprotocol-capable (SCCP, SIP, MGCP)**

© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1—2-5

Cisco designed the IP Phones 7940G, 7960G, and 7970G and 7971G-GE to meet the demand for a corporate-level, full-featured IP Phone for medium-to-high telephone use. A description of features that are common to all three phones follows:

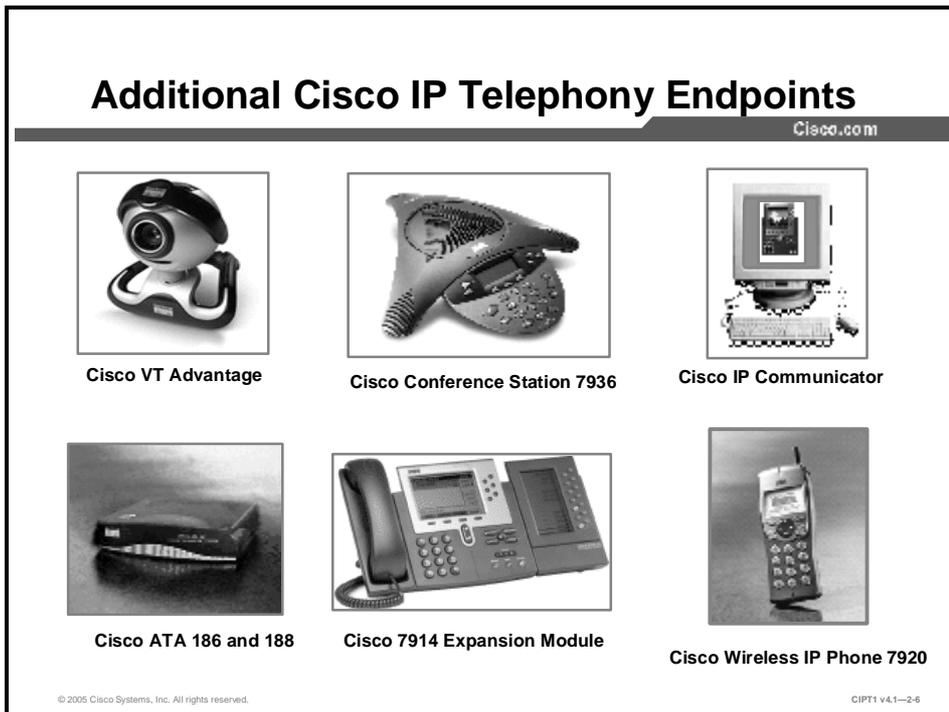
- n Multiline capability
- n Large pixel-based displays, which allow for the inclusion of XML and future features
- n Integrated two-port 10/100-Mbps Ethernet switch
- n Built-in headset connection and quality full-duplex speakerphone (does not come with a headset)
- n Information key for “online” help with features
- n A minimum of 24 user-adjustable ring tones
- n Adjustable foot stand (flat to 60 degrees) and basic or wall mounting
- n SCCP, Media Gateway Control Protocol (MGCP), and SIP support
- n XML service support
- n An EIA/TIA-232 port for options, such as line expansion and security access

Additional details of these phone models follow:

- n **Cisco IP Phone 7940G:** The Cisco IP Phone 7940G is for medium traffic and has these features:
 - Ideal for transaction workers who use cubicle phones
 - Two lines and programmable feature buttons, and four interactive softkeys
 - PoE compatible (Cisco prestandard PoE)
- n **Cisco IP Phone 7960G:** The Cisco IP Phone 7960G is for high or busy telephone traffic and has these features:
 - Ideal for professionals or managers
 - Six lines and programmable feature buttons, and four interactive softkeys
 - PoE compatible (Cisco prestandard PoE)
- n **Cisco IP Phone 7970G:**
 - Ideal for executives, decision makers, and environments with no PCs
 - Eight lines and programmable feature buttons, and five interactive softkeys
 - Color display with touchscreen
 - 3.5-mm stereo jack sockets for connection to PC-style speakers or headphones, and microphone
 - PoE compatible (both Cisco prestandard PoE and IEEE 802.3af PoE)
 - Advanced XML development platform for more dynamic applications
- n **Cisco IP Phone 7971G-GE:**
 - Delivers Gigabit Ethernet bandwidth to the desktop with an integrated 10/100/1000-Mbps switch
 - “Feature identical” to the Cisco IP Phone 7970G
 - PoE compatible (IEEE 802.3af PoE only; does not support Cisco prestandard PoE)

Additional Cisco IP Telephony Endpoints

This topic describes the features and functions of additional Cisco IP telephony endpoints.



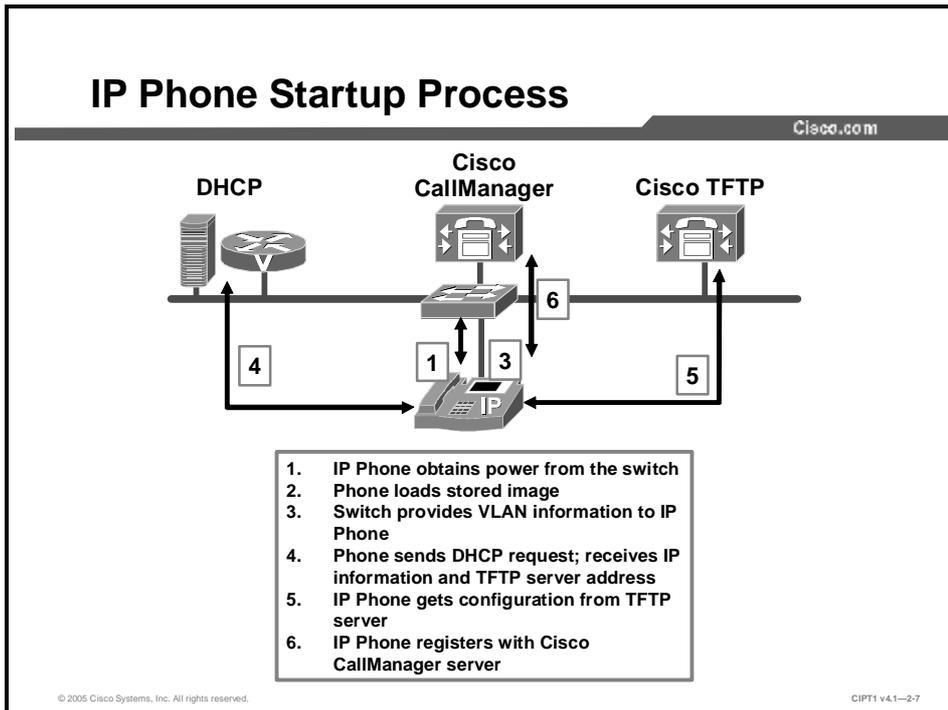
Cisco provides a complete portfolio of IP endpoints to meet business needs for conferencing, wireless voice communications, PC-based voice calls, and connecting analog phones to the VoIP network. These products are as follows:

- n **Cisco VT Advantage:** Cisco VT Advantage is a video telephony solution consisting of the Cisco VT Advantage software application and Cisco VT Camera, a video telephony Universal Serial Bus (USB) camera. With the Cisco VT Camera attached to a PC that is colocated with a Cisco IP Phone, users can place and receive video calls on their enterprise IP telephony network. Users make calls from their Cisco IP Phones using familiar phone interfaces, but calls are enhanced with video on a PC, without requiring any extra button pushing or mouse clicking. When registered to Cisco CallManager, the Cisco VT Advantage-enabled IP Phone has the features and functionality of a full-featured IP videophone. System administrators can provision a Cisco IP Phone with Cisco VT Advantage as they would any other Cisco IP Phone, which can greatly simplify deployment and management.
- n **Cisco IP Conference Station 7936:** The Cisco IP Conference Station 7936 is a full-featured, IP-based, full-duplex, hands-free conference phone for use on desktops, in offices, and in small-to-medium conference rooms. The Cisco IP Conference Station 7936 offers external microphone ports, optional external microphone kit, audio-tuned speaker grill, and a backlit LCD display. The optional microphone kit includes two microphones with 6-foot (1.8288-m) cords so that you can place the microphones across a 12-foot (3.6576-m) area, effectively expanding to a suggested conference room size of 20 x 30 feet (6.096 x 9.144 m). The backlit LCD display improves visibility in low light conditions. The display font size is also adjustable for improved distant viewing.

- n **Cisco IP Communicator:** The Cisco IP Communicator is a Microsoft Windows software-based application that delivers enhanced telephony support through personal computers. This application endows computers with the functionality of Cisco IP Phones and provides high-quality voice calls on the road, in the office, or from wherever users may have access to the corporate network. Cisco IP Communicator has an intuitive design, is easy to use, and delivers convenient access to a host of features, including eight lines and five softkeys. Cisco IP Communicator offers handset, headset, and high-quality speakerphone modes.
- n **Cisco Analog Telephone Adaptor (ATA) 186 and 188:** The Cisco ATA 186 and Cisco ATA 188 interface regular telephones with your IP-based telephony network. These adaptors are useful for customers that have existing analog devices, such as fax machines or telephones, that they do not want to replace after they have migrated to VoIP. The Cisco ATA 186 provides two voice ports, each with its own independent telephone number, and a single 10BASE-T Ethernet port for network connectivity. The Cisco ATA 188 provides two voice ports and two 10/100-Mbps Ethernet connections, which allows for network connectivity and the ability to colocate a network device with the analog voice equipment.
- n **Cisco IP Phone 7914 Expansion Module:** The Cisco IP Phone 7914 Expansion Module extends the capabilities of the Cisco IP Phone 7960 with additional buttons and an LCD display. The Cisco IP Phone 7914 helps administrative assistants and others who must monitor, manage, and cover the various status of a number of calls beyond the six-line capability of the Cisco 7960. This expansion module enables you to add 14 buttons to the existing 6 buttons of the Cisco IP Phone 7960, increasing the total number of buttons to 20 with one module or 34 with two modules. You can use up to two Cisco 7914 Expansion Modules with a Cisco IP Phone 7960.
- n **Cisco Wireless IP Phone 7920:** The Cisco Wireless IP Phone 7920 is an easy-to-use IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco CallManager and the Cisco Aironet 1200, 1100, 350, and 340 Series of Wi-Fi (IEEE 802.11b) access points. The Cisco Wireless IP Phone 7920 is designed for ease of use, with a pixel-based display to access calling features and two softkeys, a four-way rocker switch, a Hold key, a Mute key, and a Menu key that allows quick access to information such as directories, call history, and phone settings.

IP Phone Startup Process

This topic describes the process that a Cisco IP Phone uses to boot and register with the Cisco CallManager.



This figure provides an overview of the startup process for a Cisco IP Phone if you are using a Cisco Catalyst switch that is capable of providing Cisco prestandard Power over Ethernet (PoE).

1. **Obtain power from the switch:** When a Cisco IP Phone is connected to a Cisco Catalyst switch model that is capable of providing inline power (called Power over Ethernet (PoE)), the switch automatically detects an unpowered phone and sends power down the Ethernet cable to the IP Phone. The details of how the switch detects an unpowered IP Phone and how it delivers power to the IP Phone are covered in the lesson “Configuring Cisco Catalyst Switches.”
2. **Load the stored phone image:** The Cisco IP Phone has nonvolatile flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in flash memory. Using this image, the phone initializes its software and hardware.
3. **Configure the VLAN:** After the IP Phone receives power and boots, the switch sends a Cisco Discovery Protocol packet to the IP Phone. This Cisco Discovery Protocol packet provides the IP Phone with voice VLAN information, if that feature has been configured.
4. **Obtain the IP address and TFTP server address:** Next, the IP Phone broadcasts a request to a DHCP server. The DHCP server responds to the IP Phone with a minimum of an IP address, a subnet mask, and the IP address of the Cisco TFTP server.

5. **Contact the TFTP server for configuration:** The IP Phone then contacts the Cisco TFTP server. The TFTP server has configuration files (.cnf file format or .cnf.xml) for telephony devices, which define parameters for connecting to Cisco CallManager. The TFTP server sends the configuration information for that IP Phone, which contains an ordered list of up to three Cisco CallManagers. In general, any time that you make a change in Cisco CallManager that requires a phone (device) to be reset, a change has been made to the configuration file of that phone. If a phone has an XML-compatible load, it requests an XMLDefault.cnf.xml configuration file; otherwise, it requests a .cnf file.
6. **If you have enabled auto-registration in Cisco CallManager, the phones access a default configuration file (sepdefault.cnf.xml) from the TFTP server.** If you have manually entered the phones into the Cisco CallManager database, the phone accesses a .cnf.xml file that corresponds to its device name. The .cnf.xml file also contains the information that tells the phone which image load that it should be running. If this image load differs from the one that is currently loaded on the phone, the phone contacts the TFTP server to request the new image file, which is stored as a .bin file.
7. **Register with Cisco CallManager:** After obtaining the file from the TFTP server, the phone attempts to make a TCP connection to a Cisco CallManager, starting with the highest-priority Cisco CallManager in its list.

Cisco IP Phone Codec Support

This topic describes the codecs that are supported by Cisco IP Phones.

Cisco IP Phone Codec Support

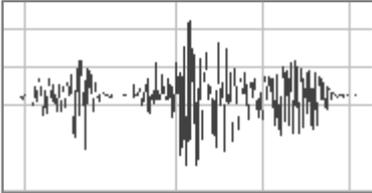
Cisco.com

Audio codecs:

- Potentially able to compress audio signals

Cisco IP Phones support:

- **G.711: 64 kbps**
- **G.729: 8 kbps**



© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1—2-8

Before a VoIP device is able to stream audio, the analog audio signal must be converted to a digitized format. This is accomplished by an audio codec, which digitizes the audio input at the transmitting end and converts the digital stream back to analog audio at the receiving end.

Because converted audio streams can consume a significant amount of bandwidth, many of the audio codecs also provide a level of compression, which can considerably reduce the bandwidth that they consume. However, compression can cause degraded voice quality, which is why the different audio codecs offer different levels of compression.

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standards committee specifies several standards (called recommendations) for audio codecs. Cisco IP Phones natively support two primary codecs: G.711 and G.729. The G.711 and G.729 codecs deliver relatively equal sound quality (both considered toll quality), with G.711 scoring slightly higher than G.729 in a mean opinion score (MOS) test. Because of this similarity, some network administrators choose to operate an entirely G.729-based network, while others choose to implement G.729 over the WAN and G.711 on the LAN.

Although this configuration is ideal for many network environments, you may eventually encounter a codec mismatch. A codec mismatch occurs when two devices cannot negotiate a common codec or when the network administrator has forbidden the use of their common codec, such as using G.711 over the WAN. Regardless of the cause, you now have a need for transcoding. Transcoding resources perform conversions between the audio codecs. These resources are often costly and can introduce significant delay and quality degradation into your IP telephony network. When designing a voice network, you should attempt to limit the amount of transcoding that takes place between devices.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Cisco IP Phones are display-based, support customization, have inline power, and provide support for the G.711 and G.729 audio codecs.**
- **Entry-level Cisco IP Phones include the Cisco IP Phone 7902G, 7905G, 7910G+SW, and 7912G.**
- **Midrange and upper-end Cisco IP Phones include the Cisco IP Phone 7940G, 7960G, 7970G, and 7971G-GE.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--2-9

Summary (Cont.)

Cisco.com

- **Additional IP telephony devices include the Cisco Conference Station 7936, Cisco IP Communicator, Cisco ATA 186 and 188, and Cisco 7914 Expansion Module.**
- **An IP Phone follows a specific process each time that it boots.**
- **Audio codecs convert analog voice signals to a digitized stream and compress the output to save bandwidth. Cisco IP Phones support the G.711 and G.729 codecs.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--2-10

References

For additional information, refer to these resources:

- n Cisco Systems, Inc. Cisco 7900 Series IP Phones product index page with links to product models, technical documentation, and Software Center.
<http://www.cisco.com/en/US/products/hw/phones/ps379/index.html>.
- n Cisco Systems, Inc. Cisco IP Phones and Services documentation.
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.

Lesson 2-2

Configuring Cisco CallManager to Support IP Phones

Overview

Configuring Cisco CallManager to support Cisco IP Phones is a critical part of implementing a Cisco IP telephony network. This lesson prepares you for the initial IP Phone setup and configuration and for the maintenance of existing IP Phones.

This lesson describes the Cisco CallManager configuration to support Cisco IP Phones. This lesson will teach you how to configure Cisco CallManager to manually and automatically add IP Phones and assign directory numbers (DNs). You will also learn how to configure device pools to provide a convenient way to define a set of common characteristics that can be assigned to devices, such as date or time zone, codec use, and other functionalities.

Objectives

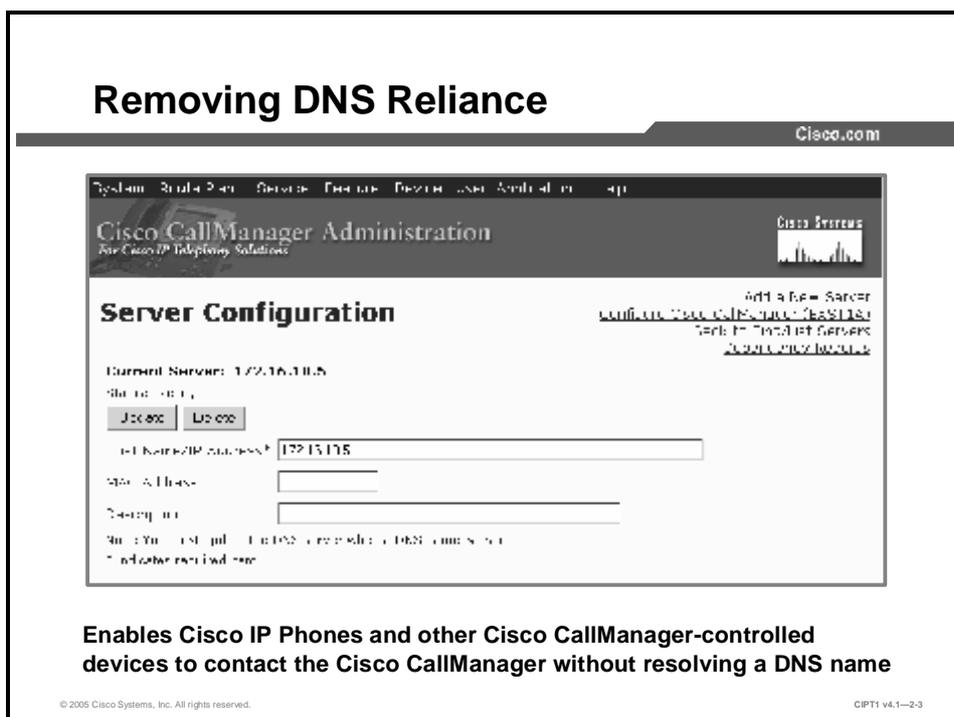
Upon completing this lesson, you will be able to configure Cisco CallManager to support Cisco IP Phones, including server configuration, device pools, phone button templates, and DN. This ability includes being able to meet these objectives:

- n Configure Cisco CallManager to eliminate IP Phone reliance on DNS
- n Configure device pools in Cisco CallManager to define sets of common characteristics for IP Phones
- n Use Cisco CallManager default phone button templates and create new templates to assign a common button configuration to a large number of IP Phones
- n Manually add and configure IP Phones in Cisco CallManager and assign DNs

- n Configure Cisco CallManager to support IP Phone auto-registration to automatically issue directory numbers to new IP Phones

Server Configuration

This topic discusses server configuration in Cisco CallManager Administration.



Changing the name of the selected server to the IP address of the server in the Cisco CallManager Administration window is the first step in configuring Cisco CallManager to support Cisco IP Phones.

Renaming the server to the IP address has the following benefits:

- n It allows IP Phones and other devices to find Cisco CallManager on the network without having to query the Domain Name System (DNS) server to help resolve the server name to an IP address.
- n It prevents the IP telephony network from failing if the IP Phones lose the connection to the DNS server.
- n It decreases the time that is required when a device attempts to contact Cisco CallManager.

Complete these steps to eliminate DNS reliance:

Step 5 In Cisco CallManager Administration, choose **System > Server**.

The Find and List Servers window appears.

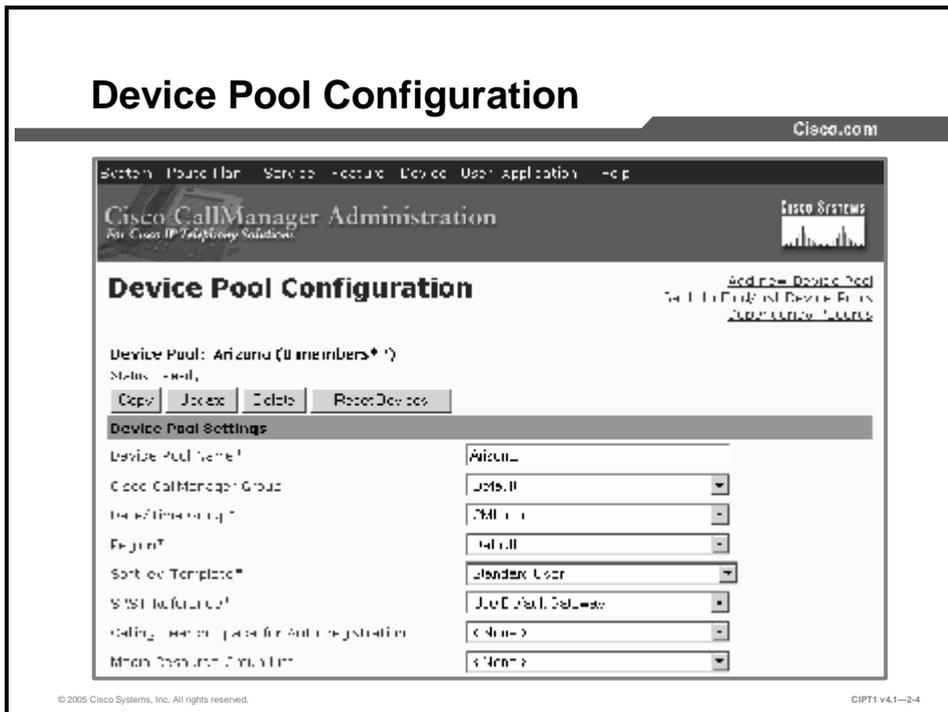
Step 6 Click a server name.

The Server Configuration window appears.

Step 7 Remove the hostname and enter the IP address for the server in the Host Name/IP Address field. Click **Update**.

Configuring Device Pools

This topic describes device pool configuration.



Device pools provide a convenient way to define a set of common characteristics that can be assigned to devices, such as IP Phones, instead of assigning individual characteristics to individual phones. Device pools enable you simply assign the phone to the device pool so that the phone automatically inherits the common configuration items. You must configure the device pool for Cisco IP Phones before adding them to the network.

To create a new device pool, you must first create (or use default settings where applicable) the following minimal mandatory components:

- n Cisco CallManager group
- n Date/time group
- n Region
- n Softkey template
- n Cisco Survivable Remote Site Telephony (SRST) reference: The SRST Reference field allows you to specify the IP address of the Cisco SRST router. Cisco SRST enables routers to provide call-handling support for Cisco IP phones when they lose their connection to remote Cisco CallManager installations or when the WAN connection is down.

These components (except for the SRST reference) are covered later in this lesson. SRST is covered later in the course.

The device pool combines all of the individual configurations that you have created into a single entity. You will eventually assign this entity to individual devices, such as IP Phones. This process will configure these devices with most of the configuration elements that they need to operate efficiently in your IP telephony network.

Complete these steps to create the device pool:

- Step 1** Choose **System > Device Pool**. The Find and List Device Pools window opens.
- Step 2** Click the **Add a New Device Pool** link to open the Device Pool Configuration window. Choose, at a minimum, the Cisco CallManager group, date/time group, region, and softkey template.

Example: Device Pool Configuration

Configuring 100 different Cisco IP Phones to use the Arizona time zone, the English language, and the classical-style music on hold (MOH) option is tedious. Instead, you can create a device pool, named “Arizona,” that configures the correct time zone, language, and MOH, and you can make a single assignment of the Arizona device pool to each IP Phone.

The configuration table here shows the device characteristics that you can specify for a device pool. You must configure these items before you configure a device pool if you want to choose the items for the device pool.

Device Pool Configuration Items

Field	Description
Device Pool Name*	Describes a name for the device pool.
Cisco CallManager Group*	Selects a redundancy group for the device pool. This redundancy group can contain a maximum of three redundant Cisco CallManager servers.
Date/Time Group*	Assigns the correct time zone to the device.
Region*	Determines the coder-decoder (codec) selection used by the device, depending on the end location of the call.
Softkey Template*	Defines the type and order of the softkeys that are displayed on the liquid crystal display (LCD) of a Cisco IP Phone.
SRST Reference*	Configures SRST and selects the gateway that will support the device if the connection to the Cisco CallManager is lost.
Calling Search Space for Auto-Registration	Defines whom an IP Phone is able to call if it auto-registers with the Cisco CallManager.
Media Resource Group List	Assigns media resource support to a device for functions such as conferencing, transcoding, or MOH.
Network Hold MOH Audio Source	Selects the audio that Cisco CallManager should play when a user presses the Transfer or Conference button on the Cisco IP Phone.
User Hold MOH Audio Source	Selects the audio that Cisco CallManager should play when a user presses the Hold button on the Cisco IP Phone.
Network Locale	Defines the tones and cadences that the device uses.
User Locale	Defines the language that the device uses.
Connection Monitor Duration	Defines the amount of time that the IP phone monitors its connection to Cisco CallManager before it unregisters from SRST and re-registers to Cisco CallManager. This is to ensure that the link is stable (not "flapping"). The default for the enterprise parameter specifies 120 seconds, which can be modified on a device-pool basis or left at the default value.
MLPP Precedence and Preemption Information	Used to manage Multilevel Precedence and Preemption (MLPP) settings: <ul style="list-style-type: none"> n MLPP Indication: Specifies whether devices in the device pool that are capable of playing precedence tones will use the capability when the devices plan an MLPP precedence call n MLPP Preemption: Specifies whether devices in the device pool that are capable of pre-empting calls in progress will use the capability when the devices plan an MLPP precedence call n MLPP Domain: A hexadecimal value for the MLPP domain that is associated with the device pool

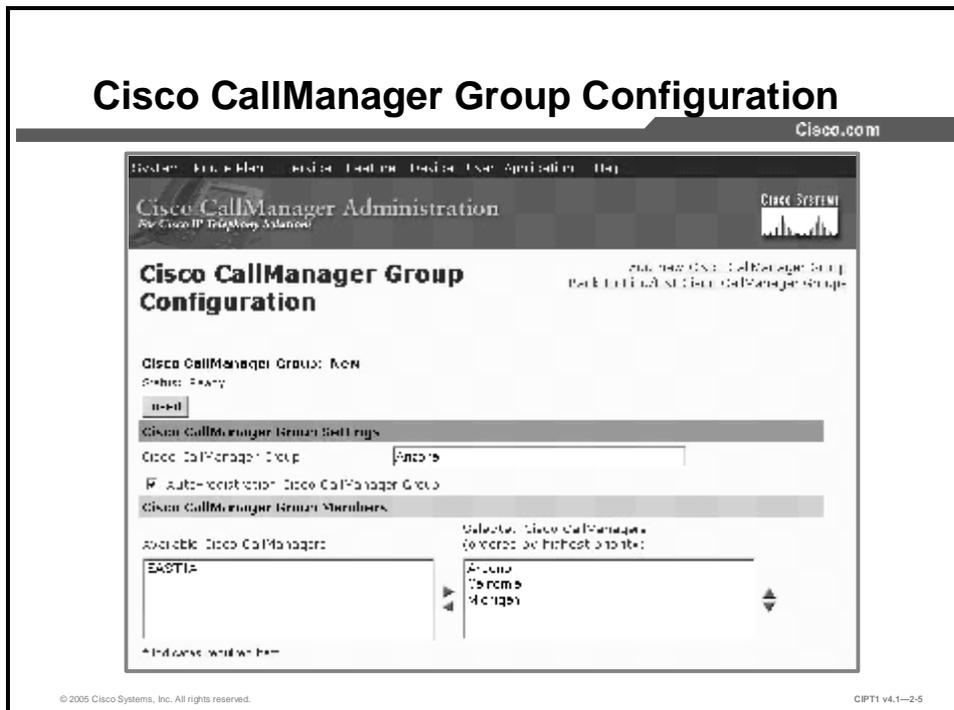
Note An asterisk (*) Indicates a required field.

If you make changes to a device pool, you must reset the devices in that device pool before the changes will take effect.

You cannot delete a device pool that has been assigned to any device or one that is used for device defaults configuration. To find out which devices are using the device pool, click the **Dependency Records** link in the Device Pool Configuration window. If you try to delete a device pool that is in use, an error message is displayed. Before deleting a device pool that is currently in use, you must perform one of the following tasks:

- n Update the devices to assign them to a different device pool.
- n Delete the devices that are assigned to the device pool that you want to delete.

Individual components of a device pool are explored in the following subtopics.



A Cisco CallManager group specifies a prioritized list of Cisco CallManager servers to register to, with a maximum of three in the list. The first Cisco CallManager in the list serves as the primary Cisco CallManager for devices that are assigned to that group. The other members of the group serve as the secondary and tertiary backups. Changes to the Cisco CallManager group affect the configuration file that is given to Cisco IP Phones by the TFTP server when they initially boot.

Example: Cisco CallManager Group Configuration

In the figure, the Cisco CallManager group, called “Arizona,” has three Cisco CallManager servers. You assign the Cisco CallManager group to a device pool, and you then assign this device pool to the Cisco IP Phone. The IP Phone uses the Arizona Cisco CallManager as its primary Cisco CallManager, the California Cisco CallManager as its secondary, and the Michigan Cisco CallManager as its tertiary. Cisco CallManager Administration will present an error message if you attempt to add a fourth Cisco CallManager (for example, the EAST1A Cisco CallManager) to the list.

Checking the Auto-Registration Cisco CallManager Group check box enables the Cisco CallManager to place any new IP Phones that auto-register (IP Phones that are added to the network without manual administrative configuration) into this group by default.

Complete these steps to configure a Cisco CallManager group:

- Step 1** Choose **System > Cisco CallManager Group**. The default group that was created by Cisco CallManager during the installation appears.
- Step 2** Choose **Add New Cisco CallManager Group** to create a new Cisco CallManager group.
- Step 3** Move the existing Cisco CallManager servers using the Left and Right arrows, and change the order of Cisco CallManager servers using the Up and Down arrows.

Date/Time Group Configuration

Cisco.com

System | Run | Plan | Settings | Features | Devices | User Applications | Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

Date/Time Group Configuration [Add a New Date/Time Group](#)
[Back](#) | [Home](#) | [Date/Time Groups](#)

Date/Time Group: New
Status: Ready

Name: CMLocal

Time Zone: Pacific Time (US & Canada) (GMT-08:00)

Separator: 1000 (applies to Date Format only)

Date Format: M-D-Y

Time Format: 12-hour

* Time zones required for:

© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1-2-6

Date/time groups define time zones for the various devices that are connected to Cisco CallManager. You can assign each device to only one device pool. As a result, the device has only one date/time group.

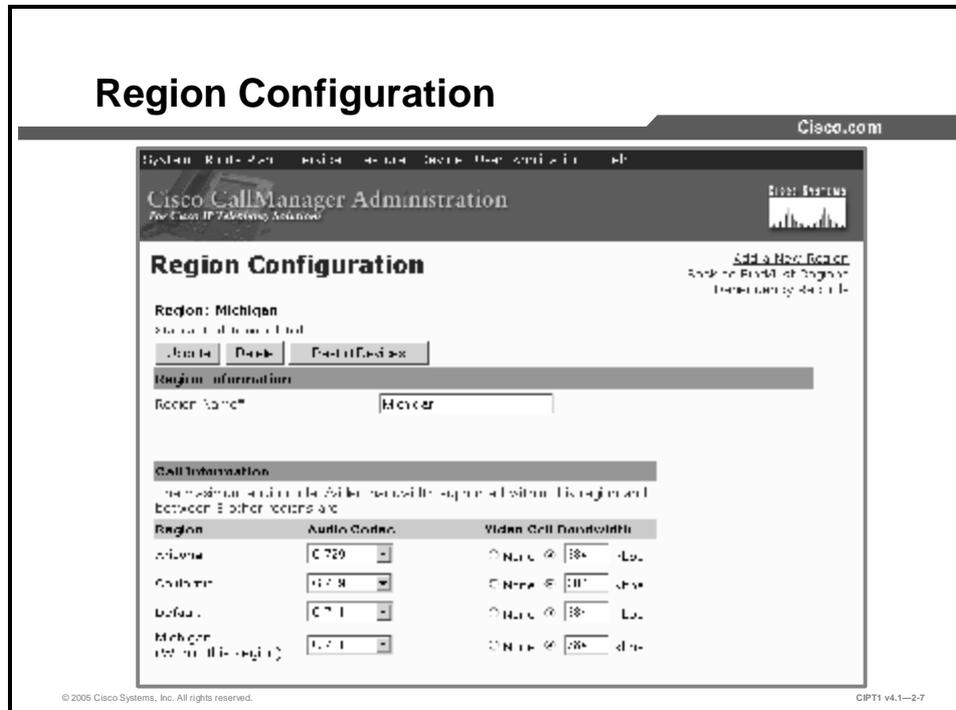
Cisco CallManager has a default date/time group called CMLocal. The CMLocal date/time group synchronizes to the active date and time of the operating system on the Cisco CallManager server. You can change the settings for CMLocal after installing Cisco CallManager.

Complete these steps to configure the date/time group:

- Step 1** Choose **System > Date/Time Group**. The default CMLocal group appears.
- Step 2** Choose **Add a New Date/Time Group** to insert additional date/time groups as required.

Note For a worldwide distribution of Cisco IP Phones, you may want to create one named date/time group for each of the 24 time zones.

Region Configuration



When you create a region, you specify the audio codec that can be used for calls between devices (such as IP Phones) within that region and between that region and other regions. As of Cisco CallManager Release 4.0, you can also specify the video call bandwidth.

You can create regions to modify the codec selection for any reason; however, most network administrators create regions based on geographical areas. The default voice codec for all calls through Cisco CallManager is G.711. If you do not plan to use any other voice codec, you do not need to use regions. The system will use the default region.

Example: Region Configuration

In the figure shown here, there are four regions: Arizona, California, Default, and Michigan; the configuration of the Michigan region is displayed. If a device that is assigned to the Michigan region calls another device in the Michigan region, the devices use the G.711 codec. However, if a device assigned to the Michigan region calls a device that is assigned to the Arizona region, the devices use the G.729 codec. Cisco CallManager creates the Default region during the installation process. You can rename the Default region to a more logical name to avoid confusion, or you can ignore it and use only regions that you have created.

Complete these steps to configure a region:

- Step 1** Choose **System > Region**. The default region that was created during the Cisco CallManager installation appears.
- Step 2** Choose **Add a New Region** to configure the regions, and choose the codec and video bandwidth as appropriate between the regions.

Softkey Template Configuration

Cisco.com

System Tools Port Profiles Feature Groups User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

Find and List Softkey Templates [Add a New Softkey Template](#)

5 matching record(s) for Name begins with ""

Find softkey templates using: Name: [] Degree: [] [Find]

and show [20] items per page. Where softkey template is [SPT] []
to list them, click find at bottom of search box.

Matching record(s) 1 to 5 of 5

Name	Description	Copy
Standard IPMA Assistant	Standard template for IPMA assistant features	[Copy]
Standard Softkey	Standard softkey template for CallManager	[Copy]
Standard Feature	Standard Softkey Template for IP Conference	[Copy]
Standard IPMA Manager	Standard template for IPMA management	[Copy]
Standard IPMA Shared Mode Manager	Standard template for IPMA shared mode	[Copy]

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1-2-8

The Softkey Template Configuration window allows the administrator to manage the on-screen softkeys that the Cisco IP Phones support (such as the Cisco IP Phone 7960 and 7940 models). You can configure these softkeys with many Cisco CallManager functions and features.

Applications that support softkeys can have one or more standard softkey templates that are associated with them; for example, Cisco IP Manager Assistant (IPMA) has the Standard IPMA Assistant, the Standard IPMA Manager, and the Standard IPMA Manager Shared Mode softkey templates associated with it. You cannot modify standard softkey templates. First you copy the template and then modify the copy.

Choose **Device > Device Settings > Softkey Templates** to access the Softkey Template Configuration window in Cisco CallManager Administration.

IP Phone Button Templates

This topic discusses the configuration and application of the Cisco IP Phone button templates.

IP Phone Button Templates

Cisco.com

- **Default 7960 template is 2 lines, 4 speed dials**
- **Prepare for anything; configure all possible combinations:**
 - 1 line, 5 speed dials
 - 3 lines, 3 speed dials
 - 4 lines, 2 speed dials
 - 5 lines, 1 speed dial
 - 6 lines, 0 speed dials



© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1--2-9

Creating and using templates provides a fast way to assign a common button configuration to a large number of Cisco IP Phones. Cisco CallManager includes several default phone button templates. When adding IP Phones, you can assign one of these templates to each IP Phone or assign custom templates that you have created.

You must assign at least one line per IP Phone; usually this line is button 1. Depending on the Cisco IP Phone model, you can assign additional lines. IP Phones generally have several features, such as speed dial and call forwarding, assigned to the remaining buttons.

Before adding any IP Phones to the system, create phone button templates with all of the possible combinations for all IP Phone models. An IP Phone model may have various combinations; for example, a Cisco IP Phone 7960 supports six lines and can use the following phone button template combinations:

- n One line, five speed dial buttons
- n Two lines, four speed dial buttons (default)
- n Three lines, three speed dial buttons
- n Four lines, two speed dial buttons
- n Five lines, one speed dial button
- n Six lines, no speed dial button

IP Phone Button Template Names

Cisco.com

- **Use the model number, line and speed dial settings in the name:**
 - 7960 1-5
 - 7960 3-3
- **Template updates affect the IP Phones that use that template**
- **Renaming a template does not affect the IP Phones using that template**
- **Cannot delete a template assigned to one or more devices**



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-10

Create easily recognizable naming conventions for the phone button template. A suggested best practice is to use the model number of the Cisco IP Phone followed by the number of lines and speed dials. For example, a phone button template named “7960 1-5” would indicate a Cisco 7960 IP Phone with one line and five speed-dial buttons.

To create a template, copy an existing template and assign a unique name to the template. You can make changes to the default templates that are included with Cisco CallManager or to the custom templates that you have created.

You can rename existing templates and modify them to create new ones. You can also update custom templates to add or remove features, lines, or speed dial buttons. When you update a template, the change affects all of the IP Phones that use it.

Renaming a template does not affect the IP Phones that use that template. All Cisco IP Phones that use this template continue to use this template after you rename it.

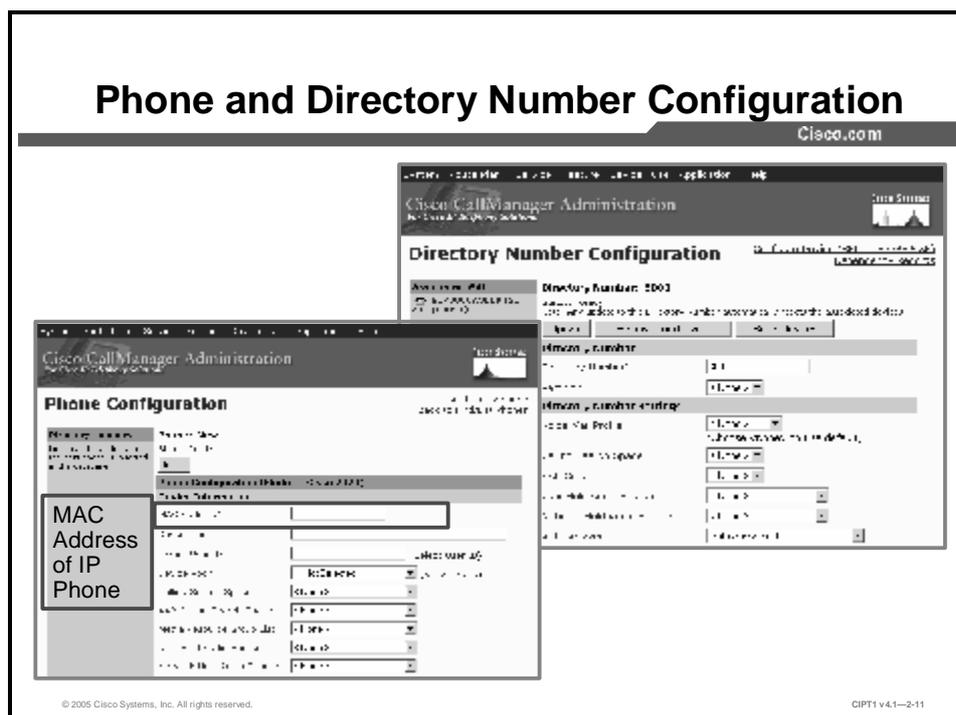
You can delete IP Phone templates that are not currently assigned to any IP Phone in your system. You cannot delete a template that is assigned to one or more devices. Currently, there is not an easy way to query whether a template is in use or not. Before you can delete a template, you must reassign all of the Cisco IP Phones that are using the template to a different phone button template.

Example: Naming a Phone Button Template

If you have a special request or only a limited number of users who need three lines and three speed dial buttons on the Cisco IP Phone 7960G, you can create a phone button template that supports three lines and three speed dials, name the template “7960 3-3,” and quickly assign the phone button template 7960 3-3 to the IP Phones.

Manual IP Phone and Directory Number Configuration

This topic discusses manual Cisco IP Phone and DN configuration in Cisco CallManager Administration.



Manually adding new IP Phones to the network is often tedious, but it can constitute a large part of day-to-day voice network management. The Bulk Administration Tool (BAT) allows you to add a large number of IP Phones to the Cisco CallManager database at once, but BAT is not appropriate for adding or modifying a single IP Phone for a new employee.

Cisco CallManager uses the IP Phone MAC address to track the phone in the voice network. Cisco CallManager ties all IP Phone configuration settings to the IP Phone MAC address. Before you can perform any configuration on a Cisco IP Phone through Cisco CallManager, you must find the MAC address of that IP Phone. Use the following guidelines to locate a MAC address:

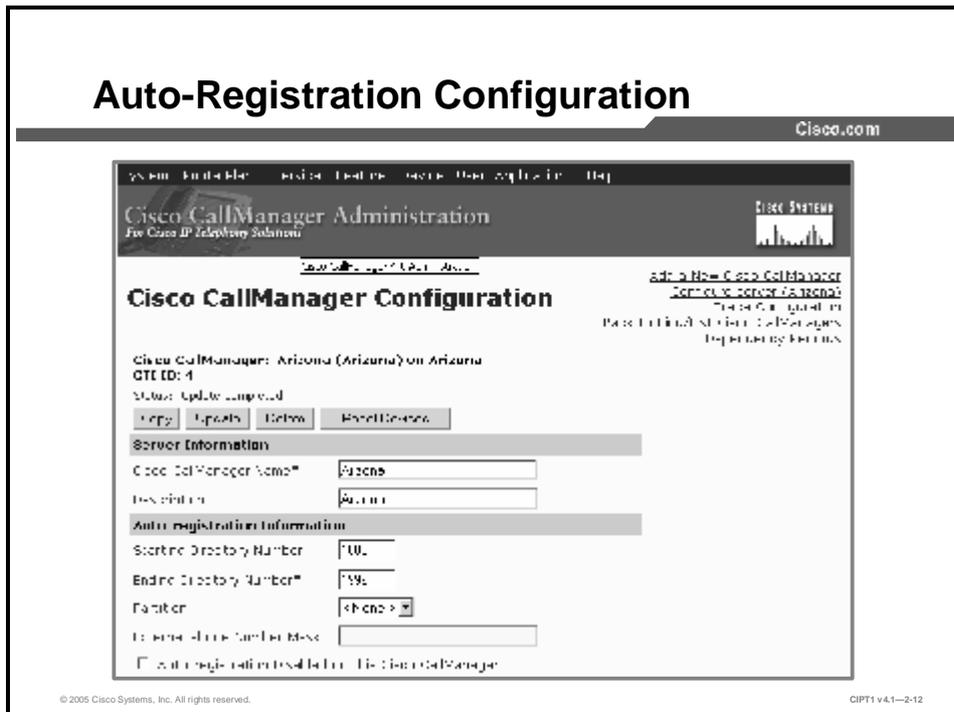
- n You can find the MAC address in the text and Universal Product Code (UPC) form, which is imprinted on the shipping box for the IP Phone. Some administrators use bar code scanners to simplify the process of adding multiple IP Phones.
- n You can also find the MAC address in the text and UPC form on the back of the IP Phone, on a sticker near the bottom.
- n If you boot the IP Phone, you can press the **Settings** button on the face of the phone. Use the arrow keys to navigate, and choose **Network Configuration**. The MAC address will be displayed on line 3 of the network configuration.

You can continue the Cisco IP Phone configuration on the Cisco CallManager configuration after you have the MAC address of the IP Phone, as follows:

- Step 1** In Cisco CallManager Administration, choose **Device > Phone** to open the Find and List Phones window.
- Step 2** Choose **Add a New Phone** in the upper-right corner of the window.
- Step 3** Choose the model of the IP Phone from the drop-down menu, and click **Next**.
- Step 4** At a minimum, you must configure the MAC Address and Device Pool fields; then click **Insert**.
- Step 5** Cisco CallManager prompts you to add a DN for line 1; then click **OK**.
- Step 6** When the Directory Number Configuration window appears, enter the DN of the IP Phone in the appropriate field, and click **Insert**.

Configuring IP Phone Auto-Registration

This topic describes how to configure Cisco CallManager for auto-registering Cisco IP Phones.



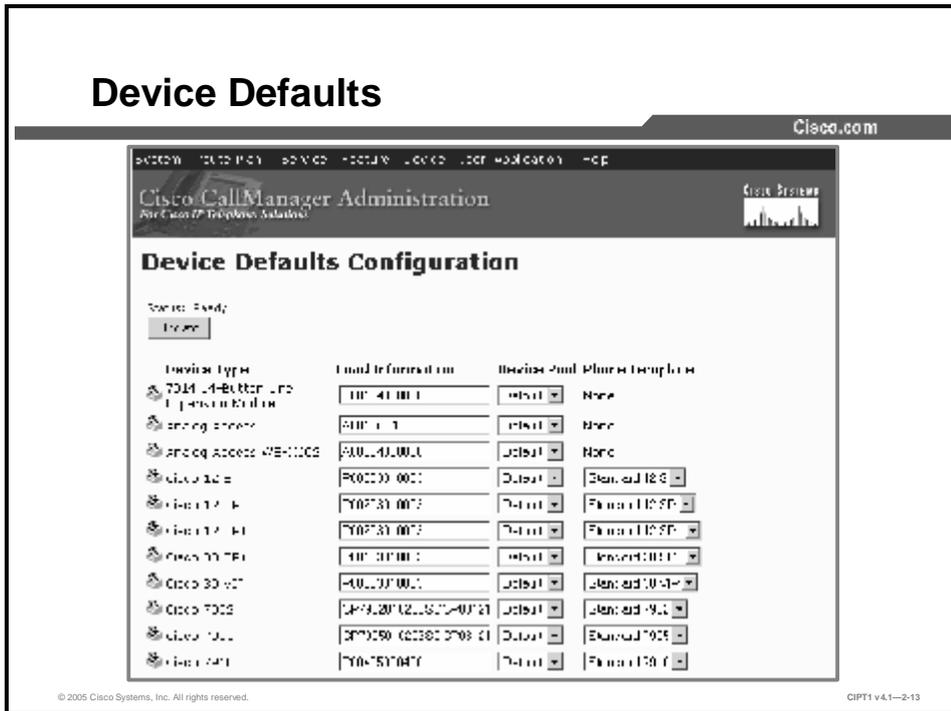
Auto-registration allows Cisco CallManager to issue extension numbers to new IP Phones, which is similar to the way in which the Dynamic Host Control Protocol (DHCP) server issues IP addresses. When a new IP Phone boots and attempts to register with Cisco CallManager for the first time, Cisco CallManager issues an extension number from a configured range. After Cisco CallManager issues the extension, it records the extension number to the MAC address mapping in the Microsoft Structured Query Language (SQL) database.

Although auto-registration simplifies the process of deploying a new IP telephony network, it is an option that is available only in some new IP telephony deployments. Because administrators deploy most IP telephony networks as a migration from a PBX environment, users have existing telephone extensions. These existing telephone extensions typically map to Direct Inward Dial (DID) numbers from the Public Switched Telephone Network (PSTN) and cannot change. Therefore, these IP telephony deployments usually use manual configuration rather than auto-registration.

You should carefully evaluate auto-registration before implementing it because its use can pose a security risk to the network. Auto-registration allows anyone with physical access to the voice network to connect an IP phone and use it, whether authorized or not. For this reason, many organizations, as part of their security policy, disable the use of auto-registration or use auto-registration in a secure staging environment for initial Cisco CallManager configuration.

Complete these steps to configure the Cisco CallManager server to support auto-registration:

- Step 1** From Cisco CallManager Administration, choose **System > Cisco CallManager**.
- Step 2** From the list of Cisco CallManager servers, select the server that you want to support auto-registration.
- Step 3** Under the Auto-Registration Information Configuration section, enter the appropriate DN range in the Starting and Ending Directory Number fields.
- Step 4** Ensure that the Auto-Registration Disabled on this Cisco CallManager check box is unchecked.



Use device defaults to set the default characteristics of each type of device that registers with a Cisco CallManager. The device defaults for a device type apply to all auto-registered devices of that type within a Cisco CallManager cluster. You can set the following device defaults for each device type to which they apply:

- n **Device load:** Lists the firmware load that is used with a particular type of hardware device
- n **Device pool:** Allows you to select the device pool that is associated with each type of device
- n **Phone button template:** Indicates the phone button template that is used by each type of device

When a device auto-registers with a Cisco CallManager, it acquires the device default settings for its device type. After a device registers, you can update its configuration individually to change the device settings.

Installing Cisco CallManager automatically sets device defaults. You cannot create new device defaults or delete existing ones, but you can change the default settings.

Complete these steps to update the device defaults:

- Step 1** In Cisco CallManager Administration, choose **System > Device Defaults** to open the Device Defaults Configuration window.
- Step 1** In the Device Defaults Configuration window, modify the appropriate settings for the device that you want to change.
- Step 2** Click **Update** to save the changes in the Cisco CallManager configuration database.
- Step 3** Click the **Reset** icon to the left of the device name to reset all the devices of that type and load the new defaults on all Cisco CallManager servers in the cluster.

If you choose not to reset all devices of that type, only new devices that are added after you change the device defaults receive the latest defaults.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Assigning an IP address to Cisco CallManager eliminates IP Phone reliance on DNS.**
- **Device pools simplify configuration by allowing you to define sets of common characteristics for devices.**
- **Creating and using IP Phone button templates provides a fast way to assign a common button configuration to a large number of IP Phones.**
- **Manually configuring the IP Phone is appropriate when you want to add or modify a single or a few IP Phones.**
- **Using IP Phone auto-registration allows you to automatically issue extension numbers and a default configuration to new phones.**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1—2-14

References

For additional information, refer to these resources:

- n Cisco Systems, Inc. *Cisco CallManager System Guide, Release 4.1(3)*, “System Configuration Overview” and “System-Level Configuration Settings.”
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ee.html.
- n Cisco Systems, Inc. *Cisco CallManager Administration Guide, Release 4.1(3)*.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ec.html.

Lesson 2-3

Configuring Cisco Catalyst Switches

Overview

Deploying IP telephony requires planning how the IP Phones will be powered and how the voice network will be combined with the data network while ensuring that the data traffic does not degrade the quality of the voice calls.

Cisco Catalyst switches provide three features that aid an IP telephony deployment: inline power, voice VLANs, and class of service (CoS). Using the Cisco Catalyst switch to power IP Phones can save on wiring costs and simplify management. Enabling multiple VLANs in a single port and placing voice packets in one VLAN and data in another VLAN saves money by reducing the number of switch ports. Extending CoS to the IP Phone improves voice quality by ensuring that voice packets receive priority over data.

This lesson discusses the three major functions that Cisco Catalyst switches perform in an IP telephony network and describes how to configure a Cisco Catalyst switch to enable these functions.

Objectives

Upon completing this lesson, you will be able to implement a Cisco Catalyst switch in an IP telephony network to provide PoE to IP Phones, prioritize voice traffic, and create a separate voice VLAN for IP Phones. This ability includes being able to meet these objectives:

- n Identify the functions that Cisco Catalyst switches perform in a Cisco IP telephony solution
- n Describe the three options for powering Cisco IP Phones
- n Describe the two types of PoE that Cisco Catalyst switches provide
- n Identify the Cisco Catalyst switches that support PoE
- n Identify the commands to configure PoE on Cisco Catalyst switches

- n Configure dual VLANs on a single port on a Cisco Catalyst switch so that the IP Phones reside in a separate VLAN
- n Configure CoS on Cisco Catalyst switches so that voice traffic has priority over data traffic as it travels throughout the network

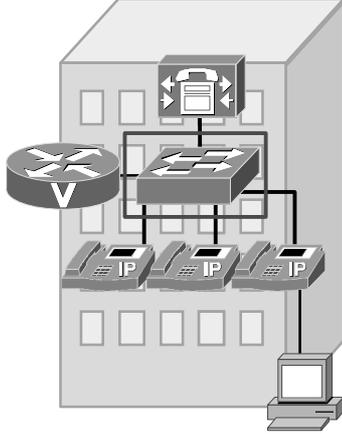
Catalyst Switch Role in IP Telephony

This topic describes the role of Cisco Catalyst switches in the IP telephony infrastructure.

Cisco Catalyst Switch Role in IP Telephony

Cisco.com

- **Supplies inline power to IP Phones**
- **Supports voice and data VLANs on a single port**
- **Prioritizes voice traffic with class of service (CoS) marking**



The diagram shows a Cisco Catalyst switch rack. A circular icon with a 'V' and a star is connected to the top of the switch. Below the switch, three IP phones are connected to the switch. A computer monitor is also connected to the switch. The diagram illustrates the switch's role in providing power and managing traffic for IP telephony.

© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1--2-3

Cisco voice-capable Catalyst switches can provide three primary features to assist you with your IP telephony deployment:

- n **Inline power:** Inline power capabilities allow a Cisco Catalyst switch to send power through the Ethernet copper to a Cisco IP Phone or other inline power-compatible devices (such as wireless access points) without the need for an external power supply. Inline power is also referred to as Power over Ethernet (PoE). Inline power was developed in 2000 by Cisco to support the emerging IP telephony solution.
- n **Auxiliary VLAN support:** Auxiliary VLAN support allows a switch to support multiple VLANs on a single port. You can connect one or more network devices to the back of the Cisco IP Phone because some Cisco IP Phones have built-in switches. Auxiliary VLANs allow you to place the IP Phone, and the devices that are attached through the IP Phone, on separate VLANs.
- n **Class of service (CoS) marking:** CoS marking is data link layer (Layer 2) marking that is used to prioritize network traffic. Prioritizing voice traffic is critical in IP telephony networks. If voice traffic is not given priority, poor voice quality may result because voice frames wait in the switch queue behind large data frames. The switch can use existing CoS marking to prioritize network traffic and can also classify and mark traffic that it receives.

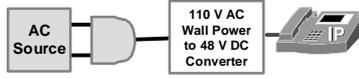
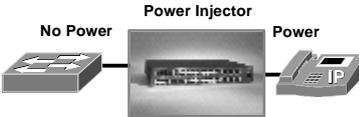
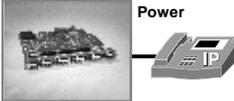
Powering the Cisco IP Phone

This topic describes the three options for powering Cisco IP Phones.

Three Ways to Power IP Phones

Cisco.com

- **Power over Ethernet (PoE):**
 - Needs PoE line cards or PoE ports for Cisco Catalyst switches
 - Delivers -48 V DC over data pairs (pins 1, 2, 3, and 6)
- **Midspan power injection:**
 - Needs external power source equipment
 - Delivers -48 V DC over spare pairs (pins 4, 5, 7, and 8)
- **Wall power:**
 - Needs DC converter for connecting IP Phone to wall outlet



© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1—2-4

Most Cisco IP Phone models are capable of using the following three options for power:

- n **PoE:** With PoE, the phone plugs into the data jack that connects to the switch, and the user PC in turn connects to the IP Phone. Power-sourcing equipment (PSE), such as Cisco Catalyst PoE-capable modular and fixed-configuration switches, insert power over the Ethernet cable to the powered device, for example, an IP Phone or 802.11 wireless access point.
- n **Midspan power injection:** Because many switches do not support PoE, the powered device must support a midspan power source. This midspan device sits between the LAN switch and the powered device and inserts power on the Ethernet cable to the powered device. A technical difference between the midspan and inline power mechanism is that power is delivered on the spare pairs (pins 4, 5, 7, and 8). An example of midspan PSE is a Cisco Catalyst Inline Power Patch Panel.
- n **Wall power:** Wall power needs a DC converter for connecting the IP Phone to a wall outlet.

Note You must order the wall power supply separately from the Cisco IP Phone.

Types of PoE Delivery

This topic discusses the two types of PoE delivery that Cisco Catalyst switches can provide.

Two Types of PoE Delivery

Cisco.com

Cisco original implementation:

- Provides -48 V DC at up to 6.3 to 7.7 W per port over data pins 1, 2, 3, and 6.
- Supports most Cisco devices (IP Phones and wireless access points).
- Uses a Cisco proprietary method of determining if an attached device requires power. Power is delivered only to devices that require power.

IEEE 802.3af Power over Ethernet:

- Specifies -48 V DC at up to 15.4 W per port over data pins 1, 2, 3, and 6 or spare pins 4, 5, 7, and 8.
- Enables a new range of Ethernet-powered devices because of increased power.
- Standardizes the method of determining if an attached device requires power. Power is delivered only to devices that require power.
- Has several optional elements, including power classification.

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1--2-5

Cisco provides two types of inline power delivery: the Cisco original implementation and the IEEE 802.3af PoE standard. You can refer to both inline power types as PoE:

- n **Cisco original implementation PoE:** Cisco was the first to develop PoE. The original Cisco (prestandard) implementation supports the following features:
 - Provides -48 V DC at up to 6.3 to 7.7 watts (W) per port over data pins 1, 2, 3, and 6.
 - Supports most Cisco devices (IP Phones and wireless access points).
 - Uses a Cisco proprietary method of determining whether an attached device requires power. Power is delivered only to devices that require power.
- n **IEEE 802.3af PoE:** Since first developing PoE, Cisco has been driving the evolution of this technology toward standardization by working with the IEEE and member vendors to create a standards-based means of providing power from an Ethernet switch port. The IEEE 802.3af committee has ratified this capability. The IEEE 802.3af standard supports the following features:
 - Specifies -48 V DC at up to 15.4 W per port over data pins 1, 2, 3, and 6 or the spare pins 4, 5, 7, and 8 (a PSE can use one or the other, but not both).
 - Enables a new range of Ethernet-powered devices that consume additional power.

- Standardizes the method of determining whether an attached device requires power. Power is delivered only to devices that require power. This type has several optional elements, such as power classification, where powered devices can optionally support a signature that defines the maximum power requirement. PSE that supports power classification reads this signature and budgets the correct amount of power per powered device, which will likely be significantly less than the maximum allowed power.

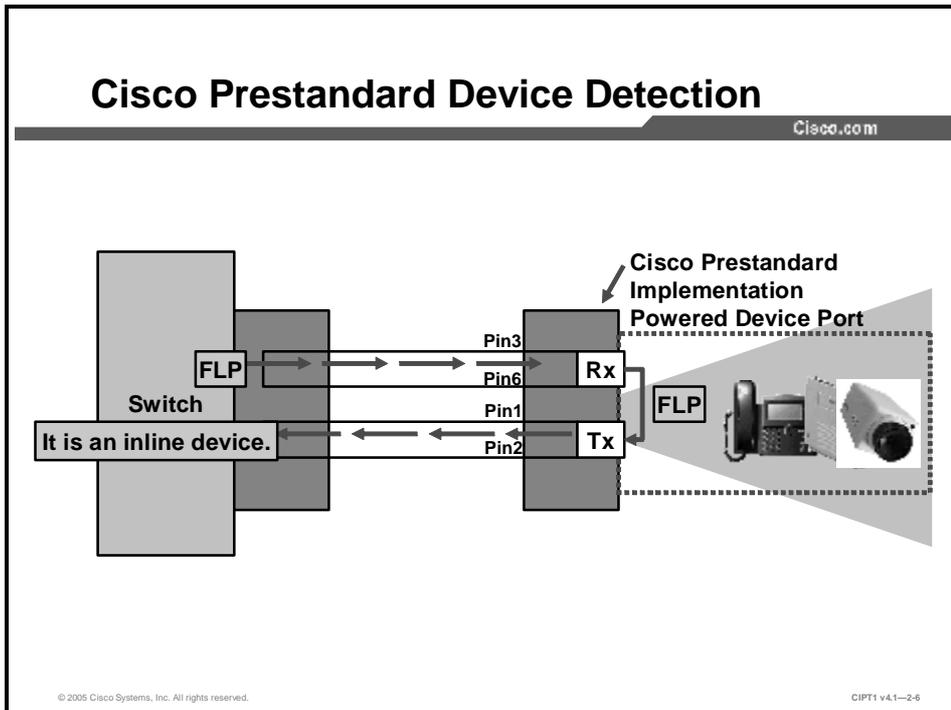
Without power classification, the switch reserves the full 15.4 W of power for every device. This behavior may result in oversubscription of the available power supplies so that some devices will not be powered even though there is sufficient power available.

Power classification defines these five classes:

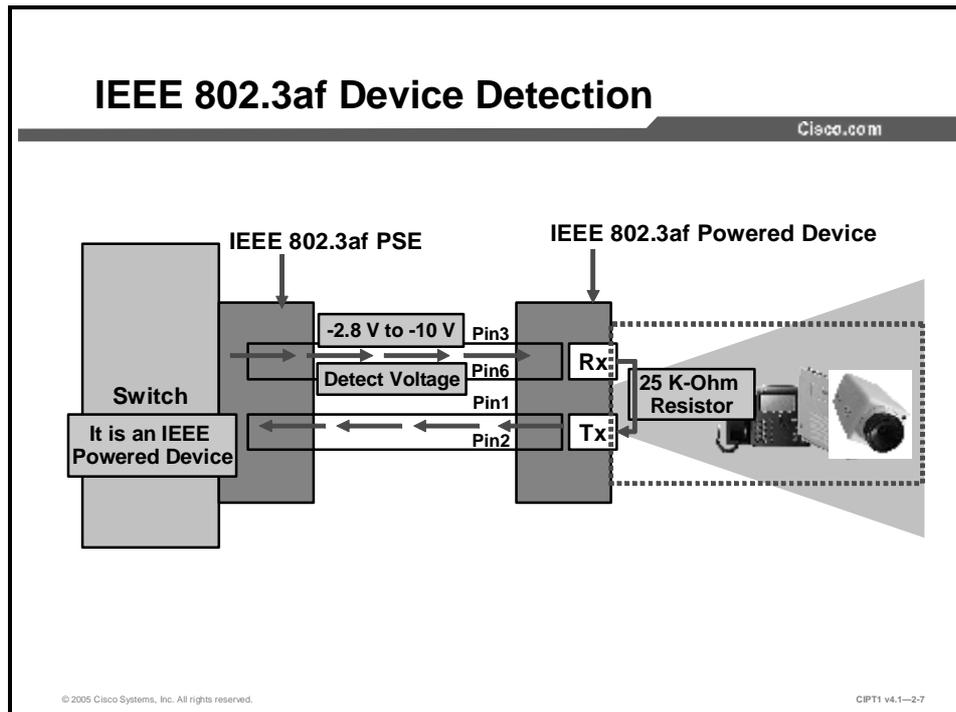
- n **0 (default):** 15.4 W reserved
- n **1:** 4 W
- n **2:** 7 W
- n **3:** 15.4 W
- n **4:** Reserved for future expansion

All Cisco IEEE 802.3af-compliant switches support power classification.

The Cisco Power Calculator is an online tool that enables you to calculate the power supply requirements for a specific PoE configuration. The Cisco Power Calculator is available to registered Cisco.com users at www.cisco.com/go/poe.



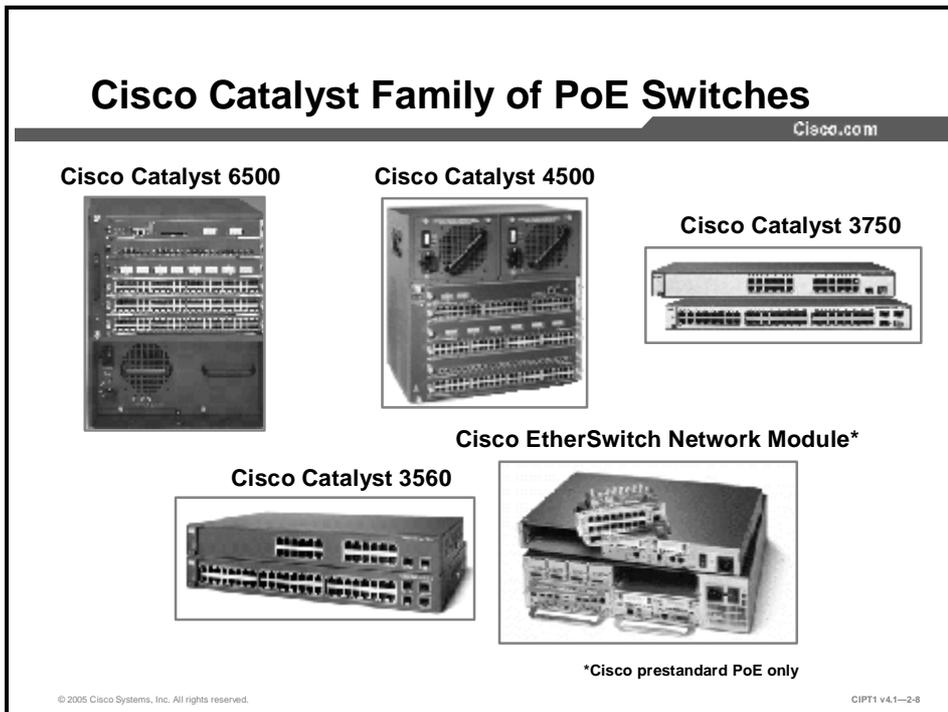
The figure illustrates how a Cisco prestandard Catalyst switch detects a Cisco IP phone, wireless access point, or other inline power-capable device. When a switch port that is configured for inline power detects a connected device, the switch sends an Ethernet Fast Link Pulse (FLP) to the device. The Cisco powered device (IP Phone) loops the FLP back to the switch to indicate its inline power capability. The switch then delivers -48 V DC PoE (inline) power to the IP Phone or other inline power-capable endpoint.



The figure illustrates how a Cisco Catalyst IEEE 802.3af-compliant switch detects a Cisco IP phone, wireless access point, or other inline power-capable device. The PSE (Cisco Catalyst switch) detects a powered device by applying a voltage in the range of -2.8 V to -10 V on the cable and then looks for a $25\text{ K}\Omega$ signature resistor. Compliant powered devices must support this resistance method. If the appropriate resistance is found, the Cisco Catalyst switch delivers power.

Catalyst Family of PoE Switches

This topic describes the Cisco Catalyst PoE switch models.



The Cisco Catalyst LAN switching portfolio is the industry-leading family of intelligent switching solutions delivering a robust range of security and quality of service (QoS) capabilities. The Cisco Catalyst switch portfolio allows organizations to enable new business applications and integrate new technologies such as wireless and IP telephony into their network infrastructure. Here are the switches in the Cisco Catalyst family:

- n **Cisco Catalyst modular switching:** The Cisco Catalyst 6500 Series delivers a 96-port 10BASE-T/100BASE-T line card and 48-port 10BASE-T/100BASE-T and 10BASE-T/100BASE-T/1000BASE-T line cards. The Catalyst 6500 Series offers a modular PoE daughter card architecture for the 96-port card and the 48-port 10/100/1000 card. The Cisco Catalyst 4500 Series delivers 48-port 10/100 and 10/100/1000 line cards. All line cards support both IEEE 802.3af and Cisco prestandard inline power. The cards are compatible with any Cisco Catalyst 6500 or 4500 chassis and Supervisor Engine. The Cisco Catalyst modular chassis switches can deliver 15.4 W per port for all 48 ports on a module simultaneously.
- n **Cisco Catalyst stackable switching:** The Cisco Catalyst 3750 Series offers 48- and 24-port Fast Ethernet switches that comply with IEEE 802.3af and Cisco prestandard PoE. The Cisco Catalyst 3560 Series offers 48- and 24-port Fast Ethernet switches that support both the industry standard and Cisco standard PoE.

- n **Cisco EtherSwitch modules:** The Cisco 36- and 16-port 10/100 EtherSwitch modules for Cisco 2600 and 3700 Series routers offer branch office customers the option to integrate switching and routing in one platform. These modules can support Cisco prestandard PoE and provide straightforward configuration, easy deployment, and integrated management in a single platform. The Cisco 2600 Series requires a separate external PoE power supply; the Cisco 3700 Series integrates the power supply.

This table lists the Cisco Catalyst PoE options.

Catalyst Switch PoE Options

	Cisco Catalyst 6500	Cisco Catalyst 4500	Cisco Catalyst 3750	Cisco Catalyst 3560	Cisco EtherSwitch Module
PoE Configuration Options	48-, 96-port 10/100 or 48-port 10/100/1000	48-port 10/100 or 10/100/1000	24-, 48-port 10/100	24-, 48-port 10/100	16-, 36-port 10/100
IEEE 802.3af-Compliant	Yes	Yes	Yes	Yes	No
Cisco Prestandard PoE	Yes	Yes	Yes	Yes	Yes

Note Cisco does not offer an IEEE 802.3af midspan injection product. The 48-port Cisco Catalyst Inline Power Patch Panel supports Cisco prestandard PoE.

Note The switches that are listed here also support multiple VLANs per port and CoS.

Configuring PoE

This topic discusses the configuration of PoE on Cisco Catalyst switches.

Cisco Catalyst Switch: Configuring PoE

Cisco.com

Cisco CatOS:

```
CatOS>(enable) set port inlinepower <mod/port> ?
      auto                Port inline power auto mode
      off                 Port inline power off mode
```

Native Cisco IOS software:

```
CSCOIOS(config-if)# power inline <auto/never>
```

© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1—2-9

Use the **set port inlinepower** command on a switch that is running Cisco Catalyst Operating System software (CatOS). The two modes are **auto** and **off**. In the off mode, the switch does not power up the port even if an unpowered phone is connected. In the auto mode, the switch powers up the port only if the switching module has discovered the phone. Examples of devices running Cisco CatOS include the Cisco Catalyst 6500, 4500, and 4000 Series.

Use the **power inline** command on switches that are running native Cisco IOS software (examples include the Catalyst 6500, 4500, 3750, and 3560 switches). The powered device-discovery algorithm is operational in the auto mode. The powered device-discovery algorithm is disabled in the never mode. Other modes exist for allocating power, depending on the version of Cisco IOS. For example, the ability to allocate power on a per-port basis with the **allocation milliwatt** mode.

Note The Catalyst 6500 Series can run either Cisco Catalyst operating system software or native Cisco IOS software if the switch Supervisor Engine has a Multilayer Switch Feature Card (MSFC). Otherwise, these switches can run only Cisco Catalyst software. The Cisco Catalyst 4500 and 4000 Series can also run Cisco Catalyst software or native Cisco IOS software, depending on the Supervisor Engine. Generally, late-edition Supervisor Engines run native Cisco IOS software; however, you should check the product documentation to determine the Supervisor Engine and the operating system that is supported on your specific model.

Cisco Catalyst Switch: Show Inline Power Status

Cisco.com

```
show port inline power 7
Default Inline Power allocation per port: 10.000 Watts (0.23 Amps @42V)
Total inline power drawn by module 7: 75.60 Watts (1.80 Amps @42V)
Port      InlinePowered  PowerAllocated
      Admin   Oper   Detected      mWatt      mA @42V
-----  -
7/1      auto    off    no             0           0
7/2      auto    on     yes            6300        150
7/3      auto    on     yes            6300        150
7/4      auto    off    no             0           0
7/5      auto    off    no             0           0
7/6      auto    off    no             0           0
7/7      auto    off    no             0           0
```

```
show power inline
Interface      Admin   Oper   Power ( mWatt )  Device
-----  -
FastEthernet9/1  auto    on     6300             Cisco 6500 IP Phone
FastEthernet9/2  auto    on     6300             Cisco 6500 IP Phone
FastEthernet9/3  auto    off    0                n/a
```

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--2-10

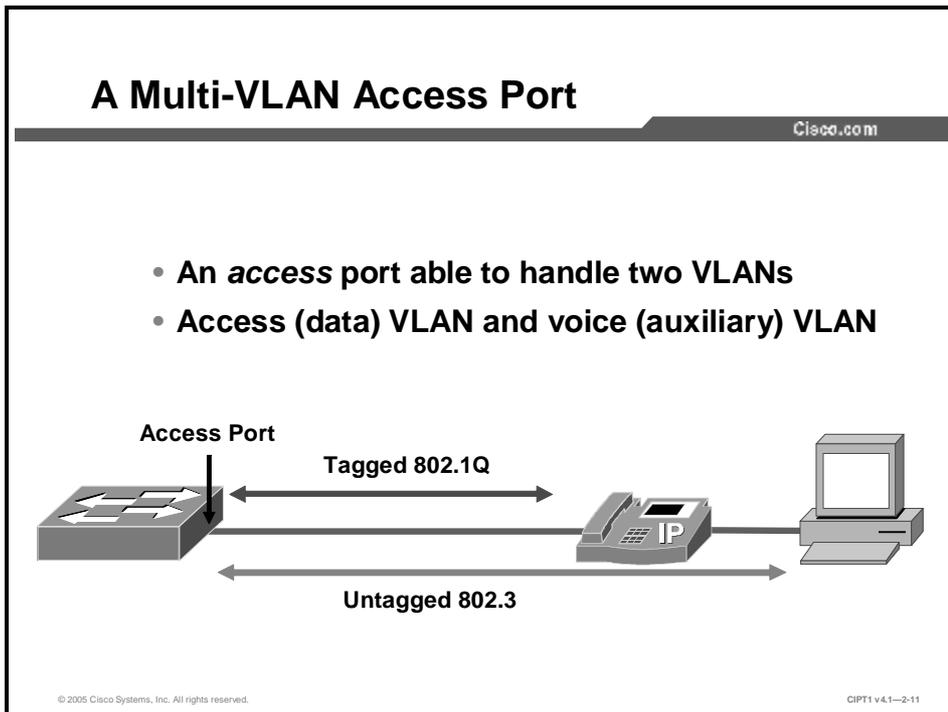
Use the command shown in the figure to display a view of the power allocated on Cisco Catalyst switches. The switch shows the default allocated power as 10 W in addition to the inline power status of every port. The “Inline Power Syntax Descriptions” table provides a brief description of the syntax output.

Inline Power Syntax Descriptions

Column Heading	Description
Port	Identifies the port number on the module
Inline Powered	
Admin	Identifies the port configuration from using the set inlinepower mod/port [auto off] command
Oper	Identifies whether the inline power is operational
Power Allocated	
Detected	Identifies whether power is detected
mWatt	Identifies the milliwatts supplied on a given port
mA @42V	Identifies the milliamps at 42 V supplied on a given port (the actual voltage is -48 V)

Configuring Dual VLANs

This topic describes the configuration of a multi-VLAN access port.



All data devices typically reside on data VLANs in the traditional switched scenario. You may need a separate voice VLAN when you combine the voice network into the data network. (The Cisco Catalyst software command-line interface (CLI) refers to this new voice VLAN as the auxiliary VLAN for configuration purposes.) You can use the new voice VLAN to represent Cisco IP Phones. Although you can think of it as a voice VLAN, in the future, other types of nondata devices will reside in the voice VLAN.

The placement of nondata devices (such as IP Phones) in a voice VLAN makes it easier for customers to automate the process of deploying IP Phones. IP Phones will boot and reside in the voice VLAN if you configure the switch to support them, just as data devices boot and reside in the access (data) VLAN. The IP Phone communicates with the switch via Cisco Discovery Protocol when it powers up. The switch provides the telephone with the appropriate VLAN ID.

Administrators can implement multiple VLANs on the same port by configuring an access port. A tagging mechanism must exist to distinguish among VLANs on the same port. 802.1Q is the IEEE standard for tagging frames with a VLAN ID number. The IP Phone sends tagged 802.1q frames. The PC sends untagged frames and the switch adds the access VLAN tag before forwarding toward the network. When the switch receives a frame from the network destined for the PC, it will remove the access VLAN tag before forwarding the frame to the PC.

There are some advantages in implementing dual VLANs:

- n This solution allows for the scalability of the network from an addressing perspective. IP subnets usually have more than 50 percent (often more than 80 percent) of their IP addresses allocated. A separate VLAN (separate IP subnet) to carry the voice traffic allows you to introduce a large number of new devices, such as IP Phones, into the network without extensive modifications to the IP addressing scheme.
- n This solution allows for the logical separation of data and voice traffic, which have different characteristics. This separation allows the network to handle these two traffic types individually.
- n This solution allows you to connect two devices to the switch using only one physical port and one Ethernet cable between the wiring closet and the IP Phone or PC location.

Configuring Voice VLANs Using Cisco CatOS

Cisco.com

Syntax:

```
set port auxiliaryvlan mod[1 port]{vlan/untagged/  
dot1p/none}  
vlan = 1 to 1000
```

Example:

```
Console>(enable) set port auxiliaryvlan 2/1-3 222  
Auxiliaryvlan 222 configuration successful.  
AuxiliaryVlan AuxVlanStatus Mod/Ports  
-----  
222          active          1/2,2/1-3
```

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1--2-12

Configure auxiliary VLAN ports in Cisco Catalyst software 5.5 and above using the **set port auxiliaryvlan** command to configure the auxiliary VLAN ports:

```
set port auxiliaryvlan mod[port] {vlan | untagged | dot1p | none}
```

Syntax Description

Command	Description
<i>mod[/port]</i>	Number of the module and (optional) ports.
<i>vlan</i>	Number of the VLAN; valid values are from 1 to 1000.
untagged	Keyword to specify that the IP Phone 7960 send untagged packets without 802.1p priority.
dot1p	Keyword to specify that the IP Phone 7960 send packets with 802.1p priority.

The voice VLAN ID in this example is set to the value of 222 for ports 2/1 through 2/3. The switch instructs the IP Phone to reside in VLAN 222 when it powers up. You can use this command to set the voice VLAN ID on a per-port basis, for a range of ports, or for an entire module.

Configuring Voice VLANs Using Native Cisco IOS

Cisco.com

Example:

```
Console(config)#interface FastEthernet0/1
Console(config-if)#switchport mode access
Console(config-if)#switchport voice vlan 261
Console(config-if)#switchport access vlan 262
Console(config-if)#spanning-tree portfast
```

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1--2-13

Use the commands shown in the figure to configure voice and data VLANs on the single-port interface of a switch that is running native Cisco IOS software. These commands apply the same functionality as setting a port to use an auxiliary VLAN on a Cisco Catalyst switch that is running Cisco Catalyst software.

Catalyst Switch Voice Interface Commands

Command	Description
switchport mode access	Configures the switchport to be an access (non-trunking) port
switchport voice vlan <i>voice-VLAN_ID</i>	Configures the switchport with the voice VLAN (261 in this example) to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5...
switchport access vlan <i>data_VLAN_ID</i>	Configure the interface as a static access port with the access VLAN ID (262 in this example); the range is 1 to 4094.
spanning-tree portfast	Causes a port to enter the spanning-tree forwarding state immediately, bypassing the listening and learning states. You can use PortFast on switch ports that are connected to a single workstation or server (as opposed to another switch or network device) to allow those devices to connect to the network immediately.

Verifying Voice VLAN Configuration Using Cisco CatOS

Cisco.com

```

Console> (enable)show port auxiliaryvlan 222
AuxiliaryVlan AuxVlanStatus Mod/Ports
-----
222             active          1/2,2/1-3
Console> (enable)

```

```

Console> (enable)show port 2/1
...
Port  AuxiliaryVlan AuxVlan-Status
----
2/1  222             active
...

```

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--2-14

You can check the status of the auxiliary VLAN on a port or module in one of two ways:

- n Use the **show port auxiliaryvlan *vlan-id*** command to show the status of that auxiliary VLAN and the module and ports where it is active.
- n Use the **show port [*module*[/*port*]]** command to show the module, port, and the auxiliary VLAN and the status of the port.

Verifying Voice VLAN Configuration Using Native Cisco IOS

Cisco.com

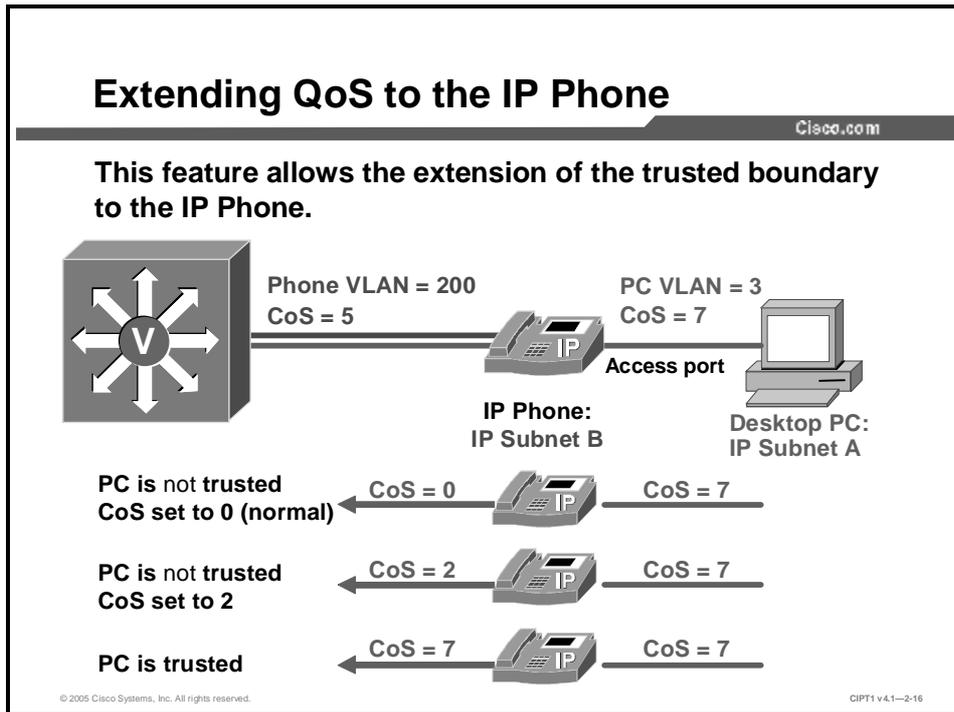
```
Class-1-Switch#sh interfaces fa0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 262 (VLAN0262)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 261 (VLAN0261)
```

```
.
.
.
```

You can verify your voice VLAN configuration on the Cisco Catalyst switches that are running native Cisco IOS software by using the **show interface *mod/port* switchport** command.

Configuring Class of Service

This topic describes the configuration of CoS when a PC and a Cisco IP Phone share the same switch port.



CoS is a data link layer marking that you can use to classify traffic as it passes through a switch. You should ensure that voice traffic has priority as it travels throughout your network because it is extremely sensitive to delay. Cisco IP Phones send all voice packets tagged with CoS 5 by default, which is the highest level of CoS that is recommended for user traffic.

The multi-VLAN port also receives packets from the devices (PCs and workstations) that are connected to the access port of the IP Phone. The attached device, if it is not in the native VLAN, can send packets with a CoS equal to or higher than the packets that are being sent by the IP Phone, which can cause severe voice quality problems on your IP telephony network. This can be done only if the device is *not* in the native VLAN.

Cisco Catalyst switches have the ability to extend the boundary of trust to the IP Phone. You can use the switch to instruct the IP Phone to accept the CoS value of frames that are arriving from connected devices (trust) and allow the CoS to remain unchanged. Alternatively, you can choose not to trust the attached device and set the CoS to 0 or set the CoS to a configured value that you determine.

The Cisco Catalyst switch uses Cisco Discovery Protocol to send this configuration information to the IP Phone. The switch sends an additional Cisco Discovery Protocol packet to the IP Phone whenever there is a change in the CoS configuration.

The switch uses its queues, which are available on a per-port basis, to buffer incoming and outgoing frames. The switch can use the CoS values to place the frames in the appropriate queues. Voice frames should be placed in the priority queue for minimal delay.

Configuring CoS

Cisco.com

Cisco CatOS

```
set port qos mod/port cos cos-value
```

- Set the default value for all packets that have arrived through an untrusted port

```
set port qos mod/ports... trust-ext {trusted | untrusted}
```

- Allows you to trust or not trust (set to 0) the CoS assigned to the device attached to the IP Phone

Native Cisco IOS

```
Switch(config)#interface FastEthernet0/1  
Switch(config-if)#switchport priority extend  
                          {cos value | trust}
```

- Choose to modify, ignore, or trust the CoS of the attached device

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--2-1

You can configure the switch with different QoS settings on a per-port basis. Use the **set port qos cos** command to set the default value for all packets that have arrived through an untrusted port. The *cos-value* specifies the CoS value for a port; valid values are from 0 to 7. Seven is the highest priority. The default is 0 (not trusted).

For example, the command **set port qos 3/1 cos 3** sets the cos value to 3 on port 3/1.

Use the **set port qos mod/ports... trust-ext {trusted | untrusted}** command to either extend trust to the PC by specifying that all traffic received through the access port passes through the phone switch unchanged, or to not trust the port and change the CoS value to 0.

Use the **switchport priority extend** interface configuration command to set a port priority for the incoming frames received by the IP phone connected to the specified port. The *cos-value* is used to set the IP phone port to override the priority received from PC or the attached device. Valid values for the *cos-value* from 0 to 7. Seven is the highest priority. The default is 0 (not trusted). Alternatively, the **trust** keyword causes the IP phone port to trust the priority received from PC or the attached device, that is, to not change the CoS value.

The *Implementing Cisco Quality of Service (QoS)* course provides more information about voice QoS theory and configuration.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Cisco voice-capable switches support three primary feature sets that can assist with an IP telephony deployment: POE, dual VLANs, and CoS.**
- **Most Cisco IP Phone models are capable of using three options for power: inline power, external power, and wall power.**
- **Two types of inline power delivery are the Cisco prestandard implementation and IEEE 802.3af PoE. These differ in the amount of power supplied, how powered devices are discovered, and optional enhancements.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-18

Summary (Cont.)

Cisco.com

- **The Cisco Catalyst 6500, 4500, 3750, and 3560 switches support 802.3af and Cisco PoE, dual VLANs, and CoS.**
- **Configure inline power using the set port inline power command (Catalyst operating system) or power inline (native Cisco IOS software) command.**
- **Using dual VLANs on a single-port Cisco Catalyst switch improves network scalability when you combine a voice network into a data network.**
- **When a PC and an IP Phone share the same switch port, you can use the CoS on Cisco Catalyst switch models to classify circuits so that voice packets have priority over data packets.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-19

References

For additional information, refer to these resources:

- n Cisco Systems, Inc. Multilayer LAN switches documentation.
<http://www.cisco.com/univercd/cc/td/doc/product/lan/index.htm>.
- n Cisco Systems, Inc. *Understanding IP Phone In-Line Power Provisioning on the Catalyst 6500/6000 Switch*.
http://www.cisco.com/warp/public/788/AVVID/cat6k_inline_pwr.html#second.

Configuring Cisco IP Communicator

Overview

Businesses often want to provide users who travel or telecommute with a supplemental telephone that provides them with the same familiar phone services on the road or in the home office that users enjoy from the main office. Cisco IP Communicator is a software-based application that delivers enhanced telephony support through personal computers with the same features, functionality, and interface as a desktop Cisco IP Phone. This application allows computers to function as Cisco IP Phones, providing high-quality voice calls on the road, in the office, or from wherever users may have access to the corporate network.

This lesson discusses Cisco IP Communicator features and functions, installation, configuration, and deployment.

Objectives

Upon completing this lesson, you will be able to install Cisco IP Communicator and make IP Phone calls from the PC. This ability includes being able to meet these objectives:

- n Describe the features and function of Cisco IP Communicator
- n Identify the steps to install and configure Cisco IP Communicator
- n Configure Cisco CallManager to enable Cisco IP Communicator
- n Deploy Cisco IP Communicator using a supported deployment option and the Cisco IP Communicator Administration Tool
- n Perform required and recommended postinstallation configuration tasks to enable Cisco IP Communicator to function properly or to allow users to access some features

Cisco IP Communicator Overview

This topic describes the features and function of Cisco IP Communicator.

Cisco IP Communicator Overview

Cisco.com

- **Gives your PC the functionality of an IP phone**
- **Allows you to access your phone extension and services outside the office (on and off campus)**
- **Provides parity with the advanced Cisco IP Phones**
- **Windows-based IP Phone implementation compatible with Cisco CallManager Version 3.3(3) SR3 and later**
- **Multiple language support using Cisco IP Telephony Locale Installer**



© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1—2-3

Cisco IP Communicator is a software-based application that endows computers with the functionality of IP Phones, providing high-quality voice calls on the road, in the office, or from wherever users may have access to the corporate network.

When registered to Cisco CallManager system, Cisco IP Communicator has the features and functionality of a full-featured Cisco IP Phone, including the ability to transfer calls, forward calls, and conference additional participants into an existing call. System administrators can provision Cisco IP Communicator as they would any other Cisco IP Phone, simplifying IP Phone management.

Cisco IP Communicator is a Microsoft Windows-based IP Phone compatible with Cisco CallManager Release 3.3(3) SR3 and later versions using the Skinny Client Control Protocol (SCCP).

Cisco IP Communicator is available in languages besides English. If you are using Cisco IP Communicator in a locale where a language other than English is spoken, install the Cisco IP Telephony Locale Installer on every Cisco CallManager server in the cluster. Doing so ensures that you have the latest translated text, user and network locales, and country-specific phone tones available. For more information, refer to “Cisco IP Telephony Locale Installer” at:

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

Cisco IP Communicator Features

Cisco.com

Ease of use

- Feature parity with advanced Cisco IP Phones
 - Multiple lines
 - IP Phone services support (XML) such as extension mobility

Management

- Unified administration with Cisco IP phones
 - Scaling 1 to 1 with IP Phones (unlike TAPI-based)
 - Automatic software updates

Deployment

- Autodetection of Cisco VPN client

Voice quality

- Advanced jitter buffer and packet loss concealment algorithms
- Audio Tuning Wizard for setting levels
- Echo suppression and noise cancellation

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--2-4

Details of Cisco IP Communicator features are covered in the slide and in the following list:

n Ease of use

- Cisco IP Communicator delivers feature parity with advanced Cisco IP Phones such as the Cisco 7940 and up
- There are multiple lines: eight line keys and five softkeys.
- IP Phone services such as extension mobility are supported. This solution also enables customers and developers to deliver Extensible Markup Language (XML)-based applications to the display.

n Management

- It scales 1:1 with IP phones. Cisco IP Communicator is a “lighter-weight” device than Telephony Application Programming Interface (TAPI)-based applications such as Cisco IP SoftPhone, so it places less load on Cisco CallManager.
- Software updates automatically. AutoUpdate is part of the Cisco IP Communicator software that helps you automatically update Cisco IP Communicator. Every time Cisco IP Communicator registers with a Cisco CallManager, AutoUpdate compares the current Cisco IP Communicator software load with the version in the configuration file. AutoUpdate downloads and installs new software components from the TFTP server when it detects that they are available. In addition, AutoUpdate can use HTTP to download from the server if you have enabled HTTP access to your TFTP server. Run the Cisco IP Communicator Administration Tool to enable HTTP.

n Deployment

- Cisco Virtual Private Network (VPN) clients are automatically detected, and support for most VPN clients (including the Microsoft Point-to-Point Tunneling Protocol [PPTP] client) is automated.

- n Voice quality
 - Kernel mode operation prevents resource intensive applications from affecting audio.
 - Cisco IP Communicator offers advanced jitter buffer and packet loss concealment algorithms.
 - The Audio Tuning Wizard can be used for setting input and output levels.
 - Features include echo suppression and noise cancellation.
 - Cisco IP Communicator also offers voice activity detection, silence suppression, and error concealment.

Cisco IP SoftPhone and IP Communicator Feature Comparison		
Feature	Cisco IP Communicator	Cisco IP SoftPhone 1.3
SCCP	Yes	No
Multiple Lines or Directory Numbers	Yes	No
Enterprise Call Features: Shared Lines, Park, Pickup, MeetMe Conference, Barge	Yes	No
XML Support	Yes	No
Automatic Software Updates	Yes	No
Date and Time Display	Yes	No
Skin (Display) Options	Yes	No
VPN Support for Remote Access	Yes	No
Third Party Application Integration—TAPI (NetMeeting for Collaboration, Outlook, and So On)	No	Yes
Drag and Drop Dialing	No	Yes
Collaboration	No	Yes
Alphanumeric Translation	No	Yes

© 2005 Cisco Systems, Inc. All rights reserved. CIP11 v4.1—2-5

The figure identifies the differences between Cisco IP Communicator and Cisco IP SoftPhone. Additional details on some of the differences are as follows:

- n **Skin (display) options:** Cisco IP Communicator comes with two desktop appearances called *skins* that enable you to change the look of the phone display.
- n **Alphanumeric translation:** Cisco IP SoftPhone can translate alphanumeric dialing strings into keypad digits. For example, if you enter 1-800-GOCISCO, Cisco IP SoftPhone correctly translates the dial string to 1-800-462-4726. The values for Q and Z are translated to 7 and 9, respectively.
- n **Drag and drop dialing:** Cisco IP SoftPhone displays a history of the calls that you have placed, missed or answered in the call log. To place a call to a number in the call log, you can select the entry and click **Dial** or select the entry and drag and drop it to the SoftPhone interface.
- n **VPN support for remote access:** Cisco IP Communicator supports autodetection of Cisco VPN client and automated support for many VPN clients that appear as alternative network interfaces (such as the Microsoft PPTP client).

Cisco IP Communicator Installation and Configuration Overview

This topic identifies the steps to install and configure Cisco IP Communicator.

Configuration Steps for Cisco IP Communicator

Cisco.com

1. **Add the device in Cisco CallManager.**
2. **Run the Cisco IP Communicator Administration Tool.**
3. **Install the phone load on the publisher or TFTP server to enable AutoUpdate.**
4. **Install Cisco IP Communicator software on client PCs.**
5. **Perform postinstallation tasks.**

© 2005 Cisco Systems, Inc. All rights reserved.CIP11 v4.1--2-6

To install and configure Cisco IP Communicator, follow this procedure:

- Step 4** Add the device in Cisco CallManager. The procedure for adding Cisco IP Communicator is similar to the procedure for adding an IP Phone.
- Step 5** Run the Cisco IP Communicator Administration Tool to enable HTTP access and access the Directory Wizard if desired.
- Step 6** Install the phone load. The phone load is a patch to enable Cisco IP Communicator to use AutoUpdate via the TFTP server of the Cisco CallManager (similar to IP Phone firmware updates). AutoUpdate will occur when the application is launched or a device reset is performed. The file name of the phone load will be of the form cmterm-CIPC.CIPC-1-1-2-0.exe or cmterm-CIPC.CIPC-1-1-3-0.exe. The phone load is bundled with the Cisco IP Communicator software package contents.
- Step 7** Install Cisco IP Communicator on the client PC.
- Step 8** Perform postinstallation tasks before first use.

Additional details on Steps 1, 2, 4, and 5 are covered in the next topics.

Configuring Cisco CallManager for Cisco IP Communicator

This topic describes how to configure Cisco CallManager to enable Cisco IP Communicator.

Adding the Device to Cisco CallManager Database

Cisco.com

Method	MAC Address?
Auto-registration	No
Auto-registration with TAPS	No
Using Cisco CallManager Administration	Yes
Using BAT	Yes

Using Cisco CallManager Administration



© 2005 Cisco Systems, Inc. All rights reserved. CIP11 v4.1—2-7

Before installing the Cisco IP Communicator application, you must add devices to the Cisco CallManager database. Just as with Cisco IP Phones, there are four ways to add devices to the Cisco CallManager database:

- n **Auto-registration:** You can use this method without first gathering MAC addresses from client PCs. When auto-registration is enabled, Cisco CallManager provides a directory number as soon as you run the Cisco IP Communicator application after installation.
- n **Auto-registration with Tool for Auto-Registered Phones Support (TAPS):** You can use this method without first gathering MAC addresses from client PCs. TAPS works in conjunction with the Cisco Bulk Administration Tool (BAT) to update devices that were previously added to the Cisco CallManager database using dummy MAC addresses. Use TAPS to update MAC addresses and download predefined configurations for Cisco IP Communicator devices.
- n **Using Cisco CallManager Administration:** To use Cisco CallManager Administration, you need to first collect the appropriate MAC address from the network interface for each client on which you want the Cisco IP Communicator application installed. After you have collected MAC addresses, choose **Device > Add a New Device** in Cisco CallManager Administration.
- n **Using BAT:** The Cisco BAT is a plug-in application for Cisco CallManager that enables system administrators to perform batch operations, including registration, on large numbers of devices, including Cisco IP Phones and Cisco IP Communicator devices. To add devices using BAT only (not in conjunction with TAPS), you first need to collect the appropriate MAC address from the network interface for each client on which you want the Cisco IP Communicator application installed.

Deploying and Updating Cisco IP Communicator

The topic describes using the Cisco IP Communicator Administration Tool to deploy the Cisco IP Communicator and the supported deployment methods.

Cisco IP Communicator Administration Tool

Cisco.com

- **Enables HTTP access**
 - **Faster AutoUpdate downloads than TFTP**
 - **Required if using unsupported VPN clients**
- **Includes Directory Wizard**
 - **Includes Quick Search feature to access a personal or corporate directory on Cisco CallManager from Cisco IP Communicator**

Directory Wizard



© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1-2-8

As part of your deployment preparations, it is strongly recommended that you run the Cisco IP Communicator Administration Tool on the Cisco CallManager publisher and select the option in the tool to enable HTTP access. This is a requirement if you have any users in your network who rely on an unsupported VPN client. Supported software VPN clients include Cisco VPN Client 3.x or 4.x and the Microsoft PPTP client. Other third-party VPN clients might be unsupported. A VPN solution is typically unsupported if it is not a Cisco product and does not function like a network interface card.

Enabling HTTP will improve the performance of AutoUpdate for remote users. (Downloading software updates over a dialup or broadband connection using TFTP can take more than 15 minutes.)

Some VPN clients, such as Cisco VPN Client 3.x, assign the VPN IP address at a very low level, which makes it difficult for Cisco IP Communicator to specify the correct address. To eliminate this problem, Cisco IP Communicator queries the Cisco VPN Client directly.

Other VPN clients, such as the Microsoft PPTP client and Cisco VPN Client 4.x, simply appear as alternative network interfaces. In these cases, the IP address can be selected with the same autodetection process that is used to resolve selection when there are multiple interfaces.

Other third-party VPN clients might be unsupported and result in one-way audio. To fix the problem, run the Cisco IP Communicator Administration Tool to create a getIP.asp audio IP address reflector web page, then specify the URL for the web page in Cisco CallManager Administration. Cisco IP Communicator will attempt to fetch this reflector page rather than using other methods of autodetection. The reflector page returns the IP address from which it sees the request originate, which is a relatively reliable way to identify the Cisco IP Communicator VPN IP address.

Quick Search enables users to access a personal or corporate directory on the Cisco CallManager server. To configure Quick Search, use the Directory Wizard. (To install the Directory Wizard, run the Cisco IP Communicator Administration Tool.) The Directory Wizard creates an XML configuration file (LdapDirectories.xml) that tells Cisco IP Communicator which Lightweight Directory Access Protocol (LDAP) directories to search. Cisco IP Communicator downloads this file at startup and saves the list of specified LDAP directories. When a user invokes the Quick Search feature, Cisco IP Communicator searches the specified LDAP directories, stopping at the first directory where one or more matches are found. (Therefore, if you have two directories specified, and your search string is matched in the first directory, the second directory will not be searched, regardless of whether or not it contains matching entries.)

You can apply Quick Search configuration to all devices in a Cisco CallManager cluster by using the Cisco IP Communicator Directory Wizard, or you can manually create a custom Quick Search XML file to apply to a specific device.

Tip Make sure that the Telephone Number field in the User Configuration window of Cisco CallManager Administration shows the user's phone number. The Quick Search feature displays this phone number in search results.

Deployment Options

Cisco.com

- **Deploy to a shared location**
 - **Deploy executable or MSI package to a shared location or use command-line option with MSI package to create a server image**
- **Use a software deployment tool**
 - **Required if users do not have administrative privileges on their computers**
- **Run the installer on a client PC**

You can deploy Cisco IP Communicator using either of the following installer packages:

- n **CiscoIPCommunicatorSetup.exe:** This executable contains the required Microsoft Windows Installer engines and default verbose logging for typical deployments.
- n **CiscoIPCommunicatorSetup.msi:** This Microsoft Windows Installer package (MSI package) allows you to provide deployment customization using command-line options. Logging is not automatically set when you use the MSI package.

Whether you use the executable or the MSI package, you have three options for performing installation:

- n **Deploy to a shared location:** You can place the installer on a shared location where you or a user can run it. (To use this method, users must have administrative privileges on their PCs.)

You can deploy the executable or MSI package to a shared location, such as a web server, where users can access it to perform installation. Alternately, you can use the following command-line option with the MSI package to create a server image of Cisco IP Communicator at a specified network location:

msiexec.exe /a CiscoIPCommunicatorSetup.msi.

- n **Use a software deployment tool:** You can perform installation for an entire enterprise by using a software distribution technology. (This method will temporarily elevate user privileges for installation purposes, if necessary.)

You can use a software deployment tool to distribute Cisco IP Communicator to client PCs. In fact, you must use this deployment method if users do not have administrative privileges on their computers (and if you want to avoid installing the application manually on each client PC). A software deployment tool can temporarily elevate user privileges on the client PC for installation purposes.

Using a software distribution tool that can pass a command line to a system allows you to take advantage of the Windows Installer package and customize values such as the device name and TFTP server address or addresses at the time of deployment. Using command-line options to specify these values at deployment means that users do not have to configure these settings after installation. This greatly simplifies the postinstallation process for users.

- n **Use the installer on the client PC:** You can perform installation operations directly on an individual computer.

You can deploy either the executable or the MSI package directly to the client PC and perform installation by running the installer and following the installation wizard. If necessary, use an administrator account to do this task.

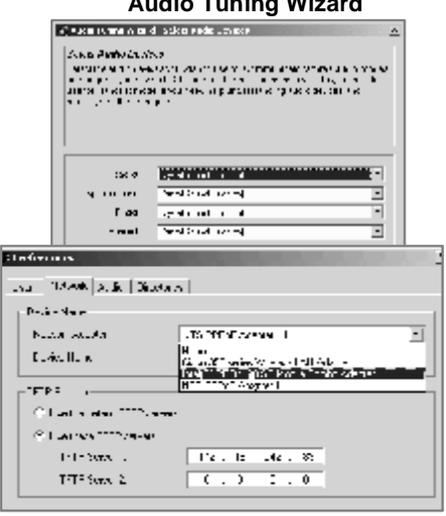
Postinstallation Configuration Tasks

This topic describes required and recommended postinstallation configuration tasks to enable Cisco IP Communicator to function properly or to enable users to access some features.

Postinstallation Configuration Tasks

Cisco.com

1. **Select and tune audio devices.**
2. **Specify a TFTP server address.**
3. **Select a device name.**
4. **Run Cisco IP Communicator Administration Tool and enable HTTP access (if not previously completed).**
5. **Provide users with usernames and passwords.**



The image shows two screenshots from the Cisco IP Communicator installation process. The top screenshot is the 'Audio Tuning Wizard' window, which has a title bar that says 'Cisco.com' and 'Audio Tuning Wizard'. It contains a scrollable text area with instructions and several dropdown menus for selecting audio devices. The bottom screenshot is the 'Cisco IP Communicator Administration Tool' window. It has a title bar with 'Cisco.com' and 'Cisco IP Communicator Administration Tool'. It features a 'Device Name' field, a 'TFTP Server' field, and a 'TFTP Server 2' field. There are also radio buttons for 'Enable HTTP Access' and 'Disable HTTP Access'.

© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1-2-10

After the software has been installed on the client PC, you or the user might need to perform a few configuration tasks before Cisco IP Communicator can function properly or before users can access some features. The need to perform these tasks depends upon variables such as settings on the client PC and the software VPN solution of the user, among other factors. These tasks are as follows:

- Step 9** Select and tune audio devices (input microphone levels and output headset levels). Use the Audio Wizard to select and tune audio devices on Cisco IP Communicator startup.
- Step 10** Specify a TFTP server address. This step is required if you are not using Dynamic Host Configuration Protocol (DHCP) with Option 150 enabled.
- Step 11** Choose a device name; this name is required at launch if the client has multiple PC interfaces.
- Step 12** Run the Cisco IP Communicator Administration Tool and enable HTTP access if you have not done so already.
- Step 13** Provide users with usernames and passwords, which are required if users are going to access the Quick Search or User Options web pages.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Cisco IP Communicator is a PC- and Windows-based application with all the functionality of a full-featured Cisco IP Phone.
- Installation and configuration entails adding Cisco IP Communicator in Cisco CallManager, running the Cisco IP Communicator Administration Tool, installing the phone load, installing the software on client PCs, and performing postinstallation tasks.
- Configuring Cisco CallManager for Cisco IP Communicator entails adding the device (PC) in Cisco CallManager either manually, using auto-registration, or by using BAT.
- Deploying Cisco IP Communicator entails running the Cisco IP Communicator Administration Tool and deploying either to a shared location, using a software deployment tool, or using the Installer directly on the client PC.
- Postinstallation configuration tasks include tuning audio devices, specifying the TFTP server address, and providing usernames and passwords to users.

References

For additional information, refer to these resources:

- n Cisco Systems, Inc. Cisco IP Communicator technical documentation, including links to data sheets, the *Cisco IP Communicator User Guide*, and the *Cisco IP Communicator Administration Guide*.
http://www.cisco.com/en/US/products/sw/voicesw/ps5475/tsd_products_support_series_home.html
- n Cisco Systems, Inc. “Install and Configure IP Communicator with CallManager 4.x” TechNote.
http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_tech_notes_list.html

Using the Bulk Administration Tool

Overview

Adding, updating, and deleting phones, users, and gateway ports are important functions in the day-to-day activities of a Cisco CallManager administrator. When you use Cisco CallManager Administration, each database transaction requires an individual manual operation. Manually adding and configuring large numbers of these entities can be time-consuming and tedious. The Cisco Bulk Administration Tool (BAT) automates the process and achieves faster add, update, and delete operations so that the system administrator can focus on more business- and network-critical activities.

The lesson covers BAT Release 5.1(4) and Tool for Auto-Registered Phones Support (TAPS). BAT is a web-based application for Cisco CallManager that allows you to add, update, or delete a large number of similar telephones, users, or ports at the same time. TAPS works in conjunction with BAT to update MAC addresses and download a predefined configuration for new phones.

Objectives

Upon completing this lesson, you will be able to use BAT and TAPS to bulk-add and auto-register Cisco IP Phones, users, and ports in an IP telephony network. This ability includes being able to meet these objectives:

- n Identify the major features and components of the BAT application
- n Install the BAT application on a Cisco CallManager publisher server
- n Use the BAT Wizard to perform bulk configuration tasks
- n Create an IP Phone template to use with BAT
- n Identify the two ways to create CSV files for importing data into BAT
- n Use the BAT Wizard to validate the IP Phone template and CSV file for errors prior to inserting the devices into the Cisco CallManager database
- n Use the BAT wizard to insert the IP Phones into the Cisco CallManager database
- n Describe how to use BAT to update IP Phone settings for a group of similar phones
- n Describe the major requirements for proper installation of TAPS

Introducing the Bulk Administration Tool

This topic examines the features and components of BAT, a product that enables the Cisco CallManager administrator to complete bulk additions, updates, and deletions for Cisco IP Phones, users, ports, and other records.

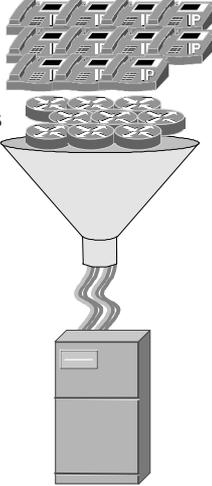
Introduction to BAT

Cisco.com

Supports bulk transactions for:

- Cisco IP Phones, CTI ports, and H.323 clients
- Users and user device profiles
- Cisco IP Manager Assistant (IPMA) managers and assistants
- Cisco Catalyst 6000 FXS Analog Interface Module
- Cisco VG200 analog gateways and ports
- Forced authorization codes and client matter codes
- Call Pickup groups
- Locally significant certificates

Includes TAPS



© 2005 Cisco Systems, Inc. All rights reserved. CIP11 v4.1—2-3

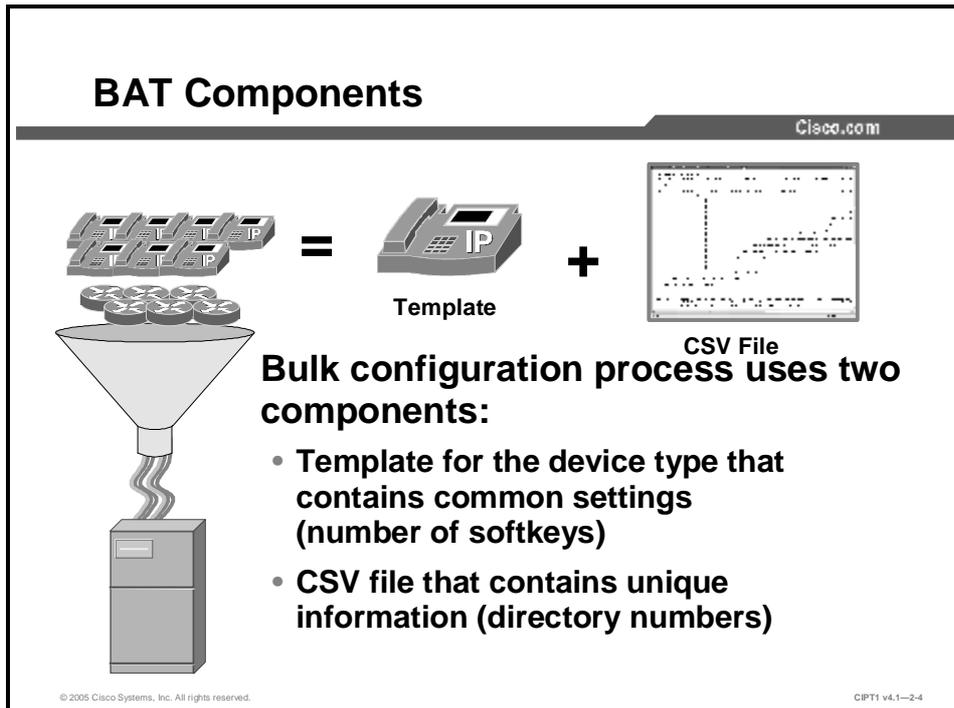
You can use BAT (Release 5.1(4) or later), to work with the following types of devices and records:

- n Add, update, and delete Cisco IP Phones, including voice gateway chalice (VGC) phones, computer telephony interface (CTI) ports, and H.323 clients
- n Add, update, and delete users
- n Add, update, and delete user device profiles
- n Add, update, and delete Cisco IP Manager Assistant (IPMA) managers and assistants
- n Add, update, and delete ports on a Cisco Catalyst 6000 FXS Analog Interface Module
- n Add or delete Cisco VG200 analog gateways and ports
- n Add or delete forced authorization codes
- n Add or delete client matter codes
- n Add or delete Call Pickup groups
- n Update or delete locally significant certificates on Cisco IP Phones

BAT provides an optional application, TAPS, which retrieves the predefined configuration for auto-registered telephones.

Only Cisco CallManager system administrators require access to BAT, but end users can use TAPS with permission from a system administrator to register new IP Phones.

Cisco Systems has based the BAT utility on the Cisco CallManager Administration interface. You can access BAT from Cisco CallManager Administration or the Application menu.



Every device includes a multitude of individual attributes, settings, and information fields that enable the device to function in the network and provide its telephony features. Many devices have the same attributes and settings in common, while other values, such as the directory number (DN), are unique to a user or to a device.

For bulk configuration transactions involving the Cisco CallManager database, the BAT process uses two components: a template for the device type that includes settings that devices have in common and a data file in comma-separated values (CSV) format that contains the unique values for configuring a new device or updating an existing record in the database. The CSV data file works in conjunction with the device template.

For instance, when you create a bulk transaction for a group of Cisco IP Phones, you set up the CSV data file that contains the unique information for each phone, such as the DN and MAC address. In addition, you set up or choose the BAT template that contains the common settings for all phones in the transaction, such as a Cisco IP Phone 7960 template.

Caution Because bulk transactions can affect Cisco CallManager performance and call processing, use BAT only during off-peak hours.

BAT Features

Cisco.com

- **Bulk Administration Tool Wizard**
- **Flexible data input file format**
- **Master phone templates**
- **Validation feature**
- **Reporting utility**
- **Custom file support**
- **Export utility**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1--2-5

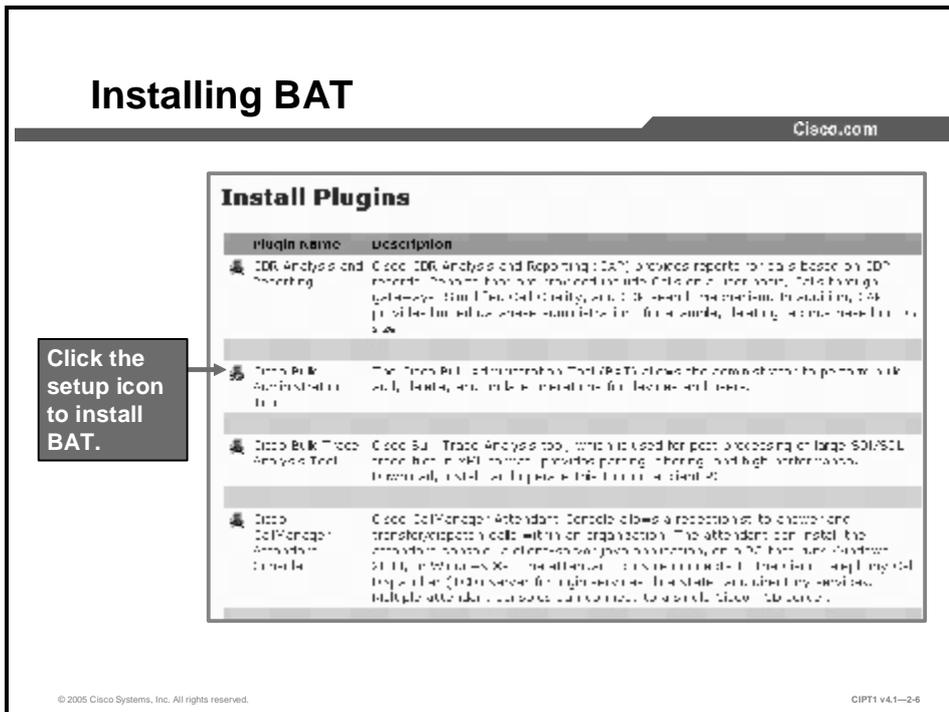
BAT Release 5.0(1) includes a number of useful feature enhancements:

- n **Bulk Administration Tool Wizard:** The Bulk Administration Tool Wizard guides administrators through bulk configuration tasks with step-by-step procedures that link to the web pages for each task. Administrators can easily update phones and lines by using the BAT web interface.
- n **Flexible CSV data input file:** Administrators can use a flexible CSV data input file format for phones and user device profiles. Administrators can choose the phone or user device profile fields to use in the CSV file and arrange the order of the fields. The first record of the CSV file shows the customized file format. Values in the CSV file take precedence over template values.
- n **Master phone templates:** When you are adding a group of phones that have multiple lines, you can create a master phone template that provides multiple lines and the most common values for a specific phone model. You can use the master template to add phones that have differing number of lines but do not exceed the number of lines in the master phone template. For example, you can create a master phone template for a Cisco IP Phone 7960 that has eight lines. You can use this template to add phones that have one line, two lines, or up to eight lines.
- n **Validation feature:** A validation routine checks that the CSV data file and BAT phone template have populated all required fields, such as device pool and locations, or that the number of lines that are configured on the device does not exceed the number specified on the device template.
- n **Report utility:** A BAT report utility generates reports in CSV format with information about phones, users, user device profiles, managers and assistants, and gateway records. Reports do not get generated for the Cisco Catalyst 6000 Foreign Exchange Station (FXS) ports. Administrators can customize reports for phones and user device profiles by selecting and arranging the fields in the report. You can import report data into Microsoft Excel to format and print the report.
- n **Custom file support:** Administrators can use a custom file to update and delete users when using queries is not feasible.

- n **Export utility:** System administrators need the ability to move large numbers of phone records to another Cisco CallManager database for department moves, reorganizations, or equipment upgrades. The export utility in BAT gives you the ability to export large numbers of phone, user, and user device profile records from a Cisco CallManager database to a data file in CSV format. Then you can import the records into a different Cisco CallManager database.

Installing BAT

This topic examines the BAT installation steps.



BAT must be installed on the same server as the publisher database for Cisco CallManager. During BAT installation, the setup program stops the following services:

- n Microsoft Internet Information Server (IIS) Administration
- n World Wide Web publishing
- n FTP publishing

These services automatically restart when the installation is complete.

When BAT is installed, the Microsoft Excel file BAT.xlt file for the BAT spreadsheet is placed on the publisher database server at the following path: C:\CiscoWebs\BAT\ExcelTemplate\.

BAT Release 5.1(4) supports Cisco CallManager Release 4.1(3). BAT Release 5.1(3) supports Cisco CallManager Release 4.1(2).

These steps describe the BAT installation process:

Step 14 Using administrator privileges, log in to the system running the publisher database for Cisco CallManager.

Note You must install BAT directly on the publisher server; do not use Windows Terminal Services.

Step 15 Choose **Application > Install Plugins**. The Install Plugins window is displayed, as shown here.

Step 16 Double-click the setup icon for the Cisco Bulk Administration Tool.

- Step 17** A standard Windows dialog box appears. Determine whether to copy the BAT installation executable to the system or run it from the current location.
- If an existing version of BAT is detected on the server, you are prompted to confirm the reinstallation or upgrade. To reinstall BAT or to upgrade from a previous version, click **OK**.
- Step 18** The Welcome screen appears. Click **Next**, and the Current Settings window appears.
- Step 19** Click **Next** to install to the default location C:\CiscoWebs\BAT\. BAT installs to C:\CiscoWebs\BAT\. You cannot change this path. The Start Copying Files window appears. The setup program begins copying files.
- Step 20** The Setup Complete window appears. You have successfully installed BAT.
- Step 21** To close setup, click **Finish**.
- Step 22** After you have installed BAT, from Cisco CallManager Administration, choose **Application > BAT** to access BAT. If after you have installed BAT, BAT is not visible under the Application menu, refresh your browser.

Using the BAT Wizard

This topic describes using the BAT Wizard to complete the bulk configuration process.

BAT Configuration Process

Cisco.com

1. **Set up the template for data input.**
2. **Create the CSV data file.**
3. **Validate the data input files with the Cisco CallManager database.**
4. **Insert the devices into the Cisco CallManager database.**

© 2005 Cisco Systems, Inc. All rights reserved. CIPT1 v4.1—2-7

BAT uses a multistep process to prepare the bulk configuration transaction. BAT Release 5.0(1) introduced a wizard to step you through bulk configurations. The BAT configuration process includes these tasks:

- Step 23** Set up the template for data input. You can create BAT templates for the following types of device options:
- n **Phones:** All Cisco IP Phone models and Cisco ATA 186, Cisco VGC phones, CTI ports, and H.323 clients
 - n **Gateways:** Cisco VG200 and ports for the Cisco Catalyst 6000 FXS Analog Interface Module
 - n **User device profiles:** Cisco IP Phone 7900 Series and Cisco SoftPhone
- Step 24** Define a format for the CSV data file. You can use the BAT spreadsheet or a text editor to create the CSV data file.
- Step 25** Validate the data input files with the Cisco CallManager database. Cisco CallManager runs a validation routine that checks the CSV file and the template for errors against the publisher database.
- Step 26** Insert the devices into the Cisco CallManager database.

Using BAT Wizard: Step 1 of 3

Cisco.com

Choose the device or option to configure.



© 2005 Cisco Systems, Inc. All rights reserved.

CIP11 v4.1-2-8

From the Configure menu, you can access the wizard by choosing one of these devices or configuration options:

- n Phones
- n Users
- n Managers/Assistants
- n User Device Profiles
- n Gateways
- n Forced Authorization Codes
- n Client Matter Codes
- n Pickup Group
- n TAPS (optional, when installed)

Using the BAT Wizard: Step 2 of 3

Cisco.com

Choose the task you want to perform.

Phone Options

<input checked="" type="radio"/> Insert Phones	Add new phones.
<input type="radio"/> Update Phones	Locate and modify existing phones.
<input type="radio"/> Delete Phones	Locate and delete phones.
<input type="radio"/> Export Phones	Locate and export specific phone records or all phone records.
<input type="radio"/> Update Lines	Locate and modify lines on existing phones.
<input type="radio"/> Add Lines	Add new lines to existing phones.
<input type="radio"/> Reset/Restart Phones	Locate and reset or restart phones.
<input type="radio"/> Insert Phones with Users	Add new phones and users.
<input type="radio"/> Generate Phone Reports	Generate customized reports for phones.
<input type="radio"/> CAPF Configuration	Locate and modify or delete the digital certificates (called locally significant certificates [LSCs]) issued by the Cisco Authority Proxy Function (CAPF) server to IP Phones.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1-2-9

After you choose a device or configuration option, the wizard displays a list of configuration tasks that are specific to that option. For example, when you choose Phones, the following list of tasks is displayed:

- n **Insert Phones:** Add new phones
- n **Update Phones:** Locate and modify existing phones
- n **Delete Phones:** Locate and delete phones
- n **Export Phones:** Locate and export specific phone records or all phone records
- n **Update Lines:** Locate and modify lines on existing phones
- n **Add Lines:** Add new lines to existing phones
- n **Reset/Restart Phones:** Locate and reset or restart phones
- n **Insert Phones with Users:** Add new phones and users
- n **Generate Phone Reports:** Generate customized reports for phones
- n **CAPF Configuration:** Locate and modify or delete the digital certificates (called locally significant certificates [LSCs]) issued by the Cisco Authority Proxy Function (CAPF) server to IP Phones

Using the BAT Wizard: Step 3 of 3

Cisco.com

Wizard guides you through steps specific to the task.

Steps to Insert Phones

Step 27: Add, view, or modify phone templates

Step 28: Create the CSV data file

Step 29: Validate phone records

Step 30: Insert phones

Step 31: Save the configuration

Use Back

After you choose the configuration task, the wizard provides a list of steps that are specific to the task. For example, to guide you through the Insert Phones task, the wizard displays the following steps:

Step 27 Add, view, or modify existing phone templates.

Step 28 Create the CSV data file.

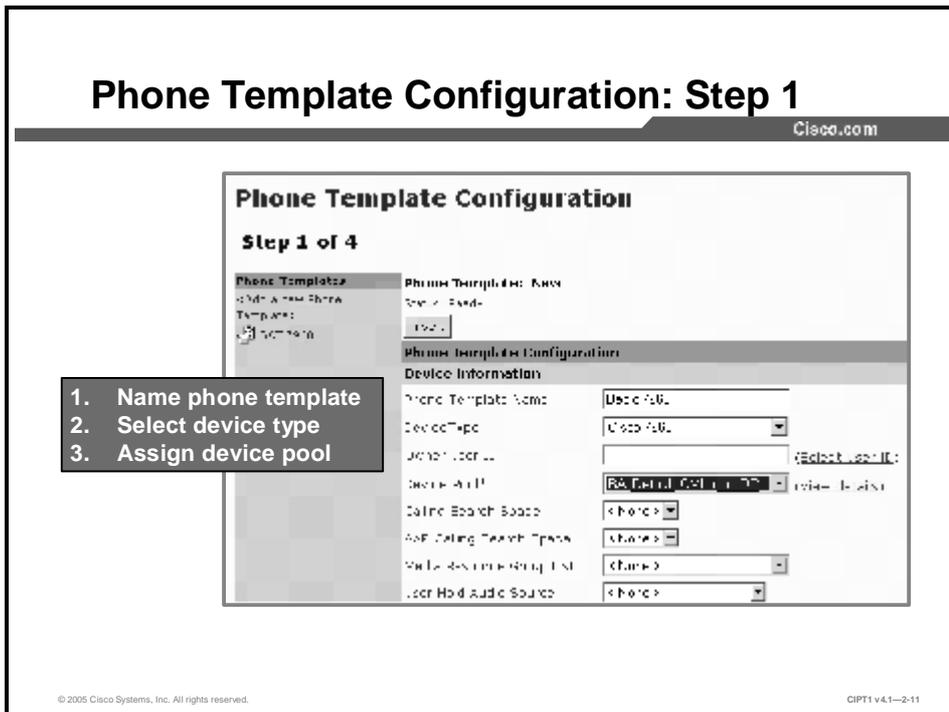
Step 29 Validate phone records.

Step 30 Insert phones.

When you choose a step from the task list, you open a configuration window such as the Phone Template Configuration window. The configuration window provides the entry fields for defining a template.

Configuring BAT Templates

This topic describes how to use BAT to configure a Cisco IP Phone template.



The first task in the BAT configuration process is to set up a template for the devices that you are configuring. You specify the type of phone or device that you want to add or modify, and then you create a BAT template that has features that are common to all the phones or devices in that bulk transaction.

Prior to creating the template, make sure that phone settings, such as device pool, location, calling search space, button template, and softkey templates, have already been configured in Cisco CallManager Administration. You cannot create new settings in BAT.

The first steps in configuring an IP Phone template are to give the phone template a unique name, and choose an IP Phone (device) type in the Phone Template Configuration window, as shown here. Choose the template that encompasses all of the IP Phones in the group. If you have multiple telephone types in a given group, you must create multiple templates.

Next, assign the template to a device pool. After you have configured the initial template information, click **Insert** to add the template to the BAT utility.

Phone Template Configuration: Step 2

Cisco.com

After adding the template in the BAT utility, you can configure necessary line settings.



Scroll down and click a line.



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-12

After configuring the initial template settings, you can modify specific line configurations. Choose a line to configure, and a new configuration window appears. These general configuration settings can apply to multiple IP Phones, such as partitions, calling search spaces, and call waiting settings. BAT obtains line configurations that are specific to the user from the imported Microsoft Excel spreadsheet.

Phone Template Configuration: Step 3

Cisco.com

Configure line settings for template

Line 1 for Phone Template Configuration Basic 7960

Line Details

Directory Number

Number

Directory Number Settings

Webbed Profile

Calling Search Space

ANI Group

Host and Auto Tone

Network Call Admission Control

Auto Answer

Call Forward and Pickup Settings

	Voice Mail	Coverage/ Destination	Calling Search Space
Forward All	<input type="checkbox"/>		<None>
Forward Busy Forward	<input type="checkbox"/>		<None>
Forward Busy Forward	<input type="checkbox"/>		<None>
Forward No Answer Forward	<input type="checkbox"/>		<None>
Forward No Answer Forward	<input type="checkbox"/>		<None>

© 2005 Cisco Systems, Inc. All rights reserved.

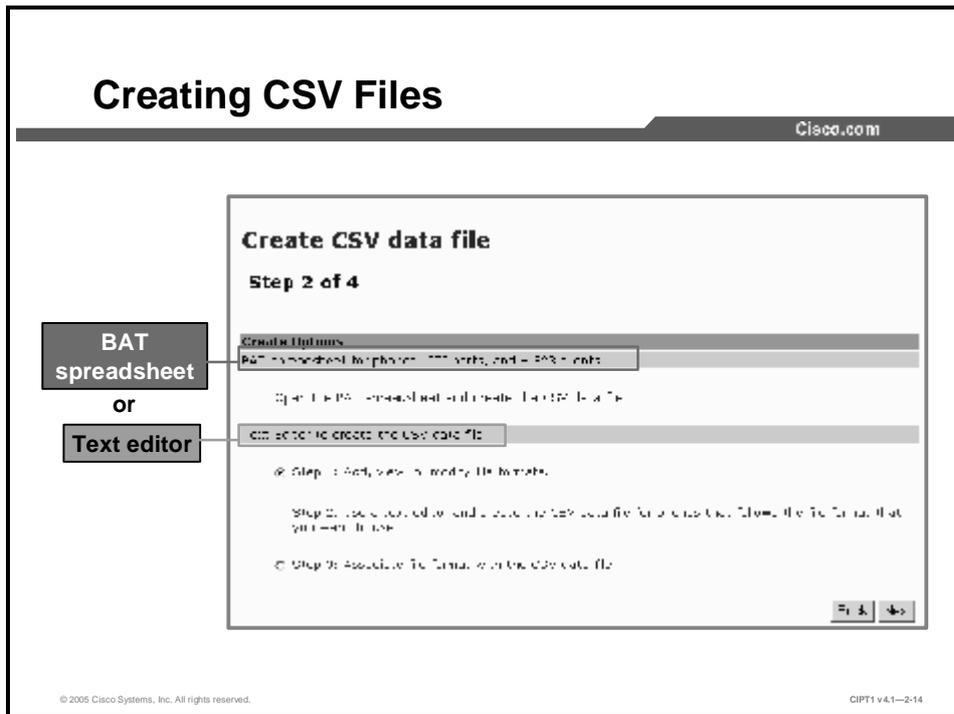
CIPT1 v4.1--2-13

Configure the line settings by choosing the desired options from the menus and then clicking **Insert and Close**.

When you are adding a group of phones that have multiple lines, you can create a master phone template that provides multiple lines and the most common values for a specific phone model. You can use the master template to add phones that have differing numbers of lines, but do not exceed the number of lines in the master phone template. For example, you can create a master phone template for a Cisco IP Phone 7960 that has six lines. You can use this template to add phones that have one line, two lines, or up to six lines.

Creating CSV Files

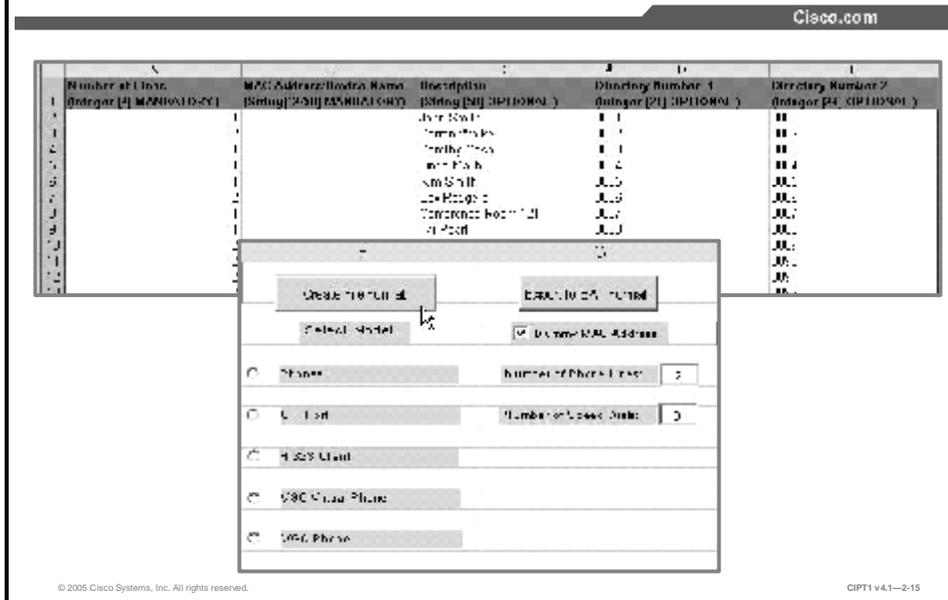
This topic describes how to create a CSV file to use with BAT.



The CSV data file contains the unique settings and information for each individual device, such as its DN, MAC address, and description. Make sure that all phones and devices in a CSV data file are the same phone or device model and match the BAT template. The CSV data file can contain duplicates of some values from the BAT template. Values in the CSV data file override any values that were set in the BAT template. You can use the override feature for special configuration cases.

You can create CSV files in one of two ways: by using the Microsoft Excel spreadsheet BAT.xlt file or by using a text editor such as Microsoft Notepad. The BAT spreadsheet simplifies the creation of CSV data files. When you are adding new devices to the system, you can use this spreadsheet, which was designed to use with BAT. You can add multiple devices and view the records for each device in a spreadsheet format. It allows you to customize the file format within the spreadsheet and provides validation and error checking automatically to help reduce configuration errors. Experienced BAT users who are comfortable with working in a CSV-formatted file can use a text editor to create a CSV data file.

Creating CVS File Using BAT Spreadsheet: Phones



This figure shows the BAT.xlt Microsoft Excel spreadsheet. You can find this spreadsheet in the directory C:\CiscoWebs\BAT\ExcelTemplate\ on the publisher database server. You probably do not have Microsoft Excel running on the publisher, so you must copy the file to a local machine (using either a floppy disk or a mapped network drive). After you have copied the file, double-click **BAT.xlt**. When prompted, click **Enable Macros**.

The BAT spreadsheet includes tabs along the bottom of the spreadsheet for access to the required data input fields for the various devices and user combinations in BAT. The CSV data file works in combination with the BAT template. For example, when you choose the Phone tab in the BAT spreadsheet, you can leave Location, Forward Busy Destination, or Call Pickup Group blank. The values from the BAT phone template are used for these fields; however, if you specify values for Forward Busy Destination or Call Pickup Group, those values override the values for these fields that were set in the BAT phone template.

After entering the data into the BAT spreadsheet, click **Export to BAT Format** to create the CSV file. The format for CSV files is <tablename><timestamp>.txt. The system saves the file to C:\XLSDataFiles\ or to a folder of your choice. You must move the converted CSV file from the C:\XLSDataFiles\ folder on your local computer back to the publisher, where BAT can access the CSV file and place it in the appropriate folder under C:\BATFiles. (For example, you would save a phone CSV data file to the C:\BATFiles\Phones\ Insert\ folder on the publisher database for Cisco CallManager.)

Using a text editor is the other way to create a CSV file. When using a text editor, follow these steps:

Step 31 Create the customized file format using the BAT File Format Configuration window. The file format specifies the order in which you enter values in the text file. This allows you to add attributes to the file format that are also in the BAT template, and override the template entry with a specific attribute for a device. For instance, you can choose the route partition attribute for your file format and enter different partitions for each phone in the CSV data file.

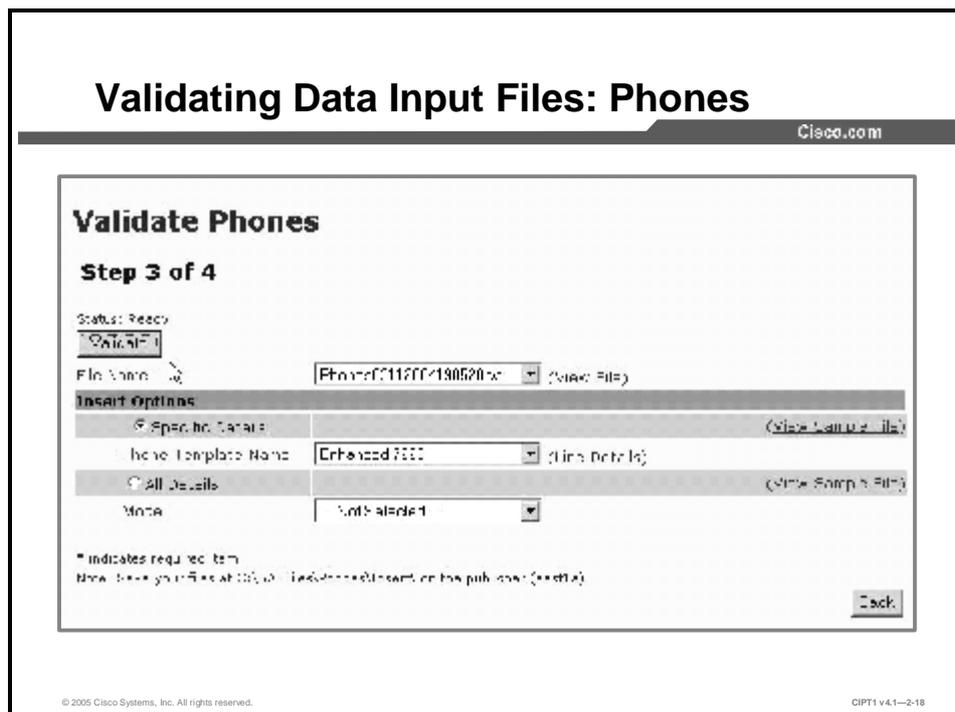
Note Earlier versions of BAT supported only a default file format with a fixed and limited number of attributes and settings for each device and an All Details format that includes all attributes and settings for each device.

Step 32 Associate the file format with the CSV data file.

You can associate only one file format with a CSV data file. Use the Add File Format window to choose the name of the CSV data file <CSVfilename>.txt from the File Name drop-down menu. Next, you choose your file format from the File Format Name drop-down menu. The data in the CSV data file must match the custom file format that you have chosen.

Validating Data Input Files

This topic describes the process for validating data input files prior to inserting the devices into the Cisco CallManager database.



In the next task in the BAT wizard, you use the Validate File option. In this task, you choose the name of the CSV data file and the BAT template for the device or the model when you have a CSV data file with all details. You have these options for how records are validated:

- n **Specific Details:** For validating records that follow the default or custom file format
- n **All Details:** For validating records from a file that was generated with the export utility by using the All Details option

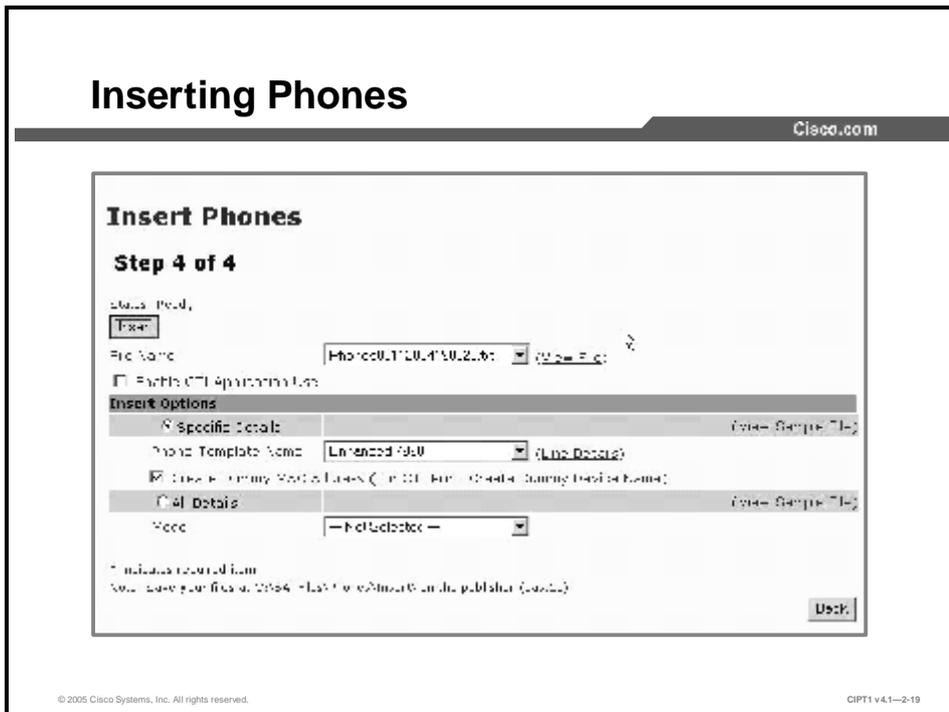
When you choose Validate, the system runs a validation routine to check for errors against the publisher database. These checks ensure the following:

- n Fields such as description, display text, and speed-dial label use valid characters.
- n Cisco CallManager groups, device pools, partitions, and other referenced attributes are already configured.
- n The number of lines that are configured on a device does not exceed the device template.

Validation does not check for the existence of a user or for mandatory or optional fields that are BAT-defined, such as the dummy MAC address.

Inserting IP Phones into Cisco CallManager

This topic describes how to insert Cisco IP Phones into the Cisco CallManager database.



Inserting the device into the Cisco CallManager database is the last step in using BAT to perform bulk configurations. The following steps are involved in this procedure:

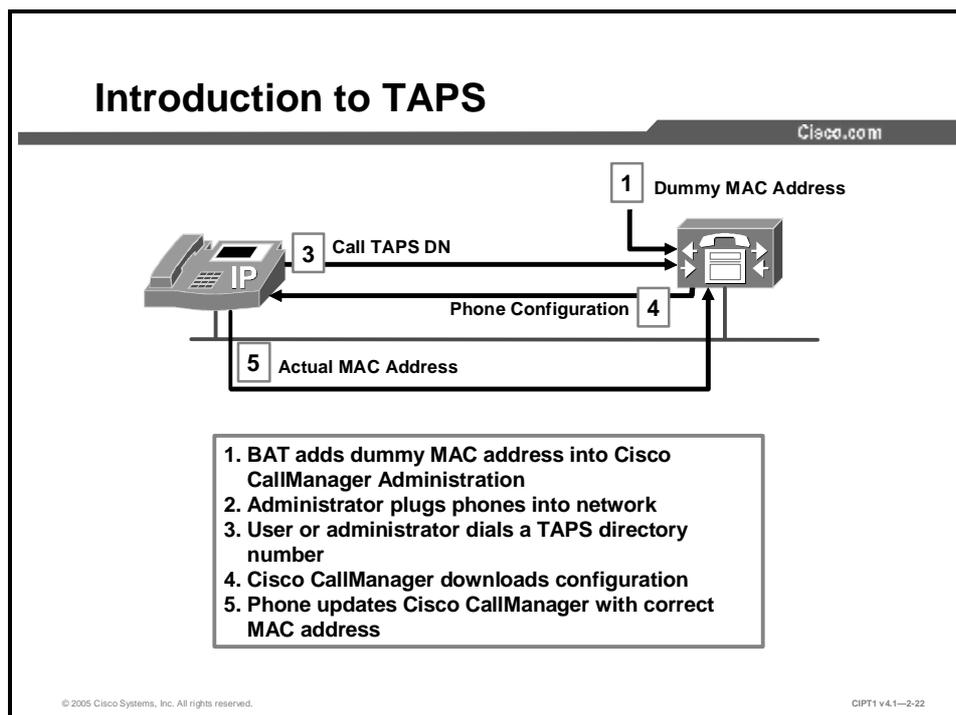
- Step 33** In the File Name field, choose the CSV data file that you created for this specific bulk transaction.
- Step 34** To enable the use of applications such as Cisco IP SoftPhone, check the **Enable CTI Application Use** check box (for CTI ports only).
- Step 35** Choose the Insert option that corresponds to your CSV data file.
- Step 36** In the Phone Template Name field, choose the BAT phone template that you created for this type of bulk transaction.
- Step 37** If you did not enter individual MAC addresses in the CSV data file, check the **Create Dummy MAC Address** check box.

This field automatically generates dummy MAC addresses in the following format: XXXXXXXXXXXX, where X represents any 16-character, hexadecimal (0 to 9 and A to F) number. You can update the phones or devices later with the correct MAC address by manually entering this information into Cisco CallManager Administration or by using TAPS.

- Step 38** Click **Insert** to insert the phone records.

Using the Tool for Auto-Registered Phone Support

This topic describes how to install and configure TAPS.



Use TAPS in conjunction with BAT to provide two features:

- n Update MAC addresses and download predefined configuration for new phones
- n Reload configuration for replacement phones

When new phones are added to Cisco CallManager, TAPS works in conjunction with BAT to update phones that were added to BAT using dummy MAC addresses. After BAT has been used to bulk-add the telephones with dummy MAC addresses to Cisco CallManager Administration, you can plug the telephones into the network. You or the user of the telephone can dial a TAPS DN that causes the phone to download its configuration. At the same time, the telephone is updated in Cisco CallManager Administration with the correct MAC address. You must make sure that auto-registration is enabled in Cisco CallManager Administration (System > Cisco CallManager) for TAPS to function.

TAPS Installation

Cisco.com

- **With BAT Release 5.0(1), TAPS is installed separately.**
- **TAPS installation prerequisites:**
 - **Make sure the publisher database for Cisco CallManager is configured and running.**
 - **Ensure that the Cisco CRS server is configured.**
 - **Ensure that the Windows 2000 Services window is closed.**
 - **Ensure that the latest BAT is installed on the publisher database server for Cisco CallManager.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-23

Prior to BAT Release 5.0(1), TAPS installation and uninstallation for Cisco CallManager was part of the BAT installation program. With BAT Release 5.0(1) and above, TAPS is installed separately.

During TAPS installation or reinstallation on the publisher database server, the setup program halts the following services:

- n Microsoft IIS Administration
- n World Wide Web publishing
- n FTP publishing

These services restart when the installation is finished.

You cannot use Windows Terminal Services to install TAPS. You must install TAPS directly from the Cisco CallManager publisher server and the Cisco Customer Response Solutions (CRS) server.

These prerequisites apply to the TAPS installation for BAT:

- n Make sure that the publisher database for Cisco CallManager is configured and running. The publisher database can reside on its own server or on the same server as Cisco CallManager.
- n Before installing TAPS, ensure that the latest BAT release is installed on the publisher database server for Cisco CallManager.
- n Have the IP address for the Cisco CallManager publisher server and the private phrase for the installation procedure.
- n Ensure that the Cisco CRS server is configured. The Cisco CRS Version 3.5 application can reside on its own dedicated server or can be colocated on the same server as Cisco CallManager.
- n Be sure to use the locale installer to create the country-specific TAPS prompts.
- n Ensure that the Windows 2000 Services window is closed.

Complete the following steps to install TAPS:

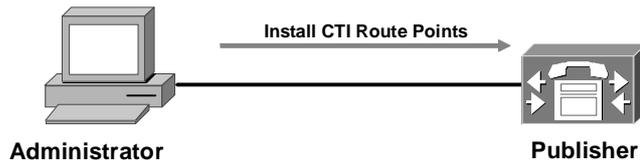
- Step 39** Log in with administrator privileges to the system that is running the publisher database for Cisco CallManager (where you installed BAT).
- Step 40** Access BAT.
- Step 41** Choose **Applications > Install Plugins**.
- Step 42** Double-click the TAPS setup icon.
- Step 43** Determine whether to copy the TAPS installation executable to the system or run it from the current location.
- Step 44** The Welcome window for the installation wizard opens. This installation program installs TAPS on the Cisco CallManager publisher server and the CRS applications server at the same time, if applications are colocated on the same server. Click **Next**.

Note When you are installing TAPS in a network with a dedicated CRS server, you must run the TAPS installation program again on the CRS server. Use CRS online help for assistance with installation and configuration.

- Step 45** Enter the private phrase for the Cisco CallManager publisher server in the Installing Cisco CallManager Components window and click **Next**. The Installing TAPSONCCM window displays a progress bar that shows the status of the installation.
- Step 46** The Installation Completed window is displayed when the installation ends. Click **Finish**.

TAPS Configuration Requirements

Cisco.com



Add a computer telephony integration (CTI) route point, CTI ports, and users in Cisco CallManager Administration.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-24

You must configure TAPS by adding a CTI route point, CTI ports, and users in Cisco CallManager Administration, as shown here. One CTI route point and at least one CTI port are required for TAPS.

The following procedure describes how to configure TAPS in Cisco CallManager Administration:

Note To use TAPS, verify that auto-registration is enabled in Cisco CallManager. Because TAPS can replace a DN, you can protect certain DNs from being overwritten by using the Secure TAPS option.

- Step 6** Create a CTI route point and assign it a unique DN.
- Step 7** Choose the **Call Forward Busy**, **Call Forward No Answer**, and **Call Forward on Failure** options for the operator number on the TAPS CTI route point.
- Step 8** Create one or more CTI ports with consecutive DNs. You can create CTI ports in BAT or Cisco CallManager Administration.
- Step 9** Create a user. The TAPS route point and ports should be in the Controlled Devices list of the user.
- Step 10** Create an auto-registration partition or calling search space or both to prevent IP Phones that have auto-registered from dialing any DN other than the number that is assigned to the TAPS CTI route point. Restricting access to this DN ensures that users download the proper configuration information for their IP Phones.

Note TAPS supports a maximum number of simultaneous sessions equal to the number of CTI ports that are configured for TAPS. For example, if you have configured five CTI ports, up to five users can dial into TAPS at same the time. The sixth caller cannot connect to TAPS.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **BAT uses a template and CSV file to insert bulk transactions into the Cisco CallManager database.**
- **You must install BAT on the same server as the publisher database for Cisco CallManager.**
- **The BAT Wizard steps you through the BAT configuration process.**
- **BAT templates enable you to insert, update, or delete IP Phones, gateways, and user device profiles.**
- **You can create a CSV file using the BAT spreadsheet or text editor.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-25

Summary (Cont.)

Cisco.com

- **After creating the CSV file, BAT must validate the file and template.**
- **Inserting the Cisco IP Phones, users, or device is the last step in bulk configuration.**
- **To update phones, query to find the phones, specify the values, and then reset the phones.**
- **TAPS, an optional application that BAT provides, retrieves the predefined configuration for auto-registered IP Phones.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT1 v4.1—2-26

References

For additional information, refer to this resource:

- n Cisco Systems, Inc. *Bulk Administration Tool User Guide, Release 5.1(4)*.
http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/voice/c_callmg/4_1/bulk_admin/index.htm.

Module 2 Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **Cisco IP telephony endpoints support the G.711 and G.729 codecs and include the full range of desktop, PC-based, and conference-room IP Phones. To register to a Cisco CallManager, an IP Phone obtains a VLAN ID and IP address and downloads configuration information from the TFTP server.**
- **Configuring Cisco CallManager to automatically or manually add IP endpoints entails changing the Cisco CallManager name to its IP address, configuring device pools, and assigning phone button templates.**
- **Cisco Catalyst switches provide three important functions in an IP telephony deployment: voice VLANs, CoS, and PoE.**
- **Cisco IP Communicator is a PC-based phone with all the features of a high-end Cisco IP Phone. Adding Cisco IP Communicator to the Cisco CallManager database is similar to adding a Cisco IP Phone 7940, 7960, or 7970.**
- **BAT enables you to add large numbers of devices, users, and ports to the Cisco CallManager database. BAT can be used anytime but is typically used during deployment or when making wholesale changes to phone extensions. Day-to-day changes to an individual phone are normally done in Cisco CallManager Administration.**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT1 v4.1--2-1

This module covered the key ingredients to enable IP telephony within a cluster. This module first presented the range of Cisco IP endpoints that you can use in an IP telephony deployment and the system-level parameters that you configure in Cisco CallManager to enable and support the endpoints. The module then covered the three functions that the Cisco Catalyst switches provide in an IP telephony deployment: enabling separate voice VLANs for the IP phones, providing CoS to the voice traffic so that it receives preferential treatment, and providing PoE to power the IP phones and potentially other endpoints. The Cisco IP Communicator was presented as a fully featured PC-based alternative to a desktop IP phone for mobile and remote users. The module ended with a discussion of how to use the BAT when you want to bulk-add or update users, phones, ports, and a variety of other settings.

Module 2 Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module 2 Self-Check Answer Key.

- Q11) BAT enables you to perform which tasks? (Source: Lesson 2-5, Using the Bulk Administration Tool)
- F) reload configuration for replacement phones
 - G) add, update, and delete IP Phones, users, and devices in mass
 - H) collect user data such as passwords and account identification
 - I) update MAC addresses and download configurations for new phones
 - J) save a detailed log of Cisco CallManager events for troubleshooting
- Q12) Place these steps in the order that an IP Phone must go through before it can register with Cisco CallManager. (Source: Lesson 2-1, Identifying Cisco IP Telephony Endpoints)
- K) obtain -48 V DC power
 - L) get configuration from TFTP server
 - M) load firmware image
 - N) obtain VLAN information
- Q13) Which five settings are required to configure a device pool? (Choose five.) (Source: Lesson 2-2, Configuring Cisco CallManager to Support IP Phones)
- O) Media Resource Group List
 - P) Cisco CallManager group
 - Q) date/time group
 - R) region
 - S) softkey template
 - T) device pool name
 - U) phone template
 - V) phone load
 - W) device defaults
- Q14) On which server must you install BAT? (Source: Lesson 2-5, Using the Bulk Administration Tool)
- X) publisher server
 - Y) subscriber server
 - Z) primary server
 - AA) secondary server
- Q15) A company wants to migrate to a VoIP network, but it has an expensive all-in-one voice-fax-copier device that it wants to connect to the VoIP network. Which device would you recommend? (Source: Lesson 2-1, Identifying Cisco IP Telephony Endpoints)
- BB) Cisco Conference Station 7936
 - CC) Cisco IP SoftPhone
 - DD) Cisco ATA 188
 - EE) Cisco 7905G
 - FF) Cisco 7914 Expansion Module
- Q16) Which command enables inline power on port 3 of module 2 of a Cisco Catalyst 6000 Series switch that is running Cisco Catalyst software? (Source: Lesson 2-3, Configuring Cisco Catalyst Switches)

- GG) **power inline** in global configuration mode
 - HH) **power inline auto** in interface configuration mode
 - II) **set port inline power default**
 - JJ) **set port inline power 3/2 802.3**
 - KK) **set port inline power 2/3 auto**
- Q17) Which of the following is a valid phone button template configuration for a Cisco IP Phone 7960? (Source: Lesson 2-2, Configuring Cisco CallManager to Support IP Phones)
- LL) 0 lines, 6 speed dials
 - MM) 2 lines, 4 speed dials
 - NN) 6 lines, 1 speed dial
 - OO) 4 lines, 4 speed dials
- Q18) Before you can create a BAT template, you must make sure which four settings have already been configured in Cisco CallManager Administration? (Choose four.) (Source: Lesson 2-5, Using the Bulk Administration Tool)
- PP) device pool
 - QQ) directory number
 - RR) softkey template
 - SS) MAC address
 - TT) calling search space
 - UU) button template
- Q19) Cisco Catalyst switches can provide which three functions in an IP telephony deployment? (Choose three.) (Source: Lesson 2-3, Configuring Cisco Catalyst Switches)
- VV) convert SCCP signaling packets from the IP Phone to MGCP
 - WW) power IP Phones through the same Ethernet cable that carries data
 - XX) enable the classification and prioritization of voice packets at Layer 2
 - YY) instruct the IP Phone to change the CoS of an incoming data frame
 - ZZ) determine available bandwidth before placing a call over the WAN
- Q20) What are the two ways to create CSV files? (Choose two.) (Source: Lesson 2-5, Using the Bulk Administration Tool)
- AAA) choose Configure > CSV File
 - BBB) use a text editor and save to the correct folder
 - CCC) modify BAT.xlt and export to BAT format
 - DDD) save the IP Phone template in CSV format
- Q21) Which navigation path would you use to configure Cisco CallManager to automatically register an IP Phone? (Source: Lesson 2-2, Configuring Cisco CallManager to Support IP Phones)
- EEE) System > Server
 - FFF) System > Cisco CallManager
 - GGG) Service > Service Parameters
 - HHH) Device > Phone
 - III) System > Device Pool
- Q22) What are three requirements for configuring dual VLANs on a single port that is attached to an IP Phone? (Choose three.) (Source: Lesson 2-3, Configuring Cisco Catalyst Switches)
- JJJ) Configure the interface as a trunk.
 - KKK) Tag the voice packets with an identifier.
 - LLL) Extend the CoS boundary to the IP Phone.

- MMM) Ensure that the IP Phone has an internal switch.
NNN) Ensure that the IP Phone is inline power-capable.
- Q23) How does Cisco CallManager tie configuration information to the IP Phones in the Microsoft SQL database? (Source: Lesson 2-2, Configuring Cisco CallManager to Support IP Phones)
- OOO) IP address
 - PPP) unique GUID
 - QQQ) hostname
 - RRR) MAC address
 - SSS) device pool ID
- Q24) Which two items must be installed for TAPS to function properly? (Choose two.) (Source: Lesson 2-5, Using the Bulk Administration Tool)
- TTT) CRS
 - UUU) BAT
 - VVV) plug-ins
 - WWW) Extension Mobility
- Q25) The BAT Wizard guides you through which four tasks? (Choose four.) (Source: Lesson 2-5, Using the Bulk Administration Tool)
- XXX) setting up a template
 - YYY) creating CSV files
 - ZZZ) installing BAT
 - AAAA) inserting phones and devices
 - BBBB) validating records
 - CCCC) obtaining MAC addresses
 - DDDD) creating the CTI point
- Q26) A firm wants to install a Cisco IP Phone in the lobby area. The IP telephony network runs only the G.729a codec. The IP Phone should support a single line and all standard features. An LCD display is not required because cost is a concern. Which IP Phone would best meet these requirements? (Source: Lesson 2-1, Identifying Cisco IP Telephony Endpoints)
- EEEE) Cisco IP Phone 7902G
 - FFFF) Cisco IP Phone 7905G
 - GGGG) Cisco IP Phone 7910G+SW
 - HHHH) Cisco IP Phone 7912G

- Q27) What must you do if you do not want to trust the device that is attached to the IP Phone?
(Source: Lesson 2-3, Configuring Cisco Catalyst Switches)
- IIII) Change the CoS value on the voice VLAN to a number lower than 5.
 - JJJJ) Use the **switchport priority extend untrust** interface command.
 - KKKK) Do nothing; the IP phone will automatically change the CoS to 0 for the attached devices.
 - LLLL) Create a dual VLAN on the access port and place the data packets in the native VLAN.
- Q28) List two functions of the Cisco IP Communicator Administration Tool. (Choose two.)
(Source: Lesson 2-4, Configuring Cisco IP Communicator)
- MMMM) collects PC MAC addresses
 - NNNN) is a software deployment tool
 - OOOO) improves audio input quality
 - PPPP) helps obtain VPN IP addresses
- Q29) If you do not know the MAC address of the Cisco IP Communicator device, which two methods can you use to add the device to Cisco CallManager? (Choose two.) (Source: Lesson 2-4, Configuring Cisco IP Communicator)
- QQQQ) BAT with TAPS
 - RRRR) auto-registration
 - SSSS) Device menu
 - TTTT) Administration Tool
 - UUUU) Directory Wizard

Module 2 Self-Check Answer Key

- Q11) B
- Q12) A, C, D, B
- Q13) B, C, D, E, F
- Q14) A
- Q15) C
- Q16) E
- Q17) B
- Q18) A, C, E, F
- Q19) B, C, D
- Q20) B, C
- Q21) B
- Q22) A, B, D
- Q23) D
- Q24) A, B
- Q25) A, B, D, E
- Q26) A
- Q27) C
- Q28) B, D
- Q29) A, B