CIPT

Cisco IP Telephony

Version 3.3

Student Guide

Text Part Number:

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • 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

ADDITIONAL RESOURCES

Course Introduction

Overview

The Cisco IP Telephony (CIPT) course is designed to prepare you for installing, configuring, and maintaining a Cisco IP telephony solution. This course focuses primarily on Cisco CallManager (CCM), the call routing and signaling component for the Cisco IP telephony solution. You will also identify many of the CCM features and capabilities throughout this course.

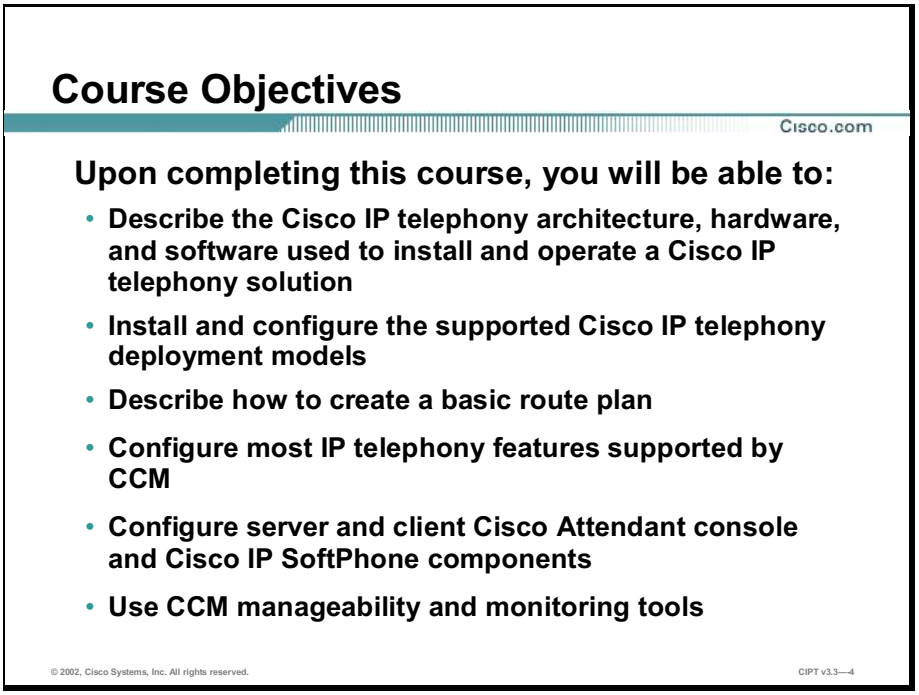
Outline

The Course Introduction includes these topics:

- Course Objectives
- Cisco Certification Track
- Learner Skills and Knowledge
- Learner Responsibilities
- General Administration
- Cisco IP Telephony Laboratory Topology
- Course Flow Diagram
- Icons and Symbols
- Sources of Information
- Learner Introductions

Course Objectives

This topic lists the course objectives.

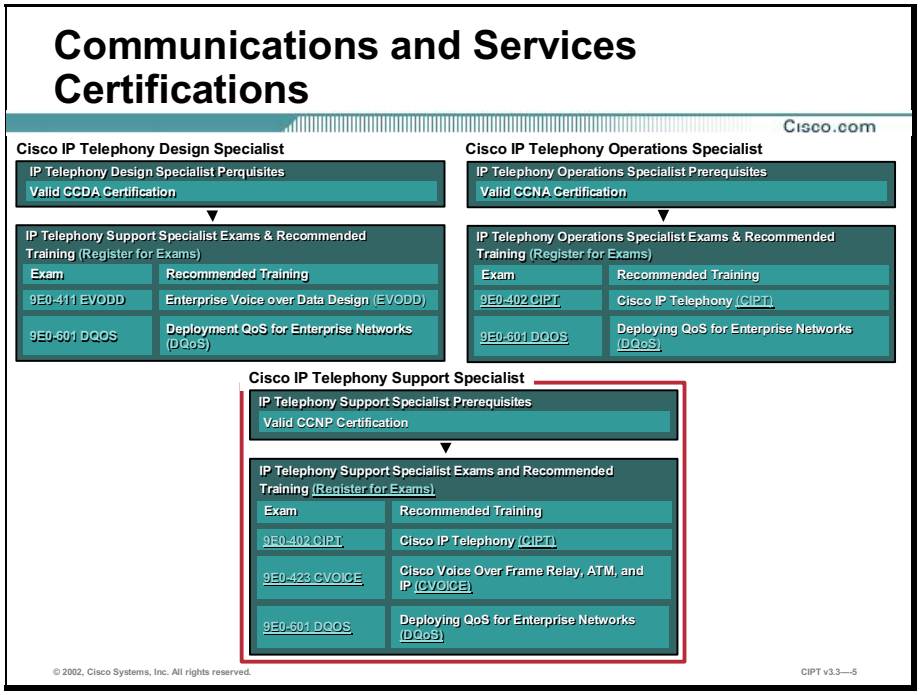


Upon completing this course, you will be able to:

- Describe the Cisco IP telephony architecture, hardware, and software used to install and operate a Cisco IP telephony solution
- Install and configure the supported Cisco IP telephony deployment models
- Describe how to create a basic route plan
- Configure most IP telephony features supported by CCM
- Configure server and client Cisco Attendant console and Cisco IP SoftPhone components
- Use CCM manageability and monitoring tools

Cisco Certification Track

This topic lists the certification requirements of this course.

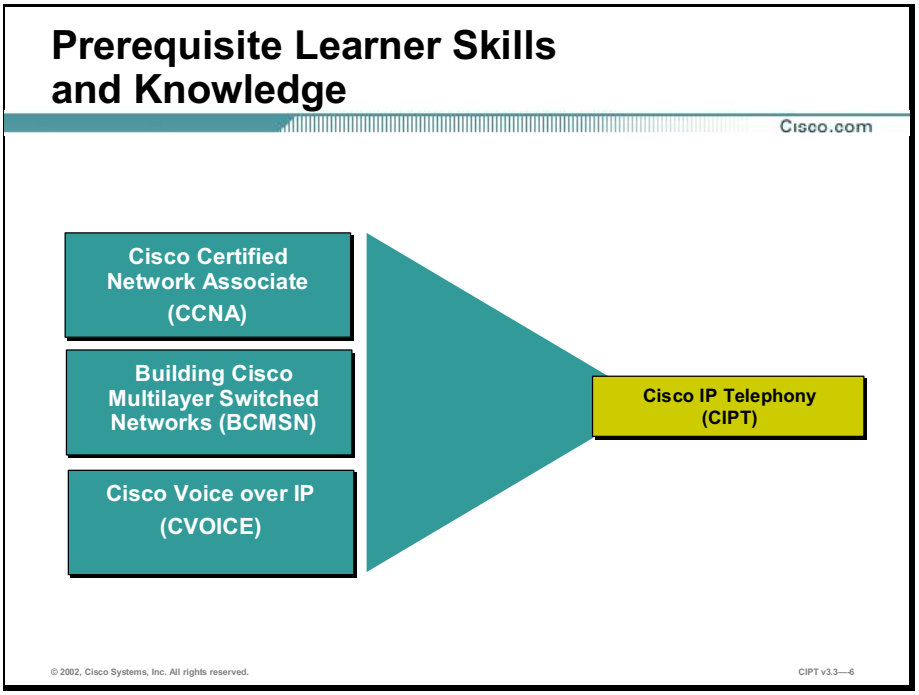


This education offering is a course focused on IP telephony, targeted towards the *Cisco IP Telephony Design Specialist* certification.

- The *Cisco IP Telephony Design Specialist* certification is a Cisco Qualified Specialist (CQS) certification.
- The requirements for the *Cisco IP Telephony Design Specialist* certification include the successful completion of the CCNP certification and the CIPT, CVOICE, and DQOS exams.

Learner Skills and Knowledge

This topic lists the course prerequisites.

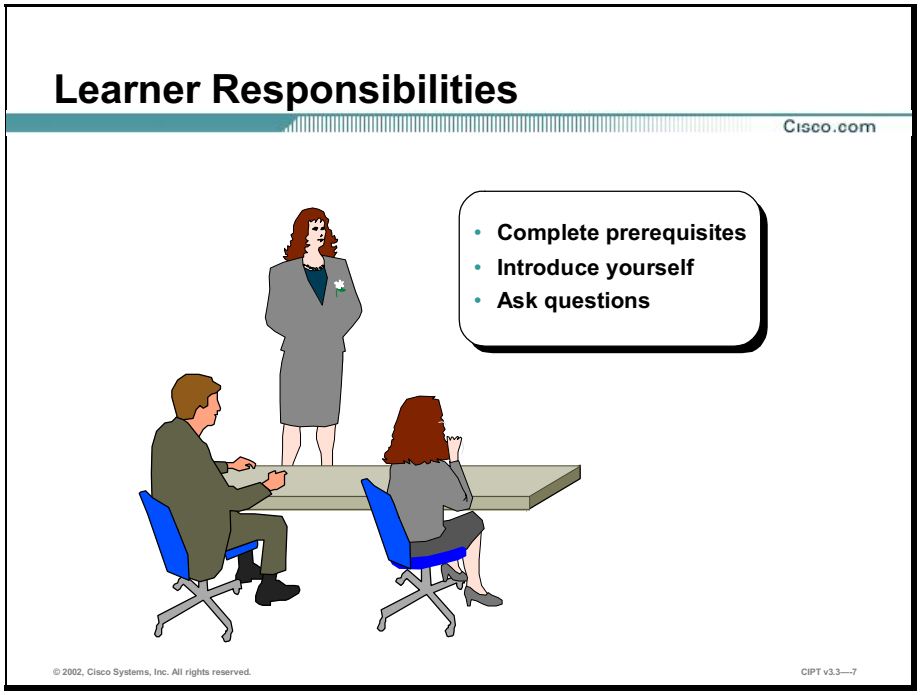


To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Obtained a Cisco Certified Network Associate (CCNA)
- Completed the Building Cisco Multilayer Switched Networks (BCMSN) course
- Completed the Cisco Voice over IP (CVOICE) course

Learner Responsibilities

This topic describes the responsibilities of the learners.



To take full advantage of the information presented in this course, you must have completed the prerequisite requirements.

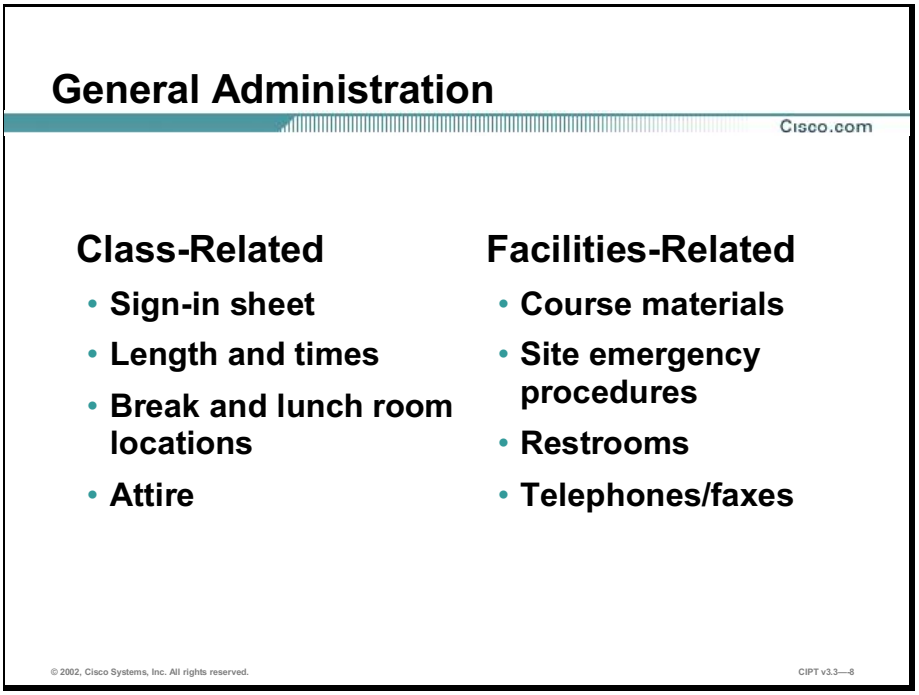
In class, you are expected to participate in all lesson exercises and assessments.

In addition, you are encouraged to ask any questions relevant to the course materials.

If you have pertinent information or questions concerning future Cisco product releases and product features, please discuss these topics during breaks or after class. The instructor will answer your questions or direct you to an appropriate information source.

General Administration

This topic lists the administrative issues for the course.

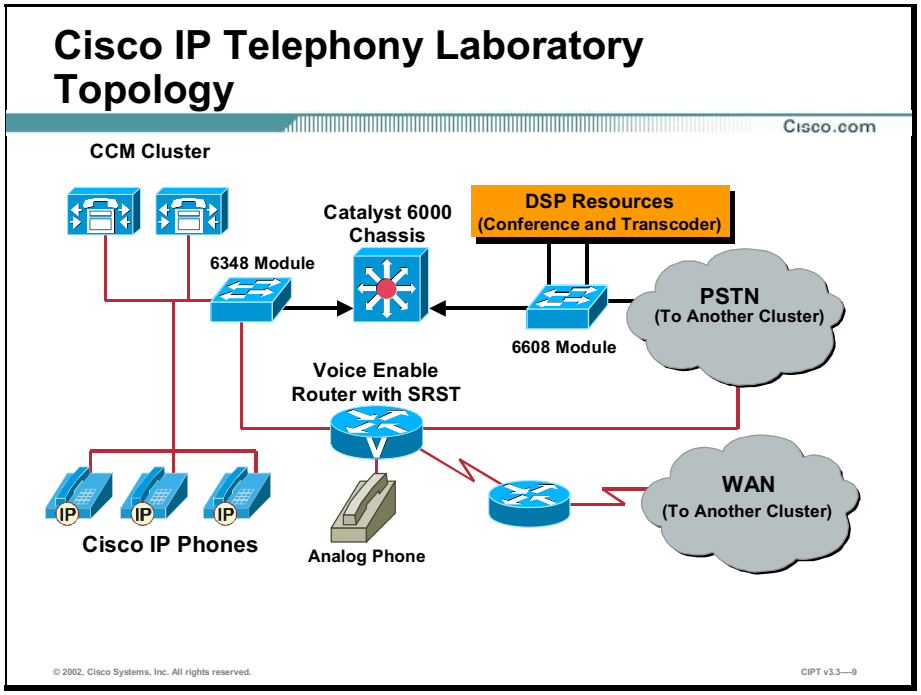


The instructor will discuss the administrative issues noted here so that you know exactly what to expect from the class.

- Sign-in process
- Starting and anticipated ending times of each class day
- Class breaks and lunch facilities
- Appropriate attire during class
- Materials you can expect to receive during class
- What to do in the event of an emergency
- Location of the restrooms
- How to send and receive telephone and fax messages

Cisco IP Telephony Laboratory Topology

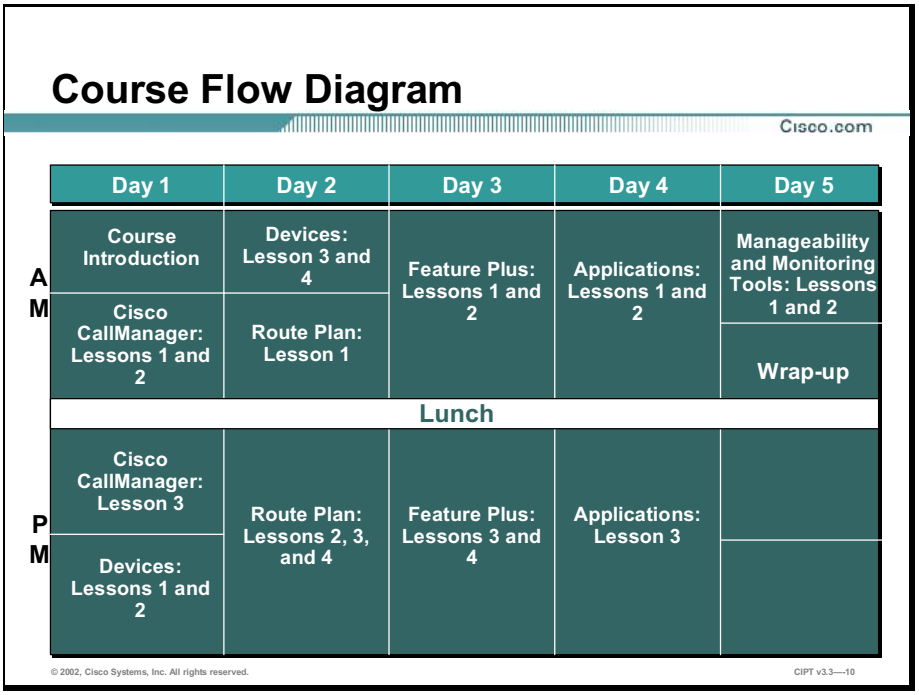
This topic introduces the Cisco IP telephony laboratory topology that is used during this course.



This figure is a generalization of the laboratory topology used for the CIPT course. Cisco offers a variety of products, with similar functionality, which can provide a consistent reinforcement of learning objectives not related to specific products.

Course Flow Diagram

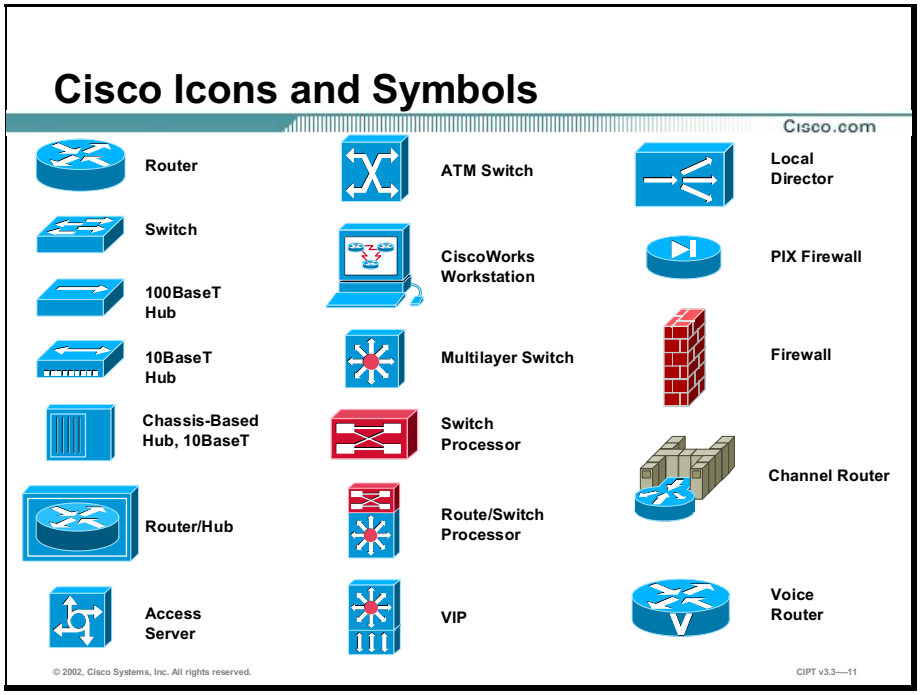
This topic covers the suggested flow of the course materials.



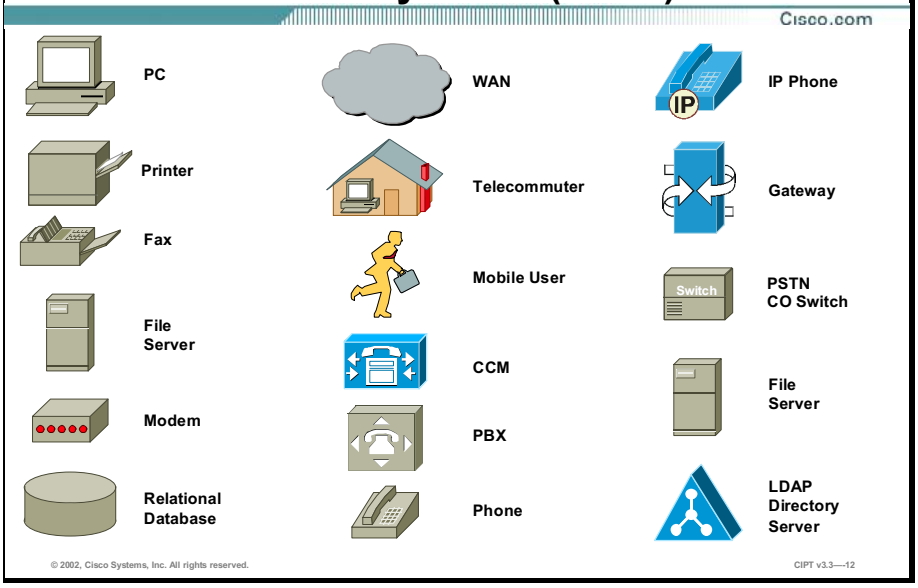
The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the laboratory exercises. The exact timing of the subject materials and labs depends on the pace of your specific class.

Icons and Symbols

This topic shows the Cisco icons and symbols used in this course.



Cisco Icons and Symbols (Cont.)



Cisco Icons and Symbols (Cont.)

Cisco.com


Building


Building


Laptop

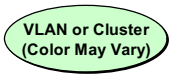

Switch
Router


IP
Standard


Video
Conference


Video
Camera

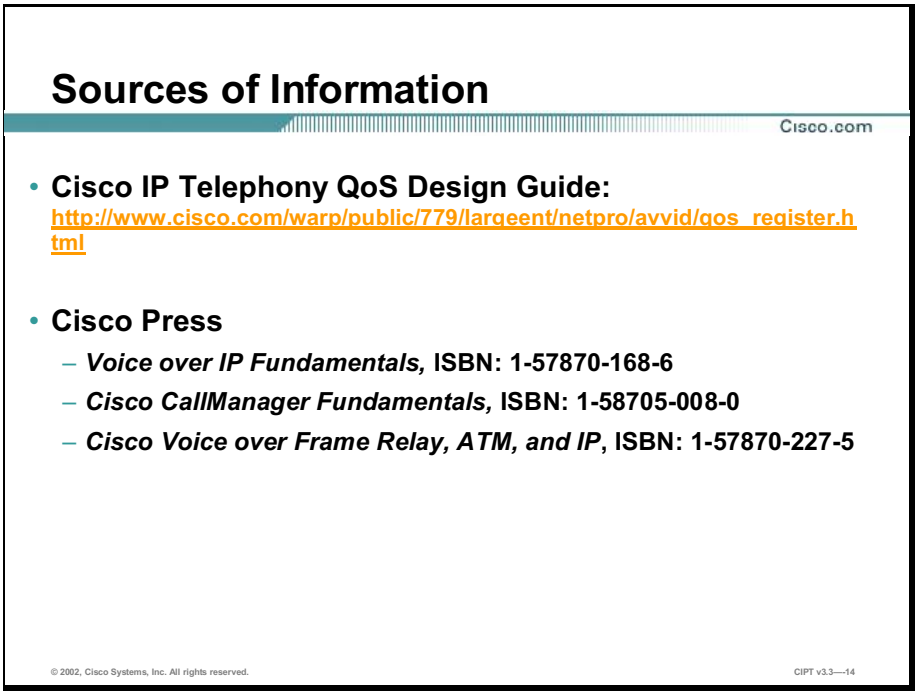

IBM
Mainframe



Digital Signal
Processor

Sources of Information

This topic shows supplemental resources.



In addition to the course material, the following resources provide supplemental information regarding voice over data design:

- Cisco IP Telephony QoS Design Guide: http://www.cisco.com/warp/public/779/largeent/netpro/avvid/qos_register.html

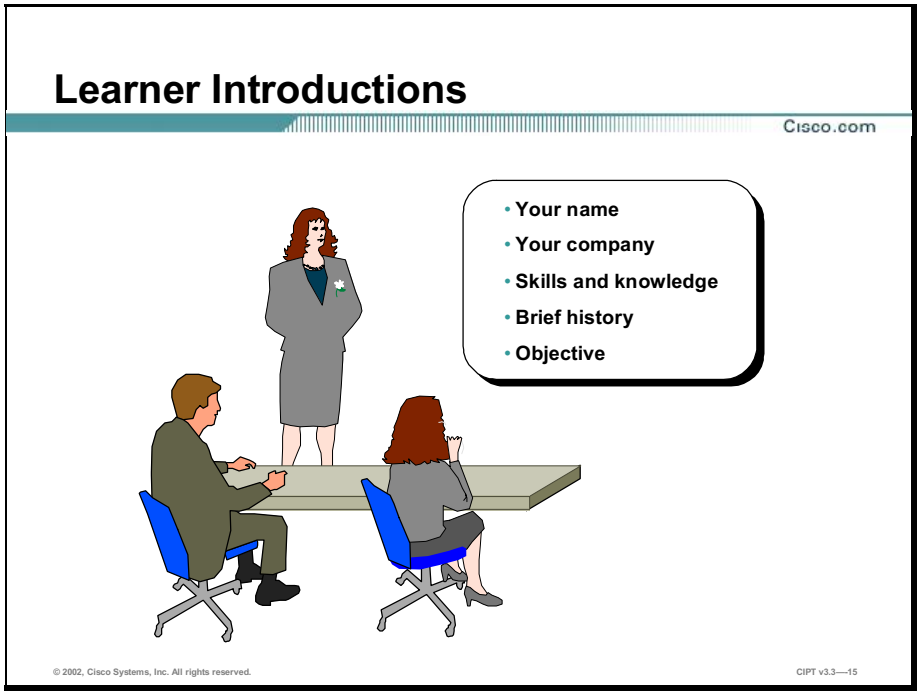
Note	These require a Cisco.com login.

- Cisco Press

1. Davidson, J. *Voice over IP Fundamentals.* San Jose, California: Cisco Press; 2000.
2. Smith, A., Chris Peace, Delon Whetton, and John Alexander. *Cisco CallManager Fundamentals: A Cisco AVVID Solution.* San Jose, California: Cisco Press; 2001.
3. McGrew, Kelly, and Steve McQuerry. *Cisco Voice over Frame Relay, ATM, and IP*. San Jose, California: Cisco Press; 2001.

Learner Introductions

This is the point in the course where you introduce yourself.



Prepare to share the following information:

- Your name
- Your company
- If you have most or all of the prerequisite skills
- A profile of your experience
- What you would like to learn from this course

1

Cisco CallManager

Overview

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

Upon completing this module, you will be able to:

- Describe the purpose of CCM and the Cisco Architecture for Voice, Video and Integrated Data strategy
- Identify the servers that CCM supports
- Install a CCM server
- Describe intracluster CCM communication
- Identify the available deployment models for a Cisco IP telephony solution

Outline

The module contains these lessons:

- Introduction to Cisco AVVID and Cisco CallManager
- Cisco CallManager Cluster and Deployment Options
- Installing Cisco CallManager

Introduction to Cisco AVVID and Cisco CallManager

Overview

Cisco Architecture for Voice, Video and Integrated Data (AVVID) provides the framework for Internet business solutions. Cisco CallManager (CCM) is the call-routing and signaling component for a Cisco IP telephony solution. This lesson will teach you about the Cisco AVVID and CCM features and functions. You will learn the fundamental components of a Cisco IP telephony solution.

Importance

This lesson benefits individuals who want to increase their understanding of Cisco AVVID and CCM and the role they play in converged networks. This lesson provides information about the advantages of a converged Cisco AVVID network, the CCM functions in a Voice over IP (VoIP) network, and the minimum requirements for installing a CCM server.

Objectives

Upon completing this lesson, you will be able to:

- Compare and contrast legacy networks with converged Cisco AVVID networks
- Describe the Cisco AVVID strategy for voice networks
- Identify the CCM functions
- Compare legacy PBX technologies with IP telephony technologies
- Describe requirements for installing a CCM server
- Describe the hardware requirements for CCM
- Identify the number of device weight units that a hardware platform can support

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Basic working knowledge of a computer and experience installing software onto a PC
- Basic understanding of network connectivity

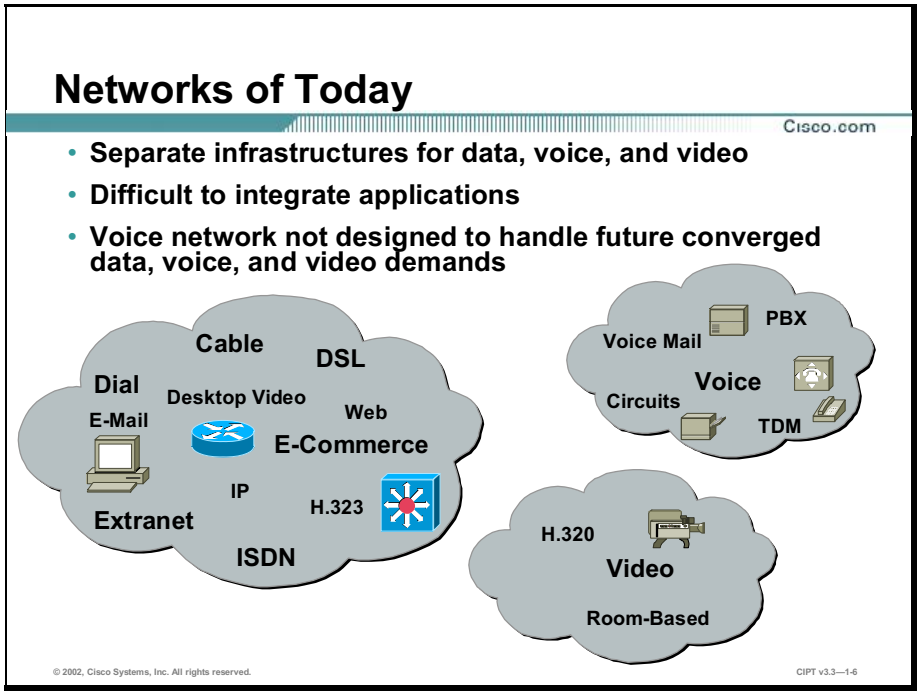
Outline

This lesson includes these topics:

- Overview
- Traditional and Converged Networks
- Cisco AVVID
- CCM Functions
- Comparing Legacy and IP Telephony Technology
- CCM Operating System, Database, and Supporting Applications
- Supported CCM Hardware
- Device Weight Units
- Summary
- Lesson Review

Traditional and Converged Networks

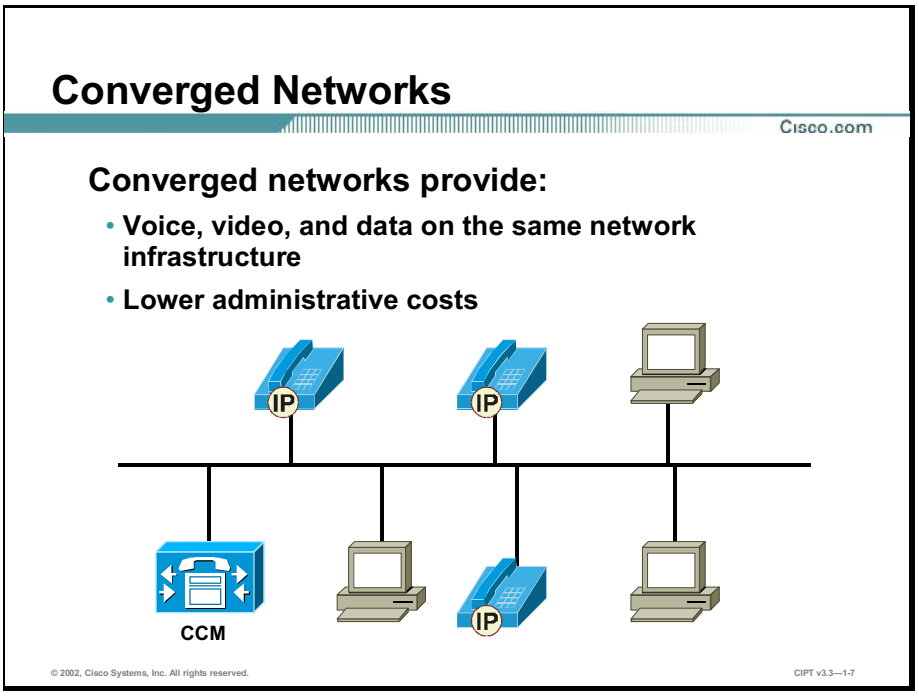
This topic describes the migration from traditional networks to converged networks.



Today, multiple communication networks are entirely separate, each of them serving a specific application. For example, the traditional Public Switched Telephone Network (PSTN) serves voice applications; the Internet and intranets serve data communications; and multiple private and public H.320 networks serve videoconferencing.

Everyday business requirements often force these networks to interoperate. Consider the last time that you participated in a videoconference using the PSTN and a Polycom for audio, or consider the last time that you used Microsoft NetMeeting.

Deploying multiservice (data, voice, and video) applications is a daunting task that requires expensive and complex links between proprietary systems (such as PBXs) and standards-based data networks.

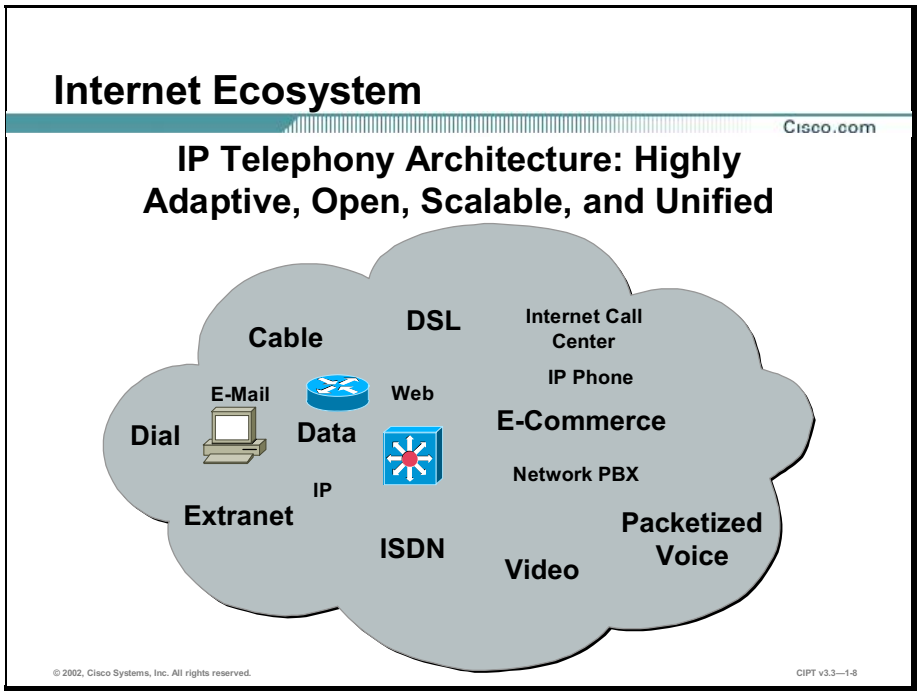


Because managing multiple networks can be extremely complex and cost prohibitive, the Cisco Architecture for Voice, Video and Integrated Data (AVVID) strategy combines voice, video, and data networks into a single entity. Although network administrators have long considered the idea of converged networks, the technology to accomplish this has only recently become available. Converged networks are easier to manage and less expensive to operate than multiple networks.

Many major networking vendors, including Cisco Systems, are designing equipment capable of supporting converged networks. This new equipment must support high-bandwidth demands and multiple interface types. Just as standard and proprietary protocols exist in the data network environment, they also exist in the voice and video network environments. Converged network equipment must be able to interface with—at a minimum—both standards-based voice and proprietary video protocols.

Example

ABC Company is running a TCP/IP-based data network. Its current voice network uses multiple PBX systems at locations throughout the United States. Its Voice over IP (VoIP) migration includes interfacing with the standards-based PBX signaling protocol, which is Q Signaling (QSIG). In addition, its VoIP migration may include transporting the Lucent Digital Crossconnect System (DCS) and DCS+ protocols.

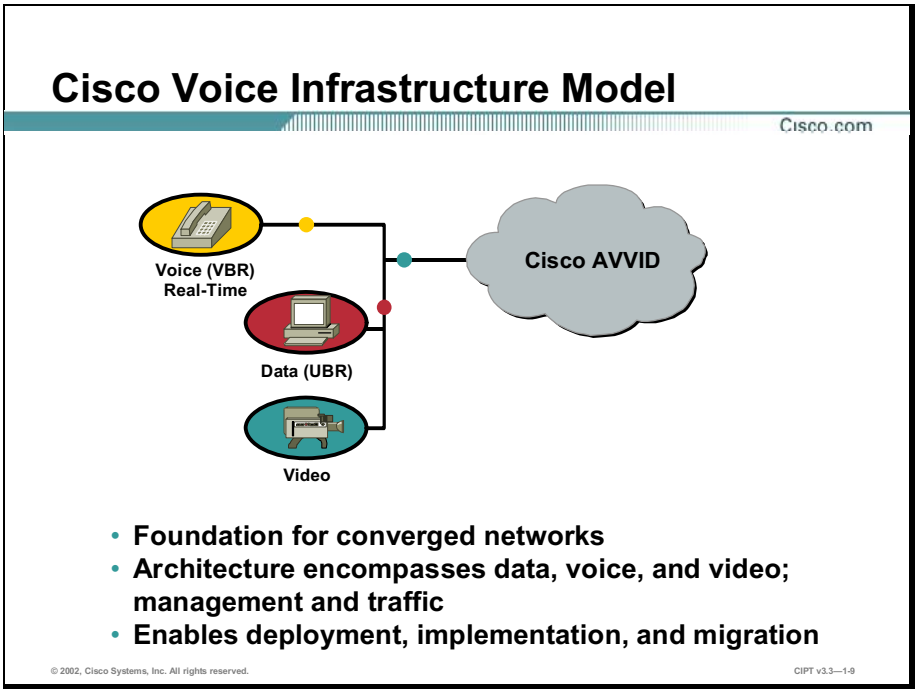


Over time, the Internet (and data-networking technology in general) has incorporated many traffic types over a massive network infrastructure. For example, you can use desktop conferencing everywhere, and the mainframe has evolved from being a separate network to a server on the IP data network. This recent convergence absorbs voice and video applications into the data network. Several large Post, Telephone, and Telegraph (PTT) carriers are using packet switching or Voice over ATM (VoATM) as their backbone technology. In addition, enterprise customers have implemented virtual trunking to avoid long-distance toll charges. Virtual trunking involves connecting disparate PBXs via a wide-area data network.

With the introduction of IP telephony technology, you can integrate previously disparate networks into a single, converged network. As a result, customers will experience a lower total cost of ownership, toll call savings, and increased productivity because of IP telephony applications.

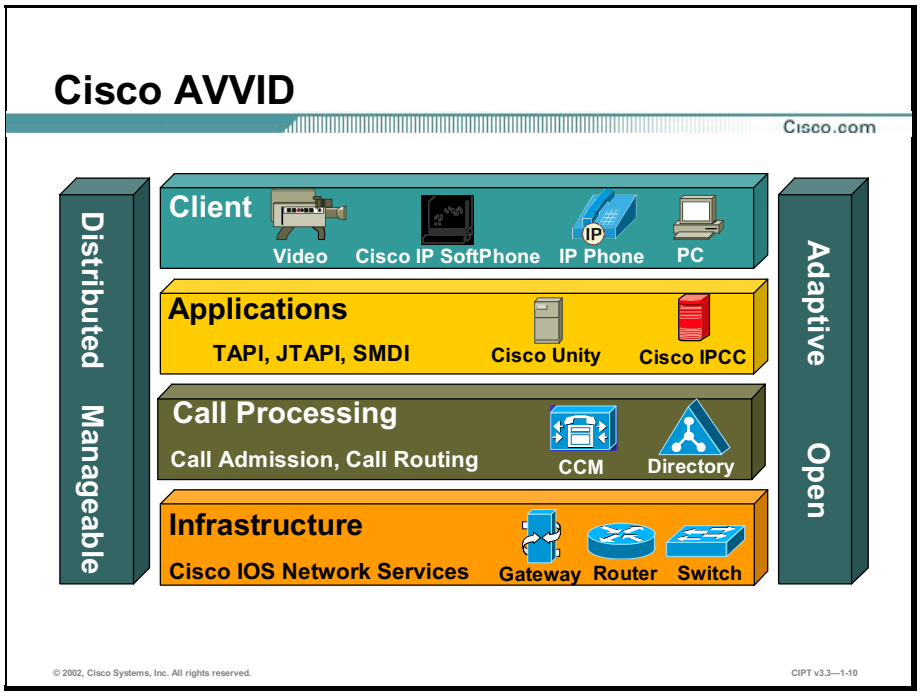
Cisco AVVID

This topic examines Cisco AVVID, the only enterprise-wide, standards-based network architecture in the industry. Cisco AVVID provides the roadmap for combining business and technology strategies into one cohesive model.



Cisco AVVID provides the foundation for converged networks by addressing the demand for converged networking equipment. As the umbrella of network management, 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. You can use the Cisco AVVID strategy to address these major areas of concern:

- **Speed:** Cisco AVVID ensures the rapid deployment of new applications.
- **Reliability:** Rather than designing small amounts of redundancy into multiple networks, you can deploy a large amount of redundancy into a single network.
- **Interoperability:** Standards-based protocols across all network classes guarantee that multiple solutions will work together.
- **Pace of change:** Cisco AVVID provides easier validation of new technologies.
- **Cost reduction:** Cisco AVVID minimizes the resource and time requirements necessary for managing multiple communication networks.



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, which is where applications that provide additional network functionality reside; and the client layer, which is where end-user devices reside. The key points about the four standard layers include:

- **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 SoftPhone, or a PC delivering converged messaging.

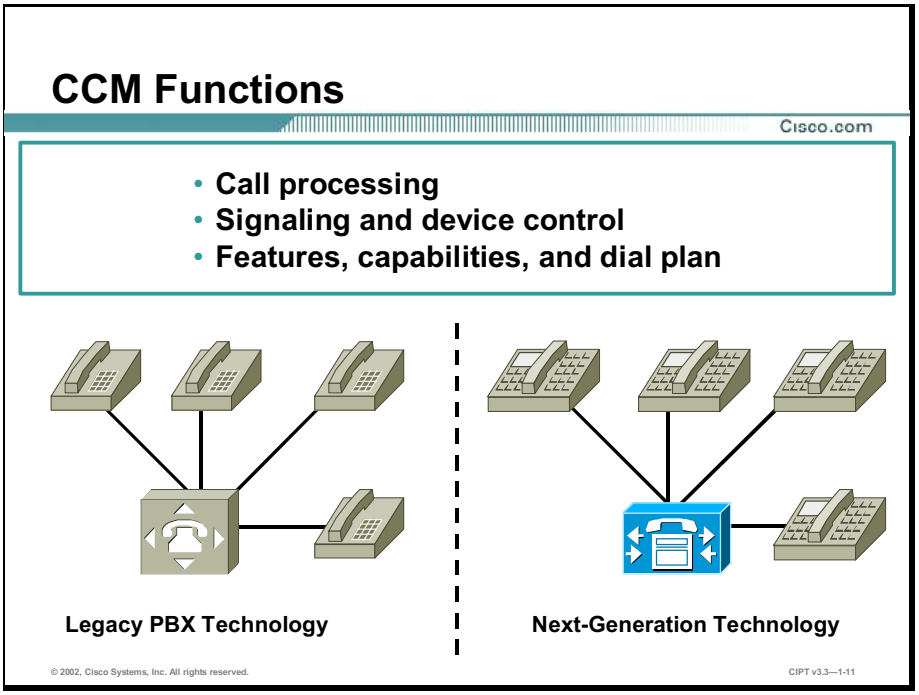
- **Applications layer:** Applications are physically independent from call-processing functions and the physical voice-processing infrastructure; that is, they may reside anywhere within the network.

- **Call-processing layer:** Call processing is physically independent from the infrastructure. Thus, a Cisco CallManager (CCM) in Chicago, Illinois, can process call control for a bearer channel in Phoenix, Arizona.

- **Infrastructure layer:** The infrastructure can support multiple client types, such as hard telephones, Cisco IP SoftPhones, and video.

CCM Functions

This topic describes the CCM functions within the Cisco IP telephony solution.

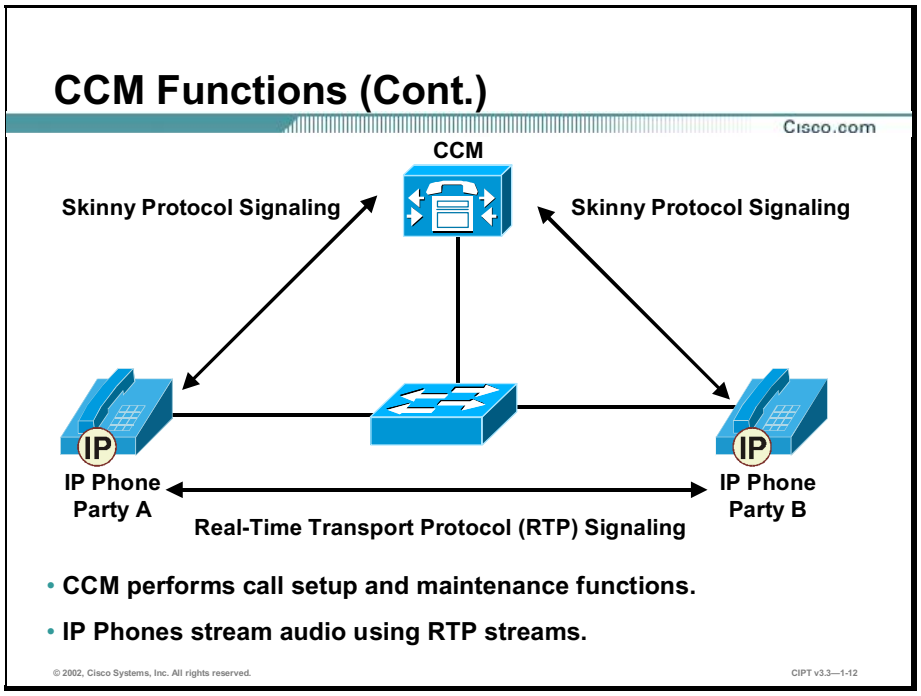


CCM extends enterprise telephony features and functions to packet telephony network devices. These network devices include IP Phones, media-processing devices, VoIP gateways, and multimedia applications. Additional data, voice, and video services, such as converged messaging, multimedia conferencing,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

Note	You can install CCM only on server platforms that are approved by Cisco.

CCM software includes a suite of integrated voice applications that perform voice conferencing and manual attendant functions. The integrated voice applications do not require special-purpose, voice-processing hardware. IP Phones and gateways use supplementary and enhanced services, such as hold, transfer, forward, conference, multiple-line appearances, automatic route selection, speed dial, and redial.

You can enhance CCM capabilities in production environments by upgrading software on the server platform, thereby avoiding expensive hardware upgrades. You can also create a virtual telephony network by distributing CCM, and all telephones, gateways, and applications, across an IP network. The benefits of this virtual telephony network include improved system availability and increased scalability. Call Admission Control (CAC) ensures that voice quality of service (QoS) is maintained across constricted WAN links. In addition, CAC diverts calls to alternate PSTN routes when WAN bandwidth is not available.



You can understand how a telephone call works by tracking an IP telephony call in its most basic form.

Example

In the figure shown here, Party A (left telephone) wants to call Party B (right telephone). Party A will pick up the set and dial the number of Party B. In this environment, dialed digits are sent to CCM, the call-processing engine. CCM finds the address and determines how to route the call.

After CCM signals the calling party over IP to initiate a ring back, Party A hears ringing. CCM also initiates ringing the set of the destination telephone.

When Party B picks up the telephone, the Real-Time Transport Protocol (RTP), or the IP media stream, begins between the two stations. Party A or Party B may now initiate a conversation.

The IP Phones require no further communication with CCM unless either Party A or Party B invoke a feature, such as call transfer or call conferencing.

This figure illustrates an IP telephony call in its most basic form. If you access an outside line to the PSTN or to a PBX system, place the call via the gateway PSTN or PBX by first dialing an access code.

You can perform nearly all administration for CCM through the Cisco CallManager Administration tool.

Reference You can find the Cisco CallManager Administration tool at: http://<*server_IP*>/ccmadmin.

Because of the URL, most administrators refer to this utility as "CCMAdmin." Cisco CallManager Administration is a series of dynamically generated web pages that allow you to configure virtually all aspects of the VoIP network. The administration interface is divided into these major menus:

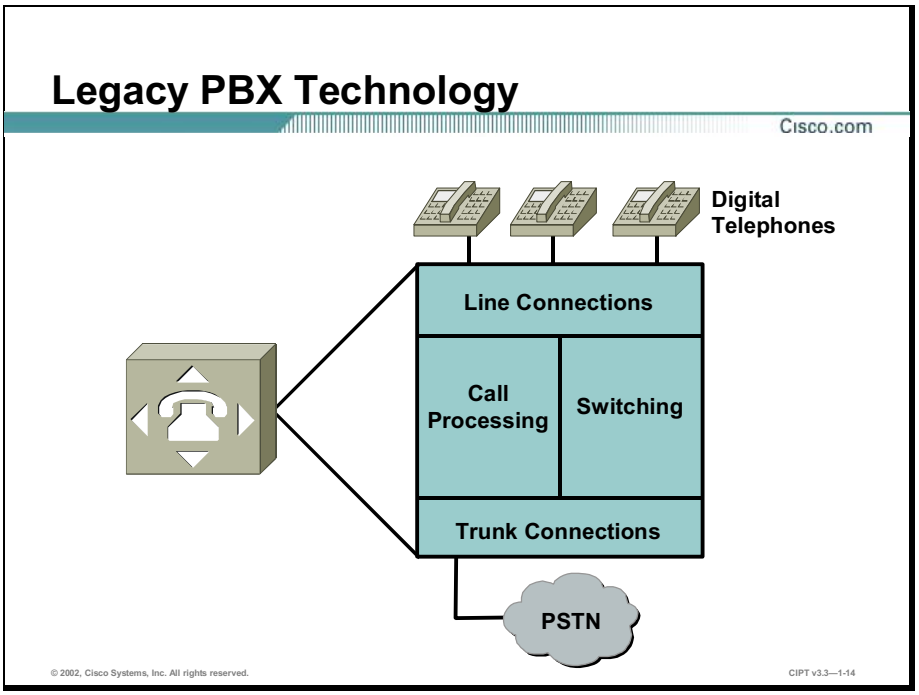
- **System:** Allows you to configure items that affect the VoIP network as a whole. For example, you can add CCM servers, or date and time zones.
- **Route Plan:** Allows you to configure routing and access control for the voice network.
- **Service:** Allows you to add additional applications or services, such as Music On Hold (MOH), to the voice network. These services are typically administrative in nature.
- **Feature:** Allows you to add telephone system features, such as call park or voice mail, to the voice network. In general, these services relate to the end user.
- **Device:** Allows you to configure VoIP hardware devices, such as gateways or IP Phones.
- **User:** Allows you to manage the Lightweight Directory Access Protocol (LDAP) user database that stores voice network information.

- **Application:** Allows you to install and manage other external applications that integrate with CCM, such as the Bulk Administration Tool (BAT) or Cisco CallManager Serviceability.

- **Help:** Allows you to find online help for CCM and other installed components.

Comparing Legacy and IP Telephony Technology

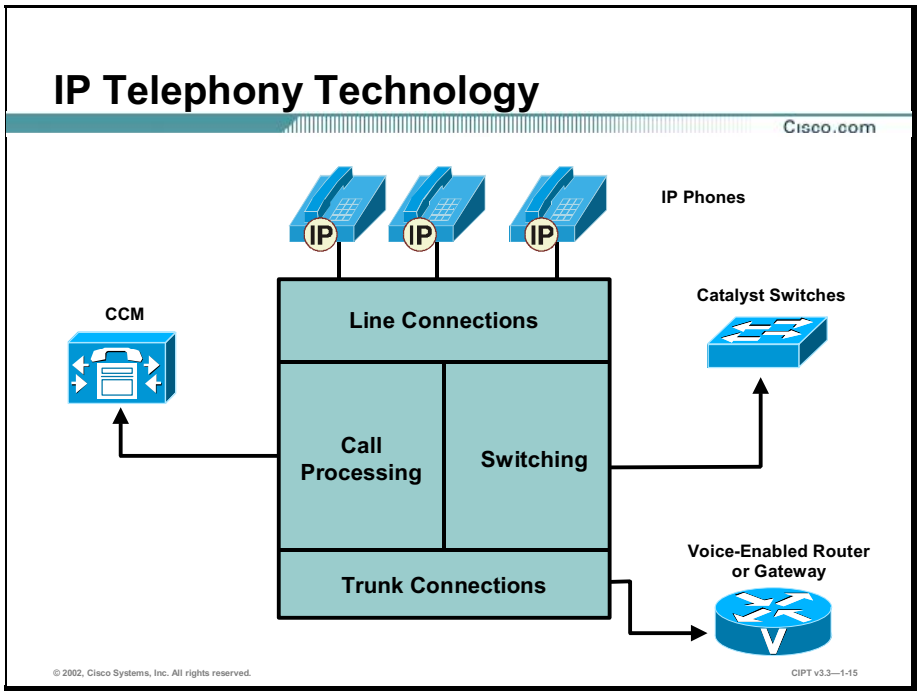
This topic describes the advantages and benefits of using IP telephony network designs.



PBX systems power the majority of voice networks around the world and enable businesses to operate and manage their own telephone systems. Depending on the size of the company, using PBX systems can save a tremendous amount of money when compared to paying an outside service provider to manage the telephone network.

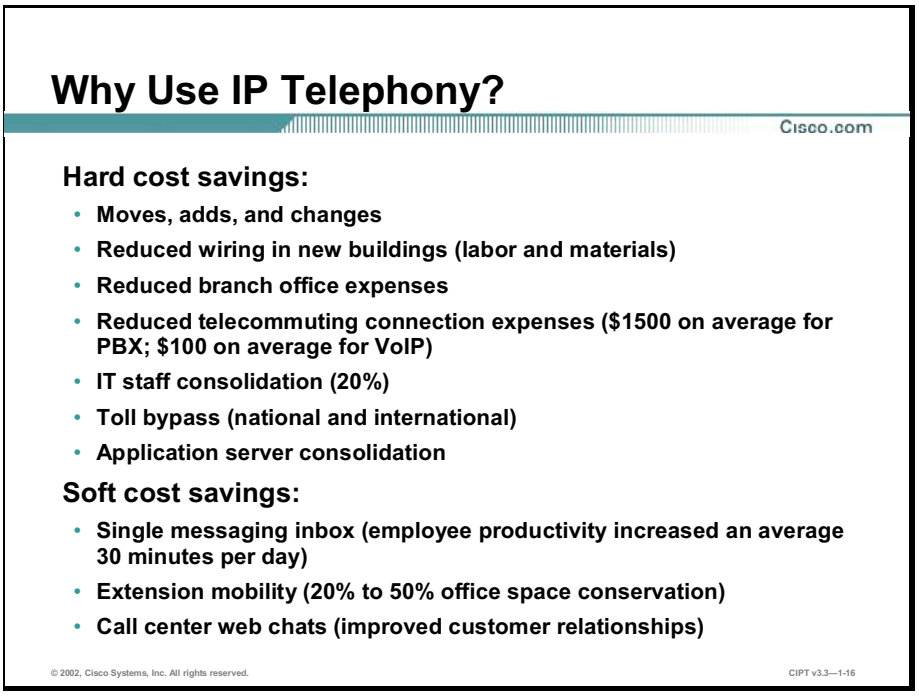
Individual PBX system components can be extremely complex and may require special training to manage. From a broader perspective, all PBX systems can be broken down into four major components:

- **Line connections:** Line connections are feature cards that are installed into a PBX system to provide ports that connect end-user telephones. These ports provide a dial tone for the end device.
- **Call processing:** This component is the PBX engine. It provides the call-routing table, device recognition, and telephone features.
- **Switching:** This component is the backbone of the PBX. It provides the circuit between the devices that are communicating across the PBX system.
- **Trunk connections:** Trunk connections are feature cards that are installed into a PBX system to provide trunks to other PBX systems or to the PSTN.



When designing a Cisco VoIP network, you can replace the PBX functionality with network equipment. Rather than having a single, centralized PBX system, you can distribute these functions to network equipment in a decentralized design. This distribution allows for easier management and cabling. In addition, this design eliminates a single-server point of failure.

Because the call-processing portions of the telephone system now run on standardized application servers, you can easily introduce new functionality or features into a network by installing various applications. For example, to add voice mail to a network, you can install a Cisco Unity server. Alternatively, if you want to create a receptionist console, you can install the CCM Attendant Console on a client PC.



Although IP telephony networks offer many new functions and features, business management is typically concerned with the overall cost of the solution. Because the initial deployment of a VoIP network has significant associated costs, you must be able to answer this question: How will these initial expenses save money in the end?

You can divide the return on investment (ROI) into hard cost savings and soft cost savings. Examples of hard cost savings include:

- In legacy voice networks, moving a telephone between locations can cost $75 to $125 on average. With IP telephony networks, you can eliminate most of this cost.
- Rather than running dual cabling (voice and data) to every user location, only one cable set is necessary.
- You do not need separate voice network administrators or maintenance contracts for corporate and branch offices.
- You can reduce costs associated with employee telecommuting.
- You can eliminate all toll charges between corporate locations.
- You can deploy multiple IP telephony network features on a single server, thus consolidating the number of servers needed.

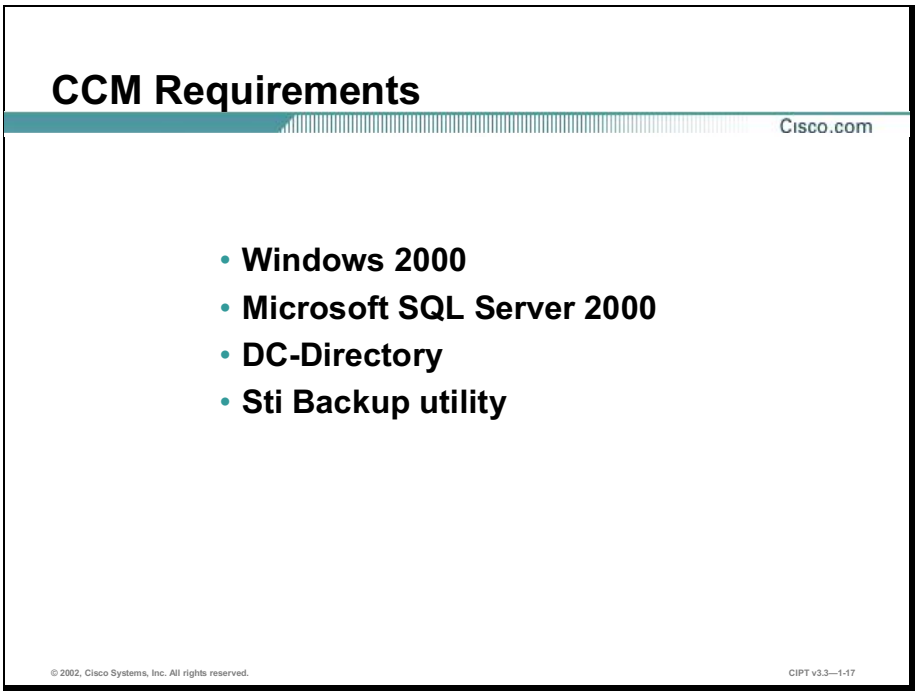
Examples of soft cost savings include:

- With Cisco Unity, you can deploy a single inbox for all message types. This deployment saves employees a significant amount of time.

- Rather than having dedicated office space for mobile employees, you can use extension mobility features to allow employees to work from any telephone in the network.
- You can deploy voice communication over a company Internet website, thus improving customer relationships.
- You can reduce integration costs because Cisco IP telephony network hardware and applications are open-source designed.

CCM Operating System, Database, and Supporting Applications

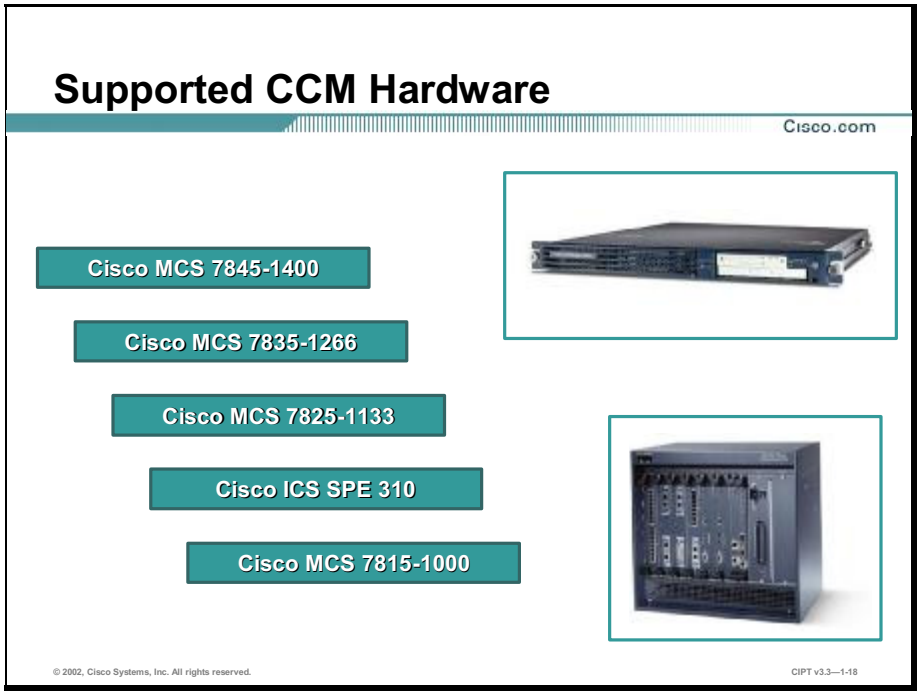
This topic describes the requirements for installing a CCM server.



The CCM server relies on Windows 2000 for its operating system and the Microsoft Structured Query Language (SQL) Server 2000 for its database. You can use the Data Connection Directory (DC-Directory) for an LDAP directory of end users if no other LDAP directory structure (such as Active Directory) is available. You can use the Spirian Technologies, Inc. (Sti) Backup utility for backing up and restoring the CCM database.

Supported CCM Hardware

This topic describes the hardware requirements for CCM.



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

All of these servers (except the Cisco MCS 7815-1000) 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.

Reference You can order these servers directly from Compaq or IBM. For more information, refer to: http://www.cisco.com/warp/public/779/largeent/avvid/products/infrastructure.html.

Cisco ICS SPE 310 Specifications

Cisco.com

Performance:

- Pentium III 700-MHz CPU
- 512-MB DRAM
- Supports 200 to 500 IP Phones per server

Components:

- Single 20.4-GB hard drive
- Two USB ports

The system processing engine (SPE) 310 is a server blade in the larger Cisco Integrated Communications System (ICS) 7750. Cisco designed the Cisco Integrated Communications System 7750 as an all-in-one system, similar to a PBX, for smaller IP telephony deployments or branch office solutions. Although you can customize the Cisco Integrated Communications System chassis, it typically contains one or more of these components:

- **System switch processor (SSP):** Provides a switched backplane for all installed modules and two external switch ports for uplink connections to additional switches.
- **System alarm processor (SAP):** Monitors the Cisco Integrated Communications System chassis and all installed modules for possible problems and sends alerts if necessary.
- **System processing engine (SPE):** Provides a complete hardware platform for CCM or other voice applications.
- **Multiservice route processor (MRP):** Provides Cisco Integrated Communications System chassis routing components and is capable of housing up to two WAN interface cards (WICs), voice interface cards (VICs), or voice WAN interface cards (VWICs) per blade.

Caution Cisco has designed specific voice software for the Cisco Integrated Communications System SPE 310. If you install retail versions of CCM or Cisco Unity on this server, unpredictable results may occur.

Cisco MCS 7815-1000

Cisco.com

Performance:

- Pentium III Celeron 1000-MHz CPU
- 512-MB DRAM
- Supports up to 200 IP Phones per server

Components:

- Single 20.4-GB hard drive
- 48x CD-ROM
- Two USB ports

CIPT v3.3—1-20

Cisco designed the Cisco MCS 7815-1000 to provide a cost-effective solution for locations with up to 200 lines installed. These locations can be standalone enterprises or branch locations.

Note	Because the Cisco MCS 7815-1000 server fits into smaller locations that may not have a dedicated information technology room, it is the only tower-encased server. Rack-mount kits are available for these servers; you can purchase them separately from Cisco.

Cisco MCS 7825-1133

Cisco.com

Performance:

- Pentium III 1133-MHz CPU
- 1024-MB SDRAM
- Supports up to 1000 IP Phones per server

Components:

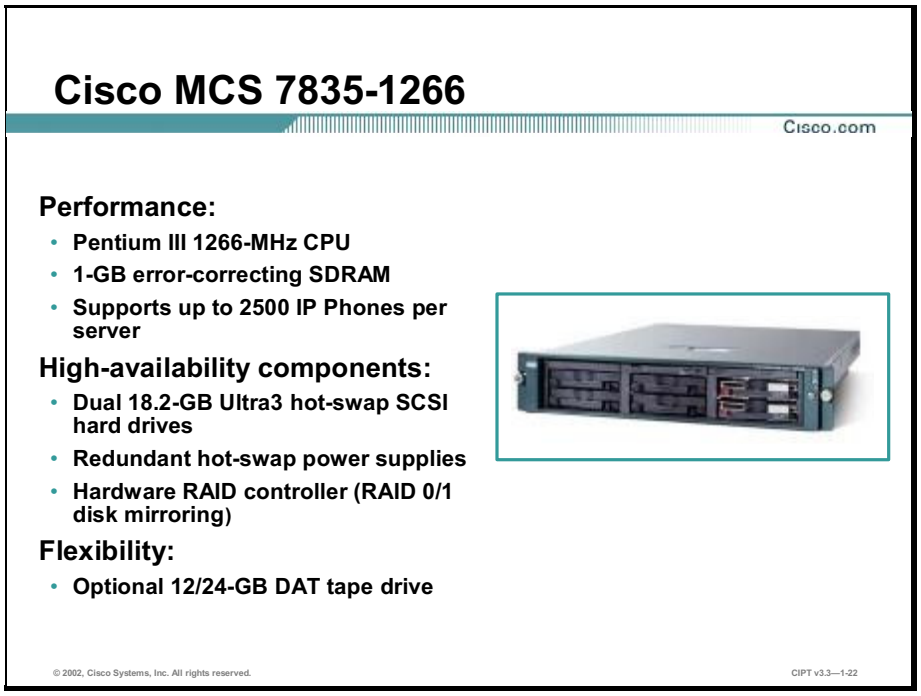
- Single 40-GB 7200 RPM hard drive
- Dual Fast Ethernet embedded NICs

Features:

- 1-RU rack-mount chassis (up to 42 servers per rack)
- Up to six servers may be stacked on a desk

The Cisco MCS 7825-1133 is a powerful platform for small- to midsize business environments. At one rack unit (RU) high, the Cisco MCS 7825-1133 is the most space-efficient member of the Cisco MCS series. These servers operate best in a cluster because they do not have either a built-in hard drive or power supply redundancy.

Although the Cisco MCS 7825-1133 servers are capable of scaling up to 1000 IP Phones, you will typically find them in environments that distribute between 500 to 800 IP Phones per server. To reduce the total number of IP Phones supported, administrators can run voice application software in addition to CCM.



The Cisco MCS 7835-1266 is a high-availability server platform. At three RU high, the server fits into a relatively low profile chassis that minimizes rack space. Cisco recommends this server for mid- to large-size businesses. However, many businesses of all sizes are using this server because of its significant redundancy.

You can replace a faulty hard drive while the server is still operating because the server hard drives and power supplies are hot-swappable. After the faulty hard drive is replaced, you can re-create the mirror between the hard drives (usually during off hours) and return to full capacity by the next day.

Cisco MCS 7845-1400

Cisco.com

Performance:

- Dual Pentium III 1400-MHz CPUs
- 2048-MB SDRAM
- Supports up to 7500 IP Phones per server

Components:

- Four 72-GB 10,000 RPM hard drives
- Dual Fast Ethernet embedded NICs
- Redundant hot-swap power supplies

Features:

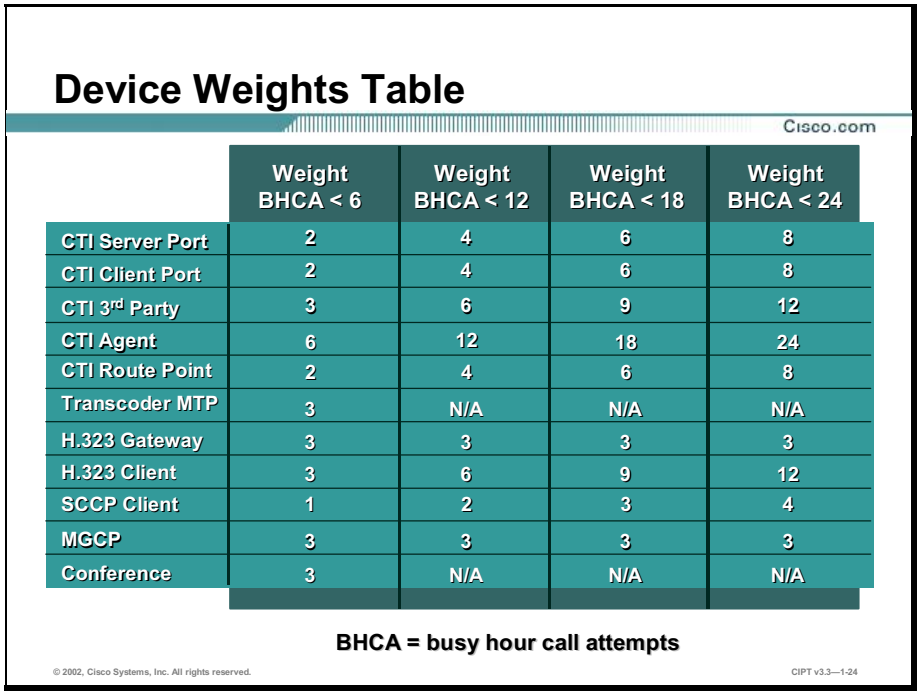
- 2-RU rack-mount chassis

The Cisco MCS 7845-1400 is currently the most powerful server platform in the Cisco MCS family. Cisco created this platform to handle massive voice application processing tasks and take advantage of the new CCM 3.3 features (such as increased cluster size). Overall, this platform satisfies the enterprise voice network requirements for most businesses.

With four 72-GB hard drives, you can create the Redundant Array of Independent Disks (RAID) needed. The RAID controller hardware, which is included, supports dual, mirrored partitions (RAID 1). This feature creates a single 72-GB partition for the CCM operation and a second 72-GB partition for trace files. Trace files allow you to log detailed CCM operations on a day-to-day basis for troubleshooting purposes.

Device Weight Units

This topic examines the number of device weight units that a hardware platform can support.



The table shown here lists the types of devices that can register to CCM. Each device that registers to CCM uses the resources (CPU cycles) of the CCM server.

Busy hour call attempts (BHCA) is the number of call attempts made during the busiest hour of the day. To audit the network appropriately, you must first determine the busiest hour of the day and then scale the type of devices that are going to be deployed within the Cisco IP telephony solution.

Example

Using the data supplied in the table shown here, a Skinny Client Control Protocol client with a BHCA of less than six is weighted at one; an H.323 gateway with a BHCA of less than six is weighted at three. In a CCM cluster, a variety of devices besides Cisco IP Phones will register. In these situations, you would experience a delayed dial tone if the device weight units were oversubscribed on a server.

CCM Server Platforms: Device Weights

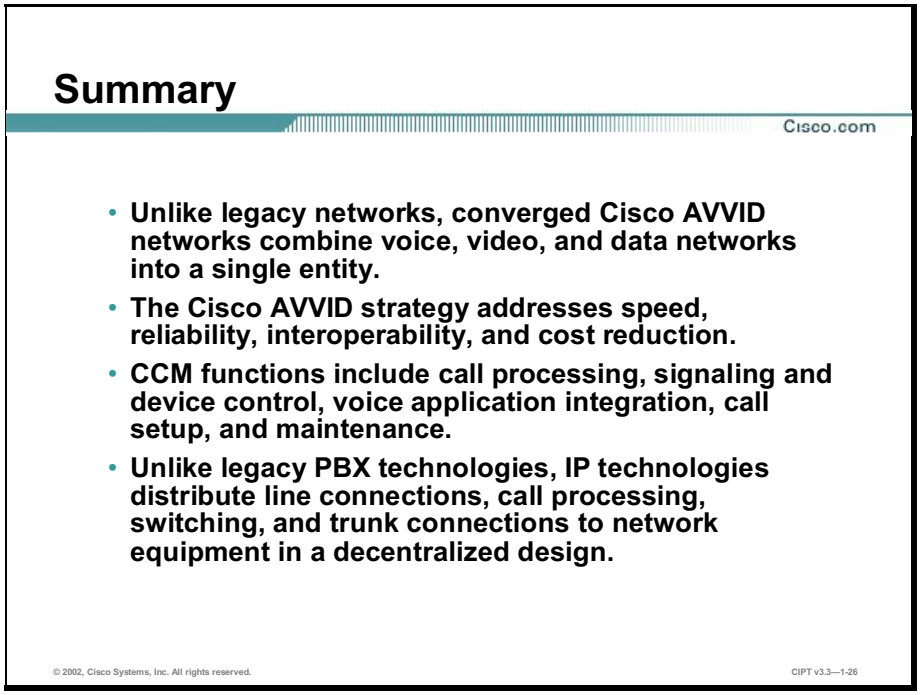
Cisco.com

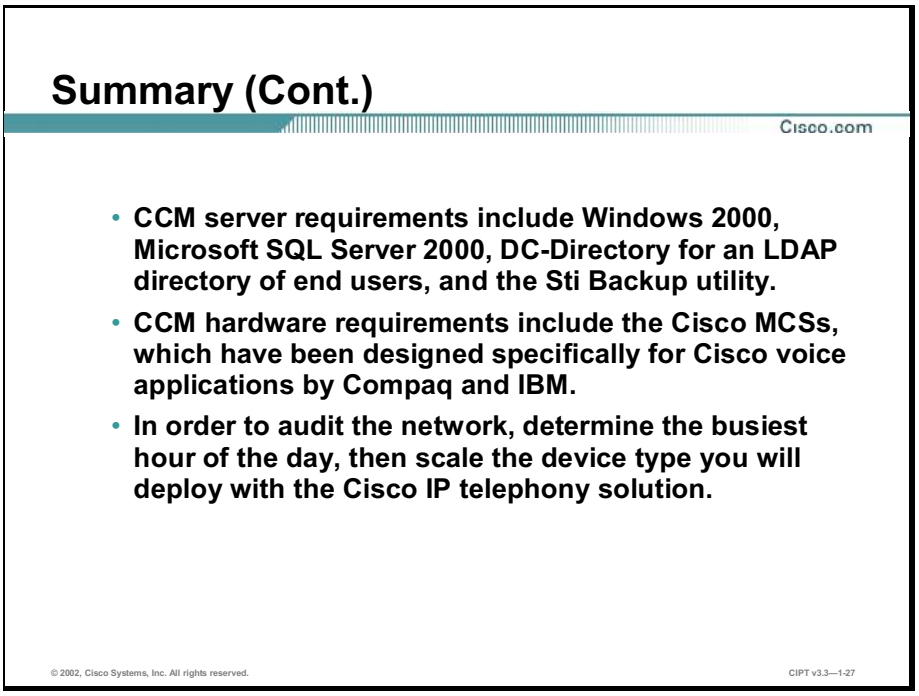
Platform	Device Units per Server	Maximum IP Phones per Server
MCS 7845-1400 (Dual)	10,000	7500
MCS 7835 All Models	5000	2500
Compaq DL 380	5000	2500
IBM xSeries 342	5000	2500
MCS 7825	2000	1000
SPE 310	2000	1000
Compaq DL 320	2000	1000
IBM xSeries 330	2000	1000
MCS 7815-1000	400	200

The table in this figure details the Cisco MCS platform capabilities of Cisco IP Phones and device weight units. You can easily calculate the number of Cisco IP Phones that are registered to a Cisco MCS platform. However, to account for all of the devices that are going to register to a Cisco MCS platform, you can use the device weight units from the previous table and compare them to the maximum number of device weight units supported by the Cisco MCS platform indicated.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Cisco CallManager Cluster and Deployment Options lesson

References

For additional information, refer to these resources:

- CCM documentation: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm, 25 November 2002.
- Cisco CallManager Administration tool: http://<*server IP*>/ccmadmin.
- Cisco MCSs: http://www.cisco.com/warp/public/779/largeent/avvid/products/infrastructure.html, 25 November 2002.

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) What is the maximum number of Cisco IP Phones that can be added to a Cisco MCS 7835-1266 if 3000 device weight units are already registered, and BHCA is less than six?

A) 1000

B) 1500

C) 2000

D) 2500

Q2) Which of these functions is NOT a function of CCM?

A) call processing

B) signaling control

C) device control

D) dial plan

E) voice messaging

Q3) Where would you expect to find configuration options relating to CCM redundancy for IP Phones?

A) system menu

B) service menu

C) feature menu

D) device menu

Q4) What type of Cisco MCS should you purchase for a small IP telephony deployment in an office that has no dedicated information technology room?

A) Cisco MCS 7815

B) Cisco MCS 7825

C) Cisco MCS 7835

D) Cisco MCS 7845

Q5) CCM uses which of these operating systems?

A) Linux

B) Windows 95

C) Windows NT

D) Windows 2000

Q6) Which of these options is a cost-saving benefit of Cisco VoIP?

A) toll bypass

B) integrated website VoIP

C) a single message inbox for all message types

D) all of the above

Q7) What layer of Cisco AVVID contains CCM?

A) client

B) applications

C) call-processing

D) infrastructure

Cisco CallManager Cluster and Deployment Options

Overview

Cisco CallManager (CCM) works in a clustered environment that relies on the Microsoft Structured Query Language (SQL) Server 2000 database. The CCM cluster is structured around the relationship between the publisher database server and the subscriber database server. This lesson will teach you about the CCM cluster and deployment options. You will learn about the communication between the servers in a cluster and the limitations of a cluster.

Importance

This lesson benefits learners who want to increase their understanding of the relationship between CCMs in a cluster. This lesson also provides information about designing and implementing an effective CCM cluster, which will provide call-processing functions to IP Phones and a redundant CCM solution.

Objectives

Upon completing this lesson, you will be able to:

- Define cluster communication
- Define intracluster communication
- Describe available clustering options
- Identify and describe supported deployment models
- List the benefits of a single-site deployment model
- List the benefits of a centralized call-processing deployment model
- List the benefits of a distributed multicluster call-processing deployment model
- List the benefits of a distributed single-cluster call-processing deployment model

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Windows 2000 navigation experience
- General knowledge of CCM

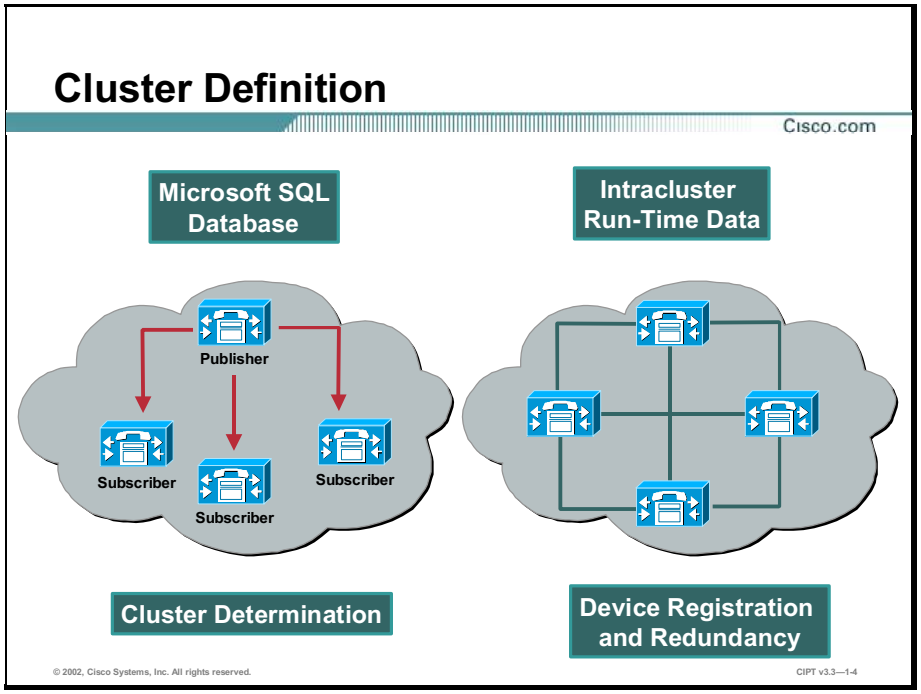
Outline

This lesson includes these topics:

- Overview
- Cluster Definition
- Intracluster Communication
- Clustering Options
- IP Telephony Deployment Models
- Single-Site Deployment
- Centralized Call-Processing Deployment
- Distributed Multicluster Call Processing
- Distributed Single-Cluster Call Processing
- Summary
- Lesson Review

Cluster Definition

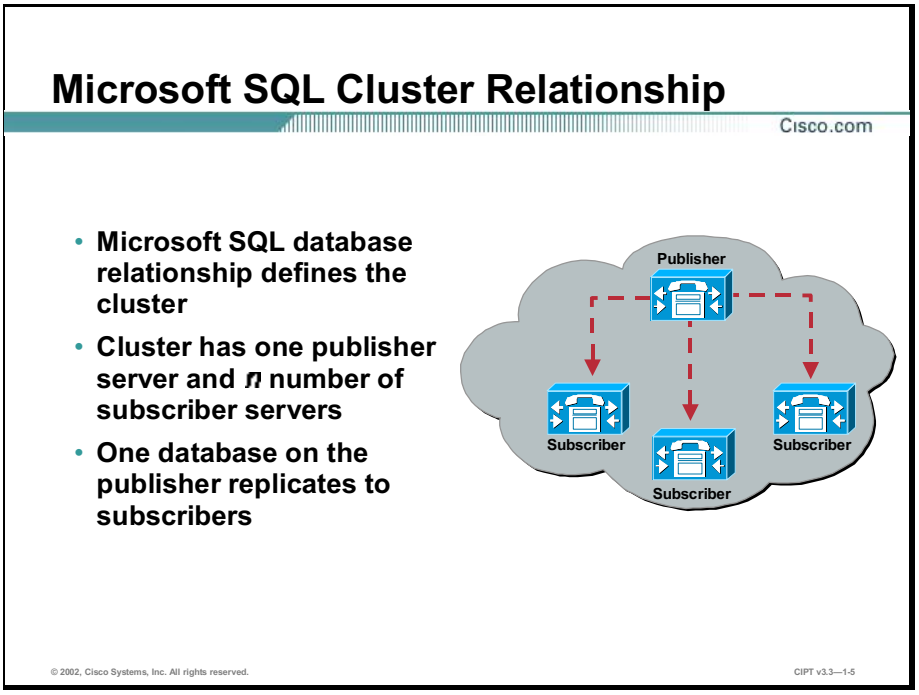
This topic defines a Cisco CallManager (CCM) cluster and the types of communication that occur in a cluster.



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 to IP telephony service, you must cluster CCM servers. A CCM cluster is two or more servers that share the same database and work together to support a common group of IP telephony devices. A CCM cluster eliminates a single-server point of failure and allows multiple devices to work together in one call-processing entity.

When you install CCM into a cluster, CCM communicates with all of the other servers assigned to that cluster. Two types of cluster communication occur: Microsoft Structured Query Language (SQL) Server 2000 database replication and intracluster run-time data. The Microsoft SQL Server 2000 database contains the device registration, configuration, and log file data. The run-time data replication tracks telephone and gateway registration, device failover, and digital signal processor (DSP) resources.

In CCM Release 3.3, a cluster is capable of handling approximately 36,000 IP Phones. (A cluster may support fewer telephones, depending on the additional tasks that CCM performs.) 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.



The primary purpose of a CCM cluster is to replicate the Microsoft SQL Server 2000 database. The Microsoft SQL Server 2000 database contains the entire configuration of the IP telephony network. A CCM cluster provides redundancy for the Microsoft SQL Server 2000 database. You must have at least two CCM 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.

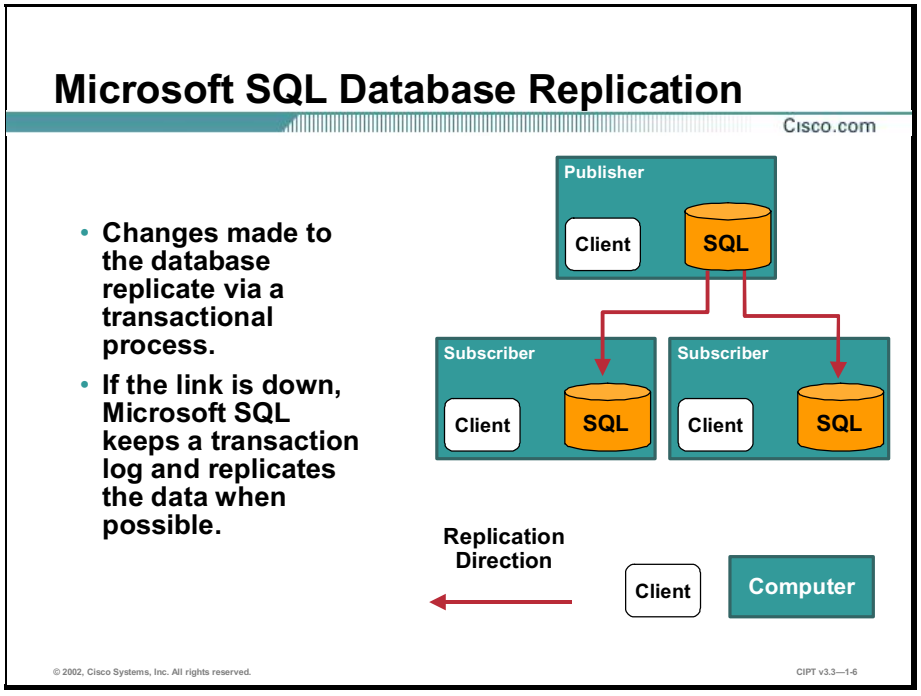
After you make all changes to the database on the publisher server, the publisher replicates these changes to the subscriber servers. When the publisher server is off line, the Microsoft SQL Server 2000 database automatically locks, thus preventing further database changes. The IP telephony network will continue to operate, but you will not be able to add or configure any CCM-managed devices.

Example

An administrator installs a Cisco IP telephony solution and must add a telephone to the database. To add the telephone, the administrator uses the web-based interface of the Cisco CallManager Administration tool. After the CCM server writes the information into the Microsoft SQL Server 2000 database on the publisher, the publisher replicates the database to the subscriber servers in the cluster.

Intracluster Communication

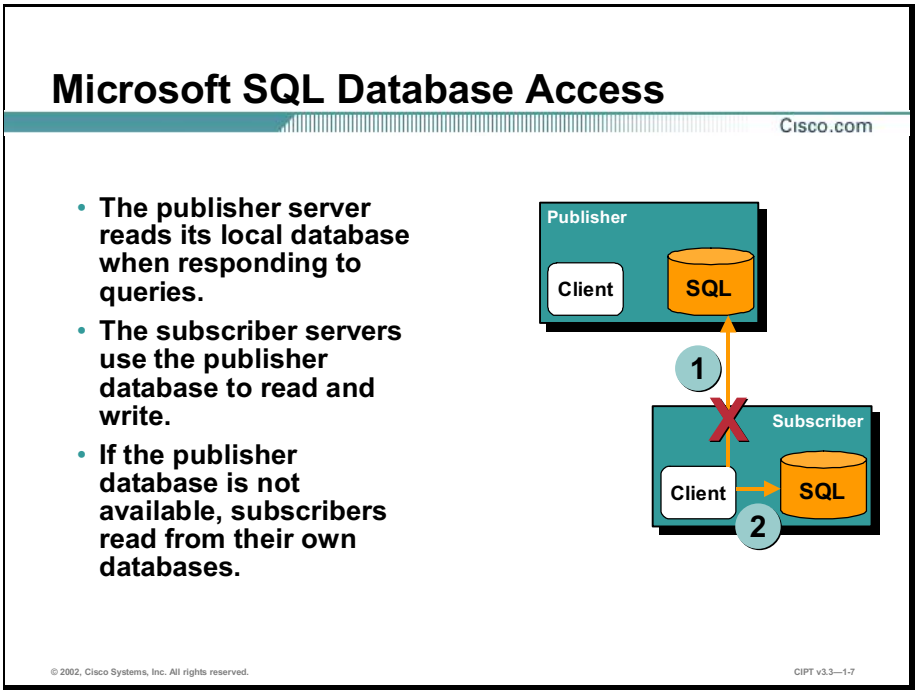
This topic examines the two types of intracluster communication.



This figure illustrates the first type of intracluster communication: Microsoft SQL Server 2000 database replication. The Microsoft SQL Server 2000 writes database information in the publisher database only. The Microsoft SQL Server 2000 writes all of the entries made through the CCM web interface on a subscriber server in the publisher database. You will still be able to access the Cisco CallManager Administration web interface if the publisher server is down because the Cisco CallManager Administration utility continues to run using the Internet Information Server (IIS) on all CCM servers. However, any attempt to write to the database when the publisher server is down returns an error message.

The replication of the database within a CCM cluster is unidirectional and works in the following way:

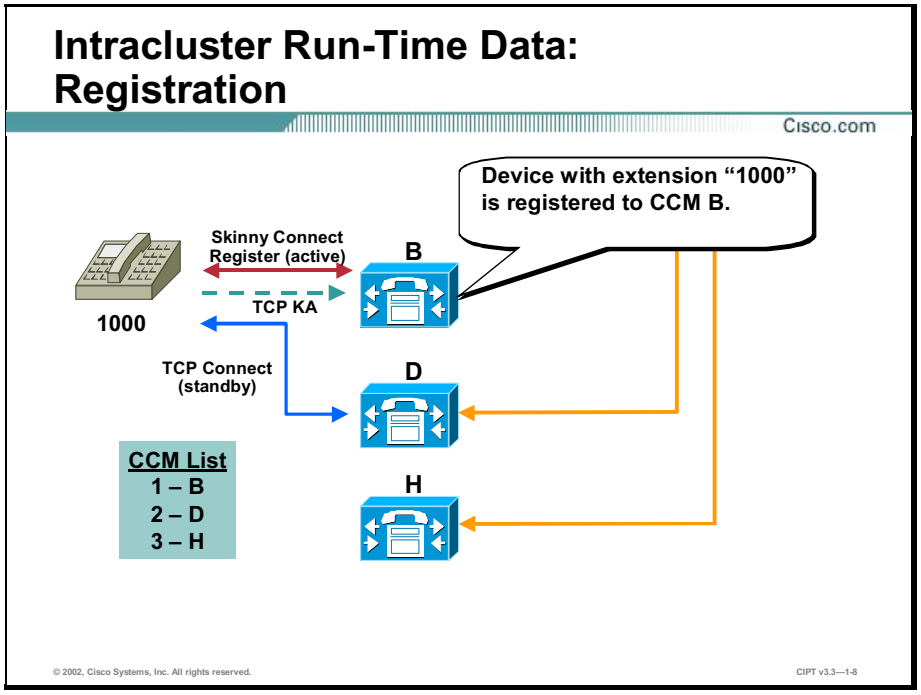
- Changes made to the publisher database replicate via a transactional process. The changes occur immediately, unless the link is down.
- The Microsoft SQL Server 2000 denies all data entry to the publisher database if the link to the publisher, or the publisher itself, is down. The replication of Call Detail Records (CDRs) is the one exception to this rule. Microsoft SQL Server 2000 database writes CDRs to the subscriber database where they are temporarily stored. The CDRs are replicated to the publisher when connectivity is restored.
- The publisher database is writable; the subscriber database is read-only.



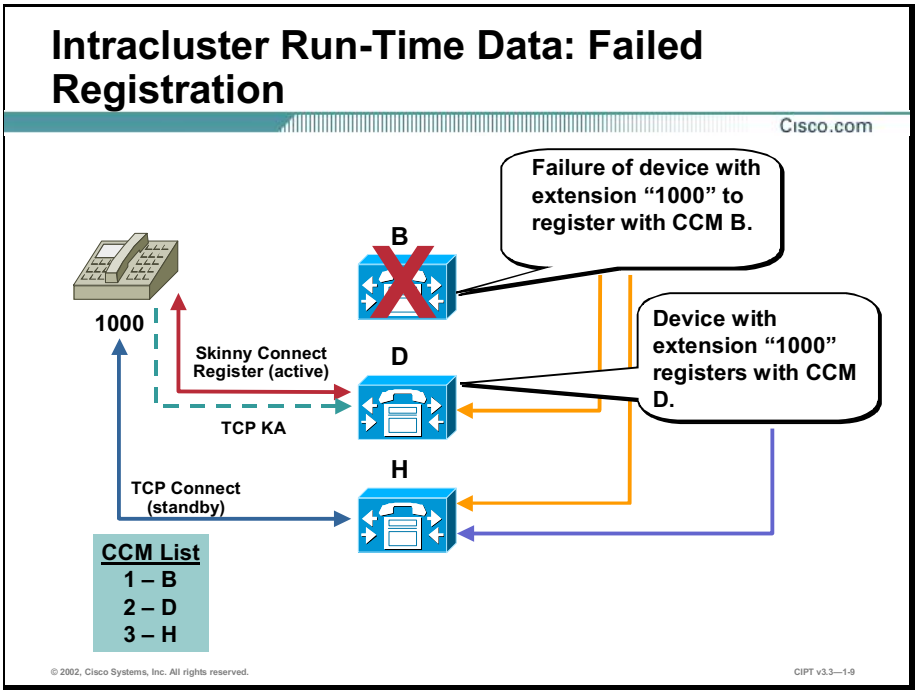
During normal operation, all of the CCMs in a cluster read data from and write data to the publisher database. Periodically, the backup copies of the database are updated automatically from the publisher. If the publisher database becomes unavailable for any reason, the various CCMs in the cluster continue to operate from their local backup copies of the database. When the publisher database is restored, normal operations resume.

The CCM publisher and subscriber databases communicate within a cluster in the following way:

- The publisher reads its local database for information.
- The subscriber uses the publisher database to retrieve information.
- In the event of a failure, the subscriber reads its local copy of the database for information.



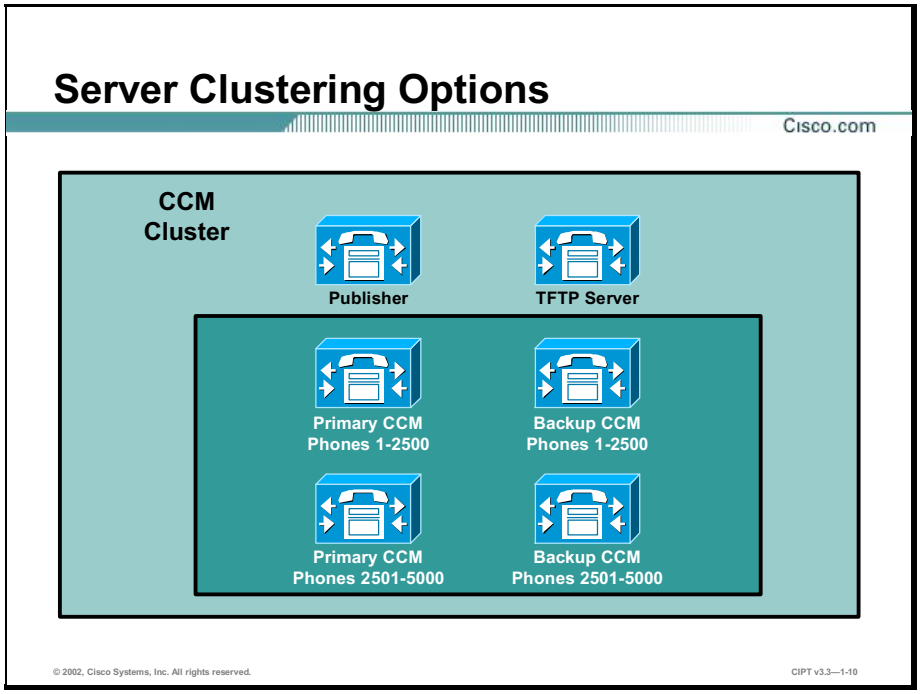
CCM run-time data is the second type of intracluster communication. When a device (such as a Cisco IP Phone) registers with a CCM cluster, the CCM server informs all of the other CCM servers in the cluster, as this figure shows. After the device registers with the primary CCM server, the device sends the server a TCP keepalive message every 30 seconds and sends a TCP connect message to the secondary CCM server.



When the Cisco IP Phone detects the failure of its TCP keepalive message with the primary CCM server, the device attempts to register with its secondary CCM server. The secondary CCM server accepts the registration from the device and announces the new registration (through intracluster run-time communication) to all of the CCM servers in the cluster. The device initiates a TCP keepalive message to the secondary CCM server (the new primary of the device) and a TCP connect message to a tertiary CCM server (the new secondary of the device).

Clustering Options

This topic examines the available options for deploying a CCM cluster.



Creating a well-designed CCM cluster is a critical element when you initially deploy the IP telephony network.

A CCM cluster is a group of CCM servers that support designated Cisco IP Phones and gateways. The CCM cluster also contains a complex database replication and management structure that is designed to create redundancy and load balancing in the voice network. Because of the database replication and management structure, you must plan and design the cluster solution thoroughly *before* deployment.

The CCM cluster identifies CCMs that have a copy of the Microsoft SQL Server 2000 database, and the amount of redundancy for the voice network. When designing a CCM cluster, you must consider that CCM Release 3.3 maintains a maximum of nine CCM servers supporting the Microsoft SQL Server 2000 database: one Microsoft SQL publisher server and up to eight Microsoft SQL subscriber servers. These CCM database servers are responsible for IP Phone registration and call processing. The number and type of CCM database servers that are installed into a cluster directly affect the number of telephones that the cluster is able to support. Because the Microsoft SQL publisher server is responsible for managing the only writable copy of the Microsoft SQL Server 2000 database, it does not typically participate in managing the call-processing aspects of the network (unless the network is relatively small and contains less than 1000 IP Phones). The Microsoft SQL subscriber servers support the IP Phones and gateways.

The type of Cisco Media Convergence Server (MCS) that you choose for the Microsoft SQL subscriber servers determines the number of devices that the cluster can support. For example,

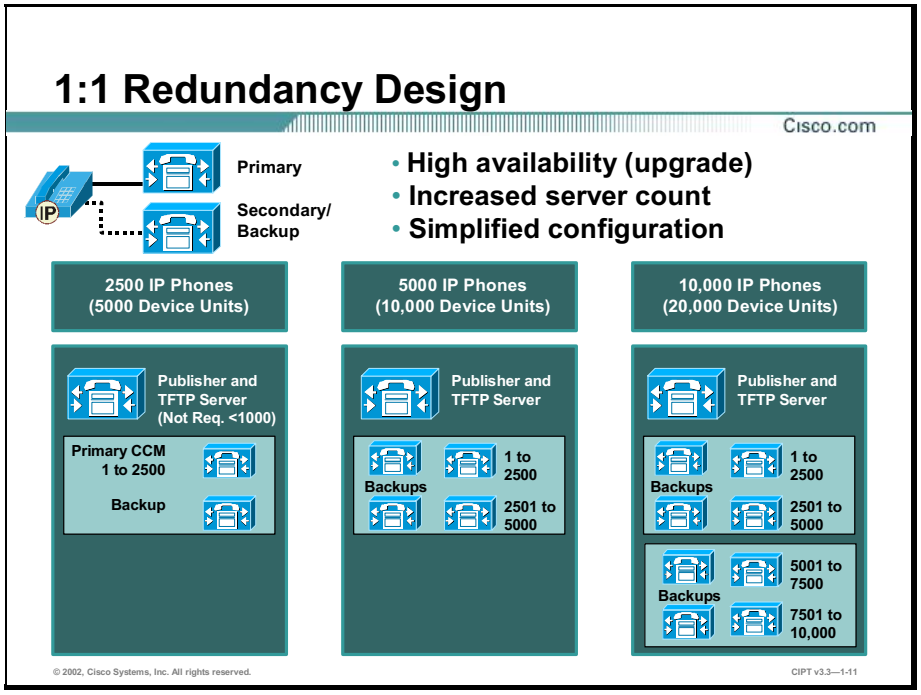
using an entry-level Cisco MCS 7815 in the cluster limits the maximum number of IP Phones to 200 per server. You can significantly increase this capacity by upgrading to a Cisco MCS 7835 or Cisco MCS 7845.

The second major design consideration is redundancy. Cisco IP Phones support triple call-processing redundancy, which means that a Cisco IP Phone can be configured with a primary, secondary, and tertiary CCM server. If the primary server fails, the telephone immediately attempts to connect to the secondary server; if the secondary server also fails, the telephone attempts to contact the tertiary server. The number of redundant servers in the network also directly affects the maximum cluster size. A dedicated backup server exists for each primary server in a 1:1 redundancy design.

This design guarantees that 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. Instead, you may choose to deploy 2:1 redundancy. This design allocates a single backup server for every two primary servers and can support additional IP Phones. It is possible, however, to overwhelm the backup server if multiple primary servers fail.

Finally, 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 CCM servers, or you can deploy the TFTP functionality on a separate, stand-alone 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 considerable network and processor load.

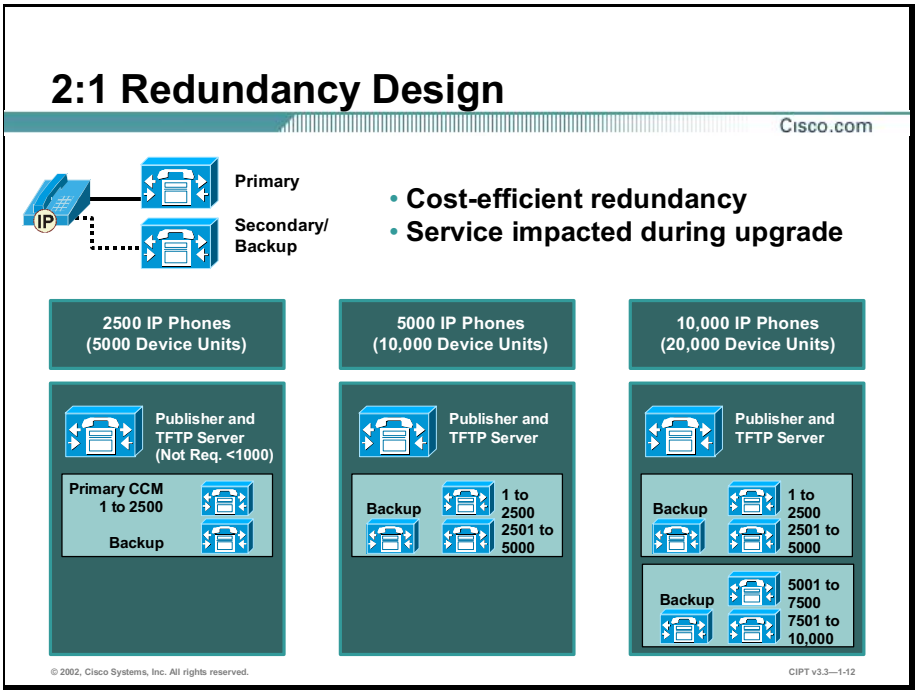
Reference The maximum number of IP Phones that each server or CCM cluster supports can change significantly, depending on the other processes that are running on each Cisco MCS and the version of CCM that you are using. For more information on server and cluster capabilities, visit:
http://www.cisco.com.



In a 1:1 CCM redundancy deployment design, you can have a dedicated backup server for each primary server. This design offers you the benefit of increased redundancy: you will not overwhelm the backup servers if more than one of the primary servers fails.

In this example, a Cisco MCS 7835 is used because each CCM server supports a maximum of 2500 IP Phones. A single CCM 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 (less than 1000 IP Phones).

When you increase the number of IP Phones, you must increase the number of CCM servers 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.

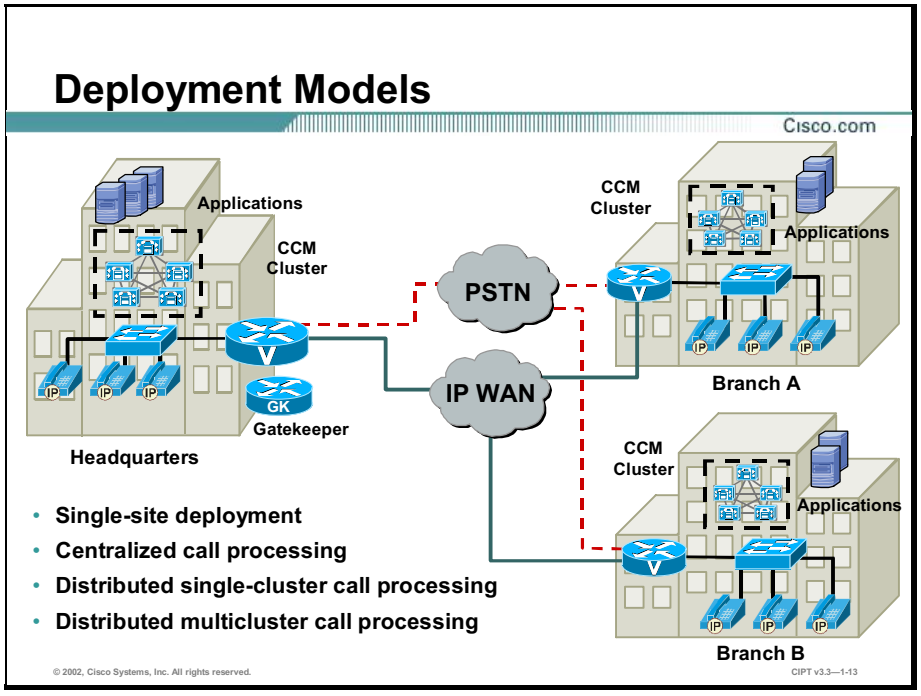


In a 2:1 CCM redundancy deployment design, you have a dedicated backup server for every two primary servers. While this design offers some redundancy, there is the risk of overwhelming the backup server if multiple primary servers fail. In addition, upgrading the CCM servers can cause a temporary loss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

IP Telephony Deployment Models

This topic lists and briefly describes the deployment models that Cisco IP telephony supports.

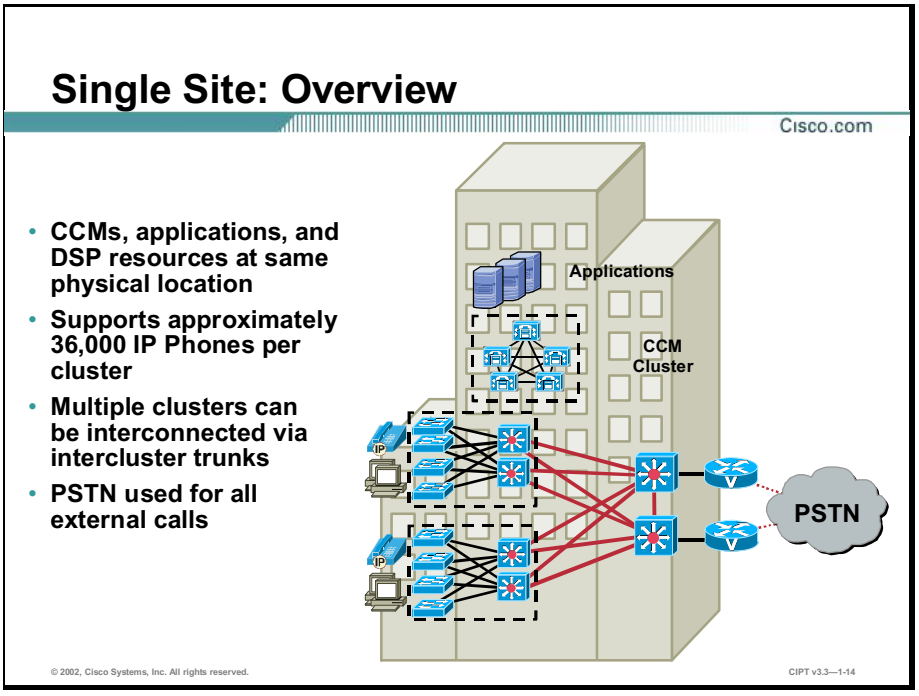


This figure illustrates the types of deployment models that Cisco Systems supports. Cisco IP telephony supports these deployment models:

- Single site
- Centralized call processing
- Distributed single-cluster call processing
- Distributed multicluster call processing

Single-Site Deployment

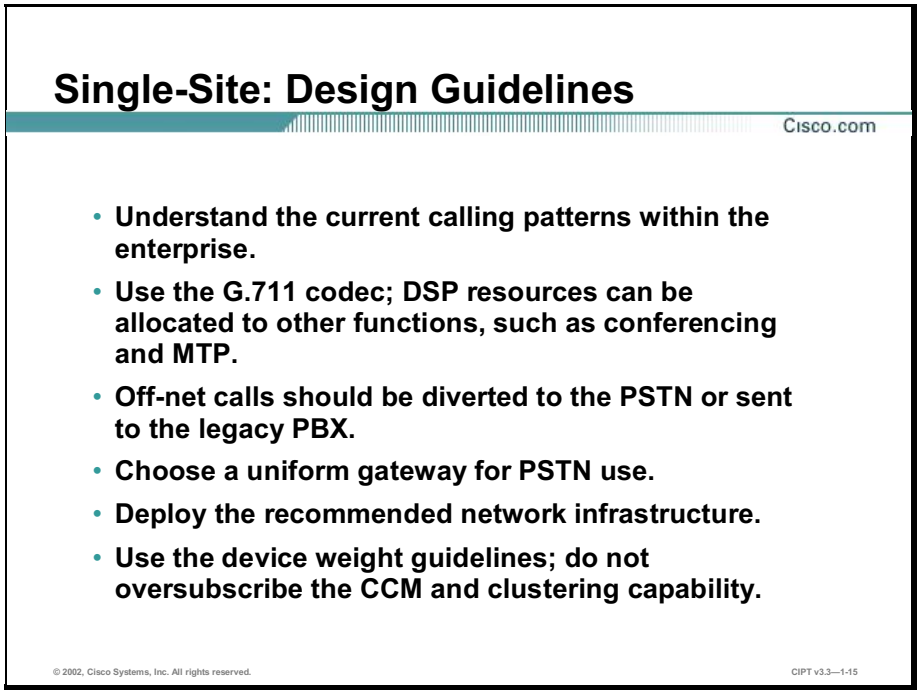
This topic describes the single-site deployment model.



In a single-site deployment model, all CCMs, applications, and DSP resources are in the same physical location. A single site consists of a single CCM cluster that can support at least 20,000 IP Phones when using Cisco MCS 7845-1400 servers. You can implement multiple clusters, and interconnect them via 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.

Design Guidelines

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 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 guidelines are relative to single-site deployments:

- 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.

- Using the G.711 codec in the LAN is a simple mechanism for deployment. It does not require dedicated DSP resources for transcoding, and many voice-mail systems support only G.711. You can allocate these DSP resources to other functions, such as conferencing and media termination point (MTP).

- 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.

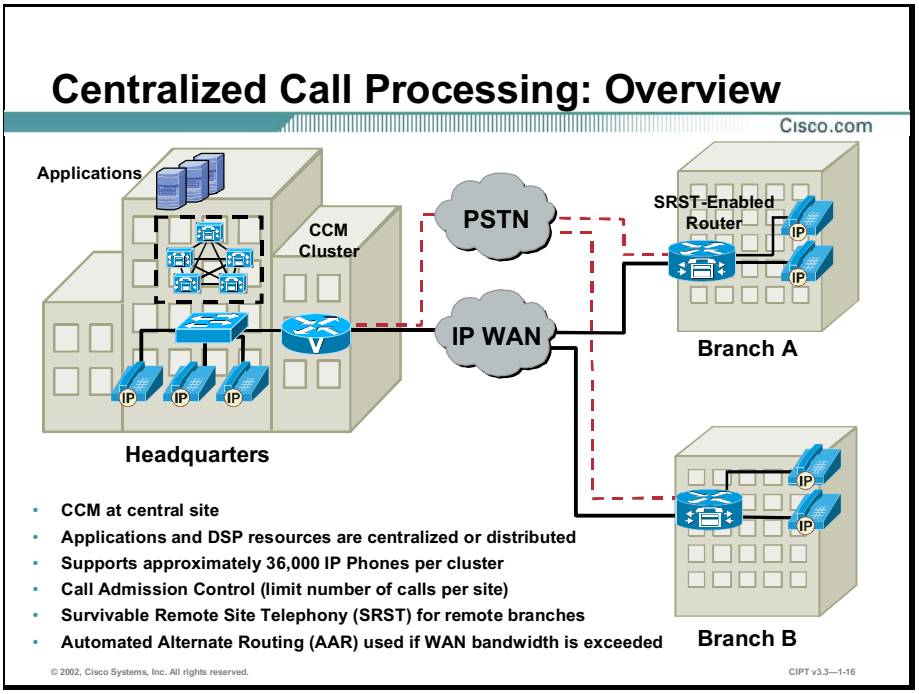
- Use Media Gateway Control Protocol (MGCP) gateways for the PSTN if H.323 functionality is not required. Centralize the gateway functions using H.323 gatekeepers when deploying multiple clusters, rather than using MGCP gateways.

- Deploy the recommended network infrastructure for high availability, connectivity options for telephones (inline power), quality of service (QoS) mechanisms, and other services.

- Use the device weight guidelines to provision resources on CCM. Do not oversubscribe CCM to scale larger installations.

Centralized Call-Processing Deployment

This topic examines the centralized call-processing deployment model.



The figure shown here illustrates the centralized call-processing deployment model with a CCM 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 CCM 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.

The WAN connectivity options include:

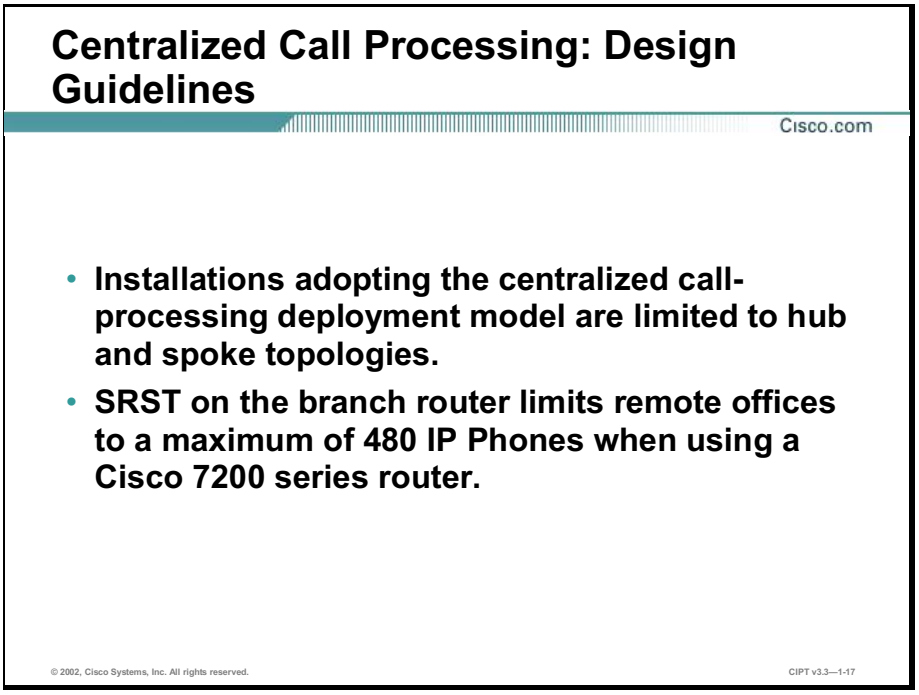
- Leased lines
- Frame Relay
- ATM
- ATM-Frame Relay Service InterWorking (SIW)

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 deteriorating the quality of established calls), the network may need a Call Admission Control (CAC) scheme. With the CCM Release 3.3, centralized call-processing models can take advantage of Automated

Alternate Routing (AAR) features. AAR allows CCM 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, or when network traffic uses all of the available bandwidth on the IP WAN, the users at remote branches can dial the PSTN access code and place their calls through the PSTN. 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. Even if the branch offices lose their connections to the central CCM cluster, you can provide call processing with the survivable remote site telephony (SRST) feature available for Cisco IOS gateways.



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

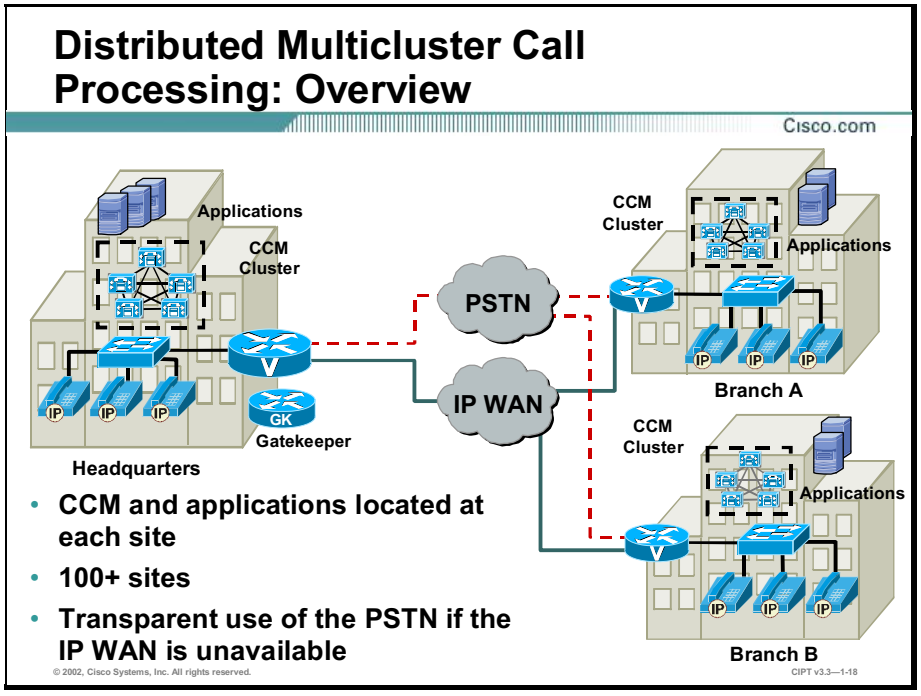
- Installations adopting the centralized call-processing deployment model are limited to hub and spoke topologies because the locations-based CAC mechanism records only the available bandwidth in and out of each location.

- There is no limit to the number of IP Phones at each individual remote branch. However, the survivable remote capability provided by the SRST feature in the branch router limits remote branches to 480 IP Phones on a Cisco 7200 router.

Note	Smaller platforms have lower limits.

Distributed Multicluster Call Processing

This topic examines the distributed multicluster call-processing design.



The distributed multicluster call-processing deployment model has one or more call-processing agents at each site, and each site has its own CCM 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:

- A single site with its own call-processing agent, which may be a CCM or other third-party call agent
- A centralized call-processing site (and all of its remote sites) that the network views as a single site for distributed call processing
- A legacy PBX with a VoIP gateway, or a legacy PBX 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 connected only through the PSTN a standalone site.

The WAN connectivity options include:

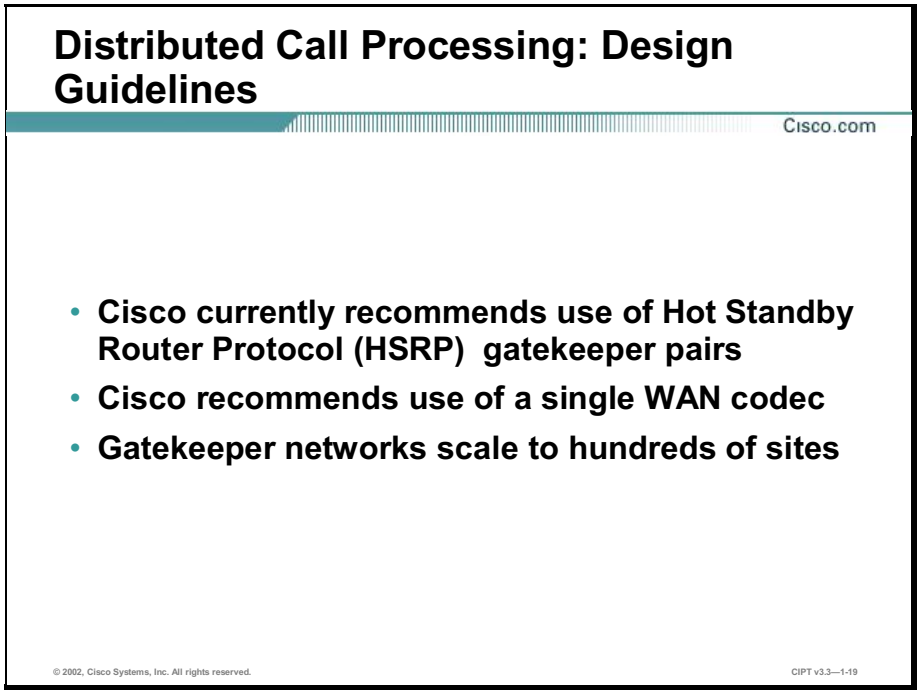
- Leased lines
- Frame Relay

- ATM
- ATM-Frame Relay SIW

Distributed multicluster 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. CCM simply sends all calls between the sites across the PSTN.

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

- Cost savings when utilizing the IP WAN for intersite calls
- Toll bypass savings when using remote gateways to drop off into the PSTN
- No loss of functionality during an IP WAN failure
- Scalability to hundreds of sites



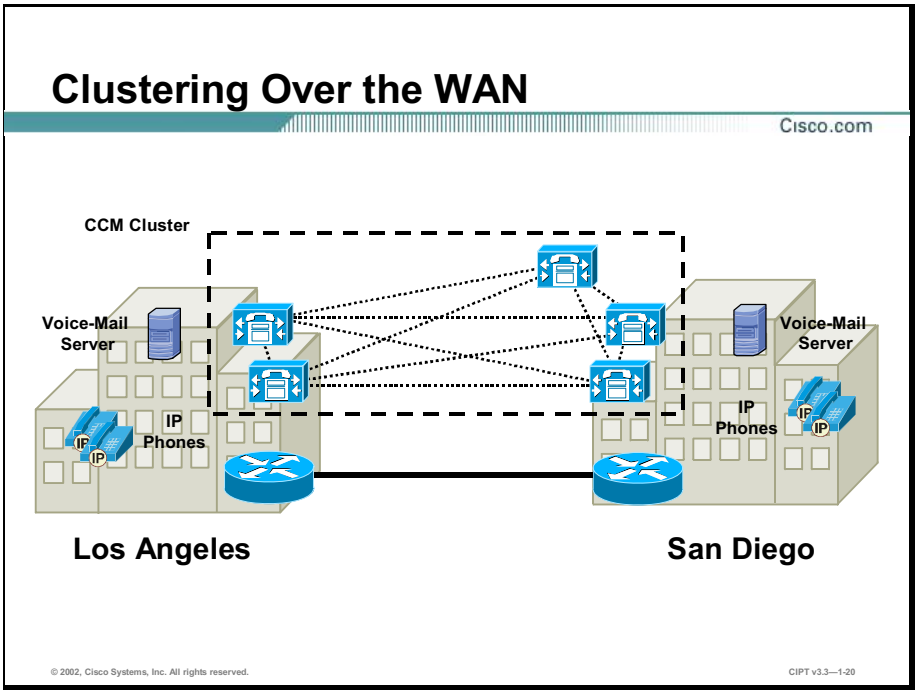
The multisite WAN with distributed call-processing deployment models is a superset of the single-site and multisite WAN with centralized call-processing models. You should follow the best practices from the single site and multisite guidelines in addition to those listed here, which are specific to this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

The key element is the gatekeeper device. This H.323 device serves two main functions: CAC and E.164 dial-plan resolution. Additional gatekeeper guidelines include:

- Cisco recommends using an alternate gatekeeper support to provide a gatekeeper solution with high availability. Cisco also recommends using multiple gatekeepers to provide spatial redundancy within the network.
- Cisco recommends using 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.
- Gatekeeper networks scale to hundreds of sites, and are not limited to hub and spoke topologies.

Distributed Single-Cluster Call Processing

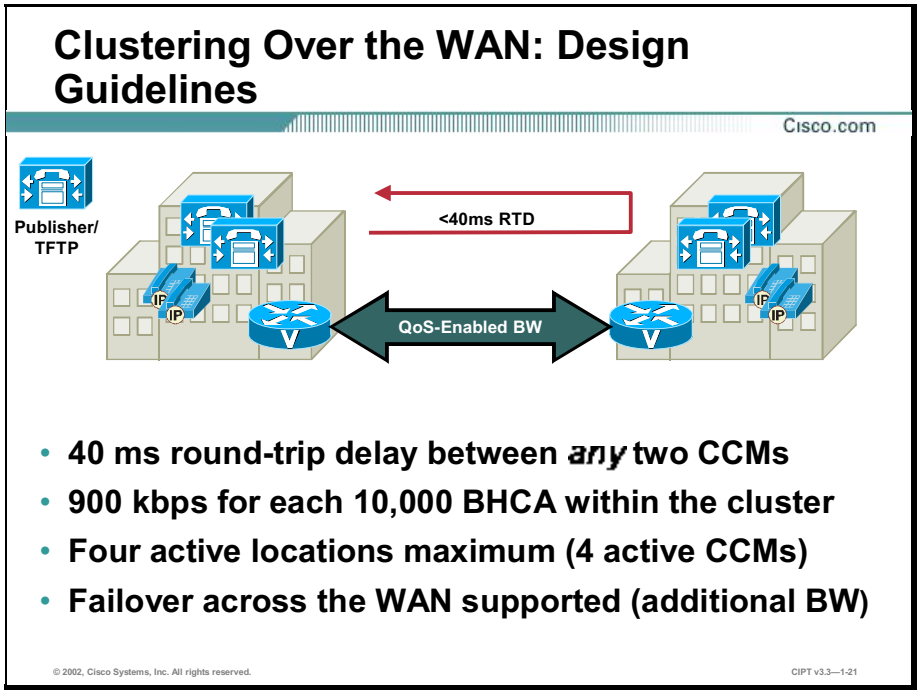
This topic examines the distributed single-cluster call-processing design.



Cisco supports CCM clusters over a WAN. While there are stringent requirements, this design offers the advantage of a unified dial plan and extends all features to all offices in the IP telephony network.

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

Because all CCMs are part of the same cluster, you also benefit from a single point of administration.

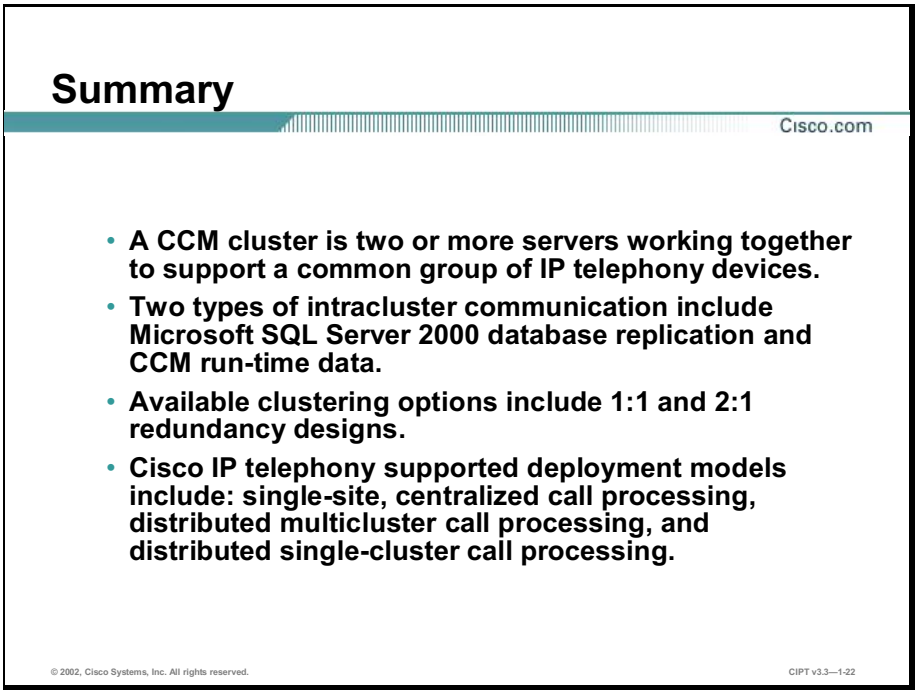


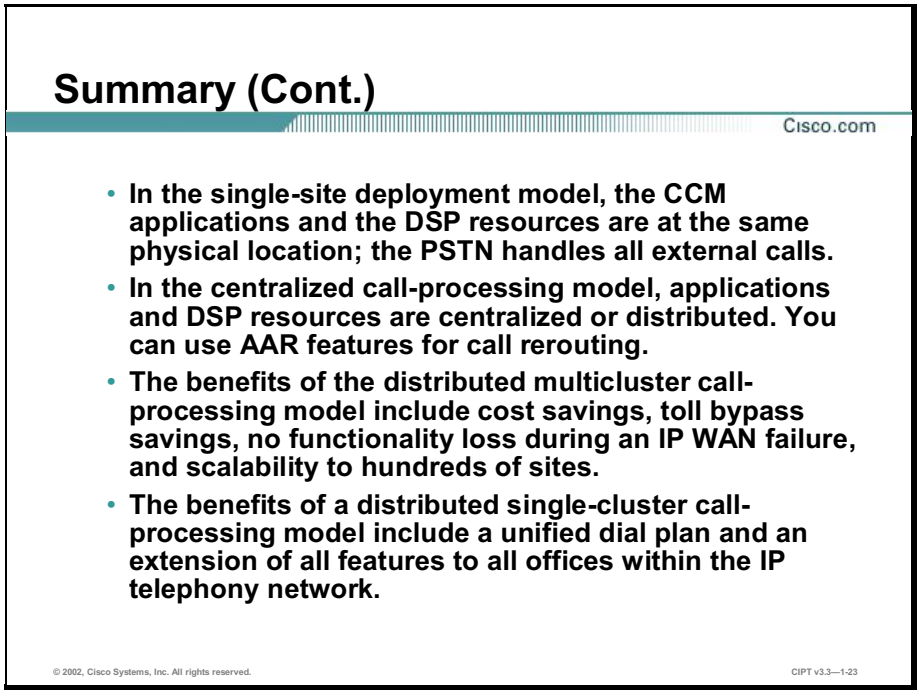
While the distributed single-cluster call-processing model offers some significant advantages, it must adhere to these strict design guidelines:

- Two CCMs 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 delay should not exceed 150 ms. Because of this strict guideline, you can use this design only between closely-connected, high-speed locations.
- For each of the 10,000 busy hour call attempts (BHCA) within the cluster, you must support an additional 900 kbps of WAN bandwidth for intracluster run-time communication.
- The distributed single-cluster design supports a maximum of four primary CCMs. This number correlates directly to the maximum number of supported locations.
- SRST can function in this model but is not necessary. The telephones can fail over across the WAN to other CCM 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.





Next Steps

After completing this lesson, go to:

- Installing Cisco CallManager lesson

References

For additional information, refer to these resources:

- CCM documentation: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm, 25 November 2002.

- Server and cluster capabilities: http://www.cisco.com, 25 November 2002.

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) What is the maximum two-way delay that is supported between CCMs when using a distributed single-cluster model?

A) 10 ms

B) 20 ms

C) 40 ms

D) 150 ms

Q2) What is the recommended best practice regarding WAN codecs in a distributed call-processing deployment?

A) G.711 only

B) G.729 and G.723

C) a single codec for the WAN

D) multiple codecs between the site

Q3) Which feature provides telephony services to a branch site when the WAN link goes down?

A) locations-based CAC

B) hub and spoke topology

C) extension mobility

D) SRST

Q4) Which codec is most often used in a single-site deployment?

A) G.729

B) G.723

C) GSM

D) G.711

Q5) Which of these servers is NOT required for a CCM cluster?

A) TFTP server

B) Microsoft SQL publisher

C) MS Exchange

D) none of the above

Q6) What does the subscriber do if the publisher does NOT answer its database lookup request?

A) waits for the publisher to become available and then makes a database request

B) sends a reorder tone to the device because it cannot access the database

C) requests the local copy of the database to look up the information

D) forces the device to register to another subscriber for a database lookup

Q7) Which of these options is NOT characteristic of a CCM cluster?

A) at least two servers

B) at least one publisher server

C) at least 2500 Cisco IP Phones

D) none of the above

Q8) What is the maximum number of IP Phones that the Cisco 7200 router can support at a remote branch location during a loss of connectivity to CCM headquarters in a centralized deployment model?

A) 280

B) 480

C) 580

D) 680

Installing Cisco CallManager

Overview

Cisco CallManager (CCM) includes the Windows 2000 operating system and the Microsoft Structured Query Language (SQL) Server 2000 relational database management system. This lesson will teach you how to install CCM on the Cisco MCS, which is shipped with a blank hard drive. Although the CCM installation process is fully automated and image based, you will learn key configuration points to consider before, and during, the installation process.

Importance

You must be able to install CCM to build a working Cisco IP telephony network. This lesson covers the installation process in a step-by-step format.

Objectives

Upon completing this lesson, you will be able to:

- Install CCM
- Identify installation configuration data
- Activate CCM components
- Describe post-installation procedures
- Upgrade prior versions of CCM

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Basic working knowledge of a computer and experience installing software onto a PC
- Basic understanding of network connectivity
- Understanding of CCM cluster design options

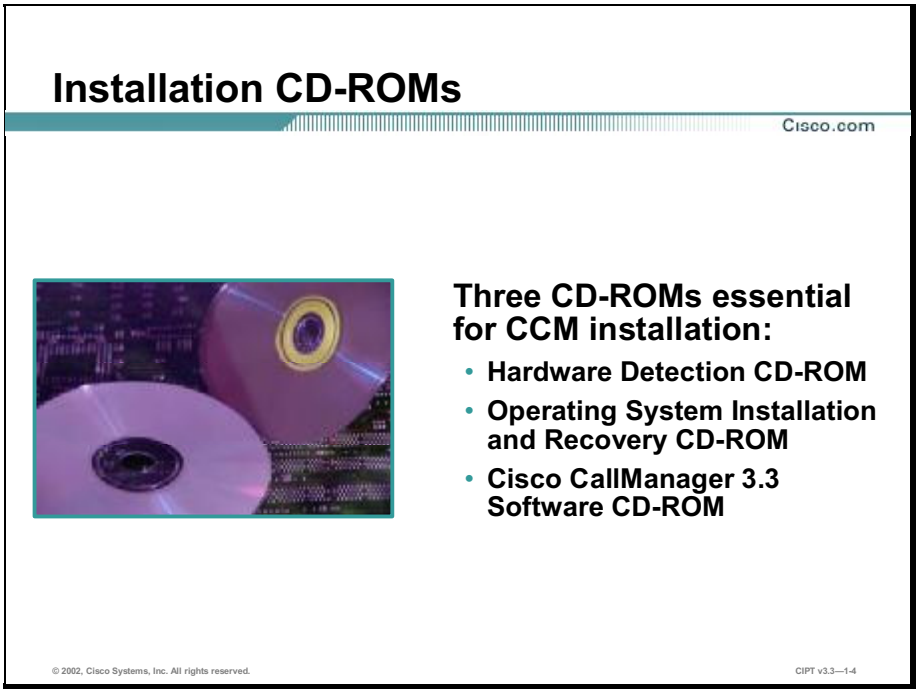
Outline

This lesson includes these topics:

- Overview
- Installation CD-ROMs
- Installation Configuration Data
- Activating CCM Components
- Post-Installation Procedures
- Upgrading Prior CCM Versions
- Summary
- Lesson Review

Installation CD-ROMs

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



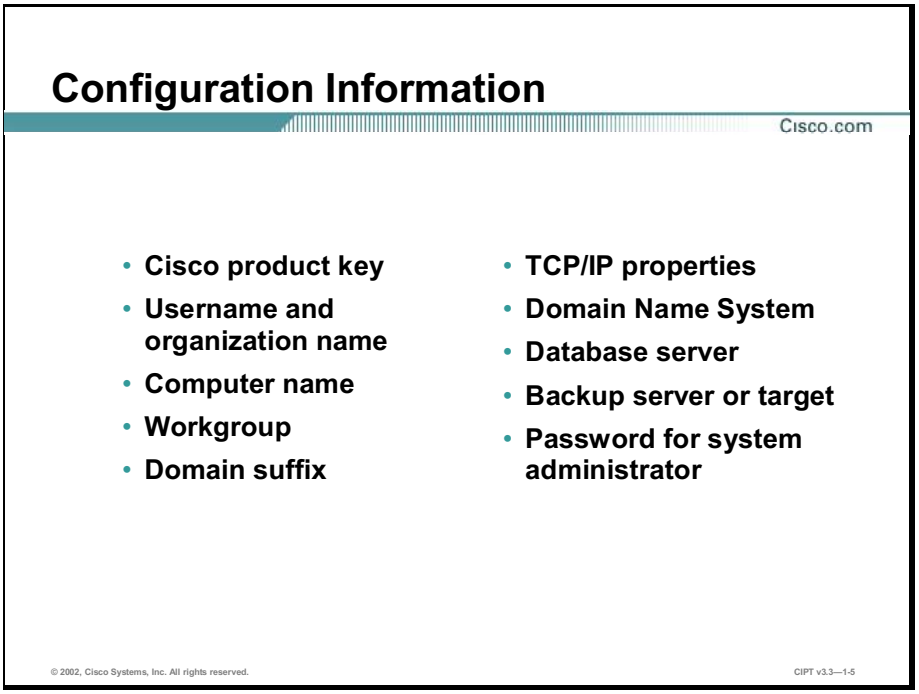
CCM is installed on the Cisco Media Convergence Server (MCS), a high-availability server platform. When you receive the CCM 3.3 software, you will use a number of CD-ROMs to perform a server installation. Because the installation of a CCM server is image based, after you boot the server using the Hardware Detection CD-ROM, the automated installation process should prompt you for the correct CD-ROMs to use. At a minimum, you will need the following CD-ROMs to perform a new CCM installation:

- Cisco IP Telephony Server Operating System Hardware Detection CD-ROM
- Cisco IP Telephony Server Operating System Installation and Recovery CD-ROM
- The Cisco CallManager 3.3 Software CD-ROM

Note Cisco provides many operating system installation and recovery CD-ROMs with the CCM software pack. The Hardware Detection CD-ROM will prompt you to insert the correct CD-ROM for your hardware platform.

Installation Configuration Data

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



As you perform the CCM installation, the automated setup process will prompt you for the information necessary to build Windows 2000, Microsoft Structured Query Language (SQL) Server 2000, and CCM 3.3 with a base configuration. This automated setup process takes between 30 and 45 minutes, depending on your server type. This process erases all data on the server hard disk. Before proceeding with the install, you should have the following information available:

- **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 letters; it does not contain numbers or special characters.

- **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.

- **Computer name:** The system will prompt you to assign a unique computer name, using 15 characters or less, to each CCM server. The computer name may contain alpha and numeric characters, hyphens (-), and underscores (_), but it must begin with a letter of the alphabet. Follow your local naming conventions, if possible.

- **Workgroup:** The system will also prompt you for a workgroup. 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 less, follows the same naming conventions as the computer name.

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

- **TCP/IP properties:** You must assign an IP address, subnet mask, and default gateway when installing a CCM server. You should not change the IP addresses after installation because they are permanent properties.

Note Cisco strongly recommends choosing static IP information, which ensures that the CCM server obtains a fixed IP address. With this selection, Cisco IP Phones can register with CCM when the telephones are plugged into the network.

If you choose to use Dynamic Host Configuration Protocol (DHCP), the Cisco Technical Assistance Center (TAC) insists that you reserve an IP address for each CCM server in the DHCP server scope. This action prevents the release, or reassignment, of IP addresses.

If you do not reserve IP addresses through the DHCP server scope, the DHCP server may assign a different address to the CCM server when the server is disconnected from, and then reconnected to, the network. You would then have to reprogram the IP addresses of the other devices on the network to return the CCM server to its original IP address.

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

Caution 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 a local name resolution using a configured lmhost file.

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

If you use a local name resolution, ensure that the lmhost 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 lmhost file on the new server during installation.

- **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 CCM server if you want to reassign the database server type at a later date.

Note	You must install a CCM publisher server before you are able to install any subscriber servers.

Caution	When you are configuring a subscriber database server, ensure that the server you are installing can connect to the publisher database server during the installation. This connection facilitates copying the publisher database to the local drive on the subscriber server. You must supply the name of the publishing 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.

- **Backup server or target:** Determine whether you will configure this server as a backup server or as a backup target.
  - The backup server performs the backup operation; it stores the backup data in the local directory, local tape drive, or network destination that you specify. You must share the directory Windows 2000 if you select a network area as the backup server.
  - The backup target contains the data to be backed up. You can select more than one target, but you can select only one server. CCM will automatically add a server to the backup target list in the Spirian Technologies, Inc. (STI) Backup utility if you configure the server as a backup server.
- **New password for the system administrator:** CCM Release 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 CCM database replication, you must enter the same replication account password for the publisher and all of the subscribers in the cluster.

Example

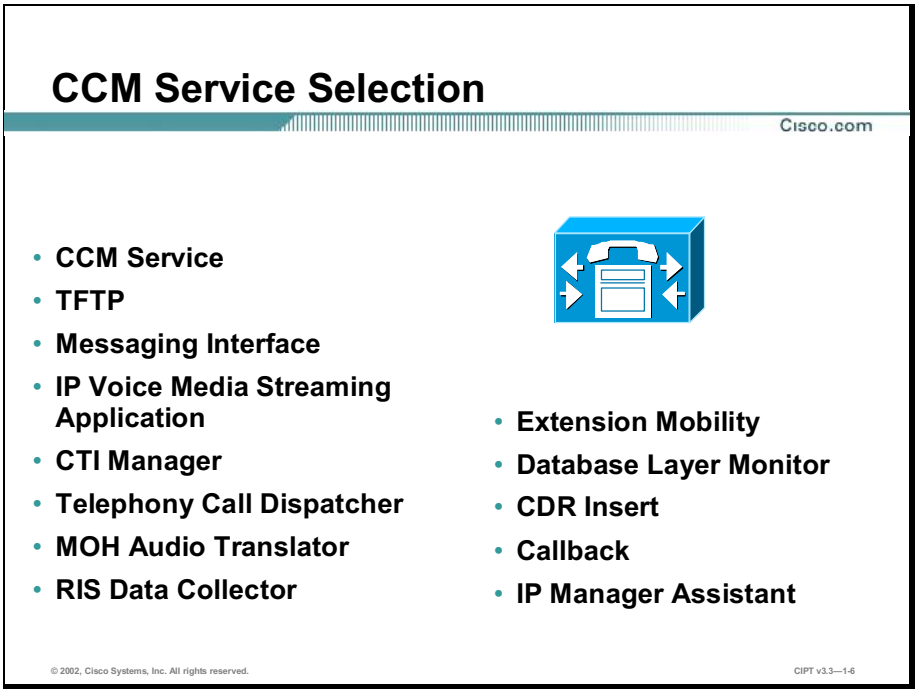
This table shows the configuration information that you need to install software on your server. You should complete all of the fields in the table, unless otherwise noted. You must gather this information for each CCM server that you are installing in the cluster. Make copies of this table, and record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

Table: 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	Cisco recommends that you program a fixed IP address in TCP/IP properties for the server instead of using DHCP.
TCP/IP properties (required if DHCP is not used) • IP address • Subnet mask • Default gateway	
DNS servers (optional) • Primary • Secondary WINS servers (optional) • Primary • Secondary	
Database server (choose one) • Publisher • Subscriber If you are configuring a subscriber server, supply the username and password of the publishing database server: – publisher username – publisher password	
Backup (choose one or both) • Server • Target	
New Win2k administrator password	

Activating CCM Components

This topic explains the process of selecting and activating the CCM components after installation.



When you complete the initial installation of CCM, you must activate the required CCM service components for this specific server. All components are in the deactivated default state. Cisco recommends that you activate only the required components for each server in the cluster. Each component that you activate adds additional load to the server.

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

The following information briefly describes each available CCM service:

- **CCM Service:** Allows the server to actively participate in telephone registration, call processing, and other CCM functions. CCM Service is the core service of the CCM platform.
- **TFTP:** Activates a TFTP server on CCM.
- **Messaging Interface:** Allows CCM to interface with a Simplified Message Desk Interface (SMDI)-compliant, external voice-mail system.
- **IP Voice Media Streaming Application:** Allows CCM to act as a media termination point (MTP), a conference bridge, and a Music On Hold (MOH) server.

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

- **Telephony Call Dispatcher:** Distributes calls to multiple telephone numbers (hunt groups). Cisco WebAttendant and Auto Attendant require Telephony Call Dispatcher.

- **MOH Audio Translator:** Allows CCM to convert MP3 or WAV audio files into the MOH format.

- **Real-Time Information Server (RIS) Data Collector:** Allows CCM to write trace and alarm file information to a database, or alert a Simple Network Management Protocol (SNMP) server.

- **Extension Mobility:** Allows CCM to support extension mobility functions for roaming users.

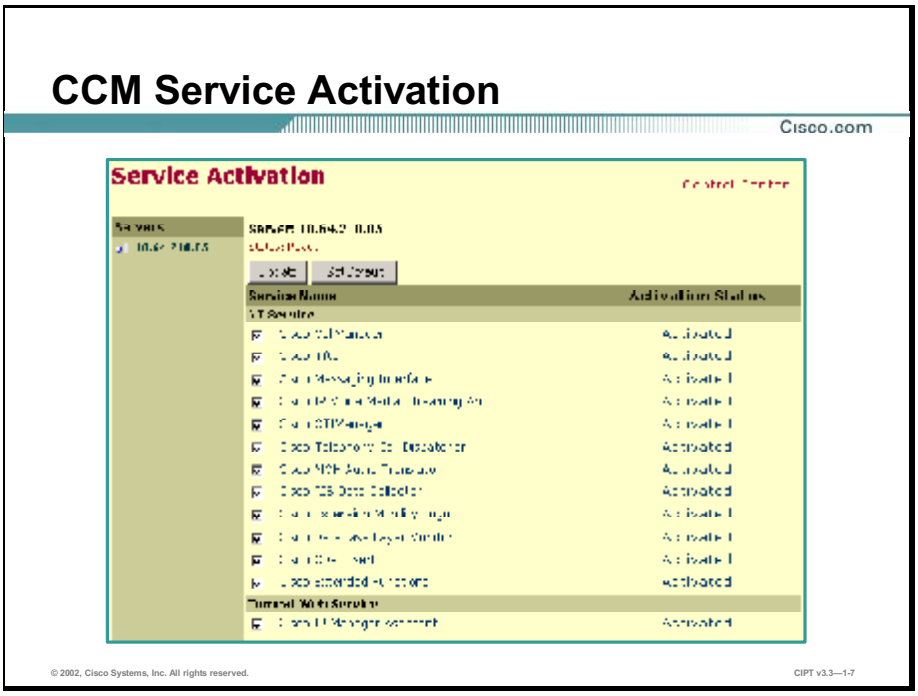
- **Database Layer Monitor:** Monitors aspects of the Microsoft SQL 2000 database, as well as Call Detail Records (CDRs).

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

- **Callback:** Allows CCM to support the callback function on user IP Phones.

- **IP Manager Assistant:** Allows CCM to support the Cisco IP Manager Assistant (IPMA).

CCM Service Activation



You can activate the CCM services on the Service Activation page. To activate these services, perform the following steps:

Step 1 Open Internet Explorer, and go to **http://<CallManager_IP_Address>/ccmadmin**. Enter the administrative username and password information.

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

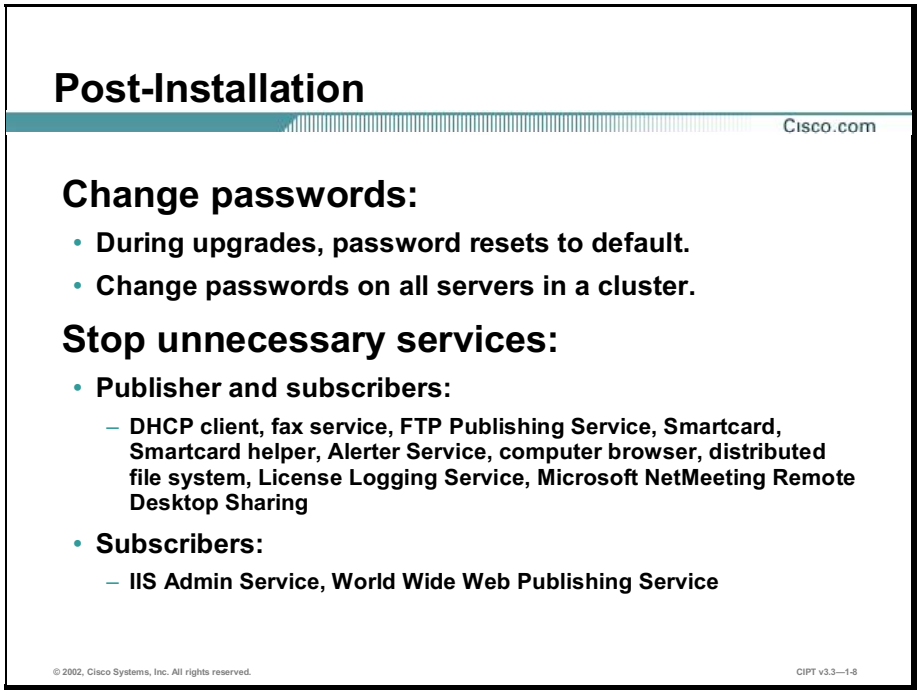
Step 3 From the Tools menu, choose **Service Activation.** A window similar to the window shown here appears.

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 CCM services from the Service Activation window. If you manually start the services through the Windows 2000 Services administrative tool, unpredictable results may occur.

Post-Installation Procedures

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



You should perform post-installation tasks to ensure the optimal operation of CCM. Perform the following tasks for each server that you have installed:

- **Change passwords:** During installation, all accounts are set to a default password. The server will prompt you to change the passwords for the CCM accounts after installation is complete. These passwords must be the same for each of the CCM servers in the cluster.

- **Stop unnecessary services:** The Windows 2000 operating system may have services running that are not necessary. When you stop unnecessary services, you will gain additional resources that you can allocate to mission-critical CCM processes. In addition, some Windows 2000 services can open security holes on CCM. You should stop these services to prevent potential intruders from finding server vulnerabilities.

You should stop all of the following services and set them to Manual Start status, unless otherwise needed on the system:

- DHCP client

- Fax service

- FTP Publishing Service

- Smartcard
- Smartcard helper
- Alerter Service
- Computer browser
- Distributed file system
- License Logging Service
- Microsoft NetMeeting Remote Desktop Sharing

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

- Internet Information Server (IIS) Admin Service
- World Wide Web Publishing Service

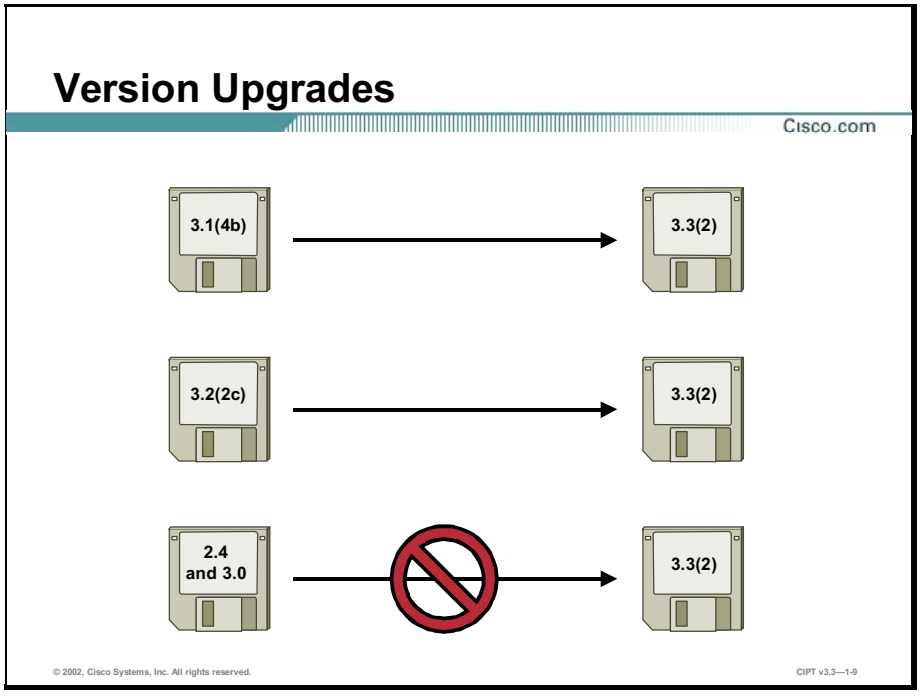
Both the FTP Publishing Service and the World Wide Web Publishing Service depend on the IIS Admin Service. When the IIS Admin Service stops, the FTP Publishing Service and World Wide Web Publishing Service also stop. You must set the FTP Publishing Service and the World Wide Web Publishing Service to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

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

After you have performed these tasks, and CCM is operational, run the Cisco MCS Backup utility to back up your CCM data.

Upgrading Prior CCM Versions

This topic describes the upgrade process for a CCM server.

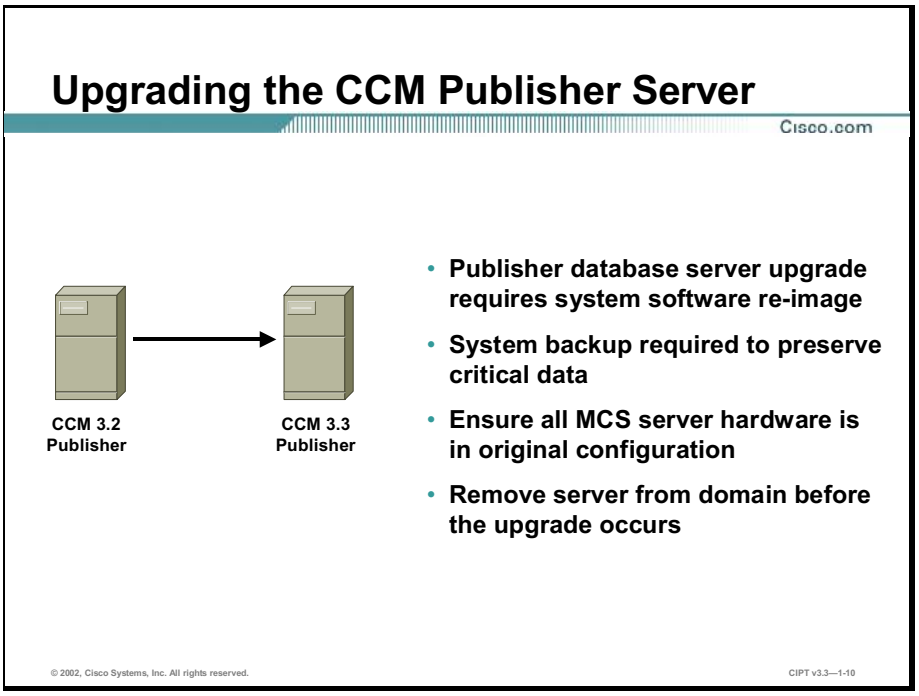


Cisco supports upgrading the publisher database server to CCM Release 3.3(2), a full version of CCM, from CCM Releases 3.1(4b) and 3.2(2c), which serve as minimum requirements.

Reference To verify whether other versions of CCM are compatible for upgrade to this release, use the following URL to refer to the *Cisco CallManager Compatibility Matrix*: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

If your server runs CCM Release 2.4 or 3.0, you must upgrade every server in the cluster to the latest version of CCM Release 3.1 before you can upgrade to a version of CCM Release 3.3.

Note The upgrade of the publisher server can take two to four hours, depending on your server type and the amount of CCM data that you need to back up.



Cisco requires a re-image of the publisher database server during the CCM Release 3.3(2) upgrade. Because this process erases all data on your server, you will need to back up all critical data. To perform this backup, you must upgrade your backup software with the Cisco IP Telephony Applications Backup 3.5 or later software located on the Cisco CallManager 3.3 Software CD-ROM in the \backup folder. This ensures compatibility with the backup software version installed with CCM 3.3.

Use the following steps when upgrading the CCM publisher server:

Caution Before starting the upgrade, make sure that you perform the recommended backup procedures for all coresident software applications installed on the server. Failing to complete a backup causes data and configuration settings to be lost. For information on performing the backup, refer to the documentation that supports the applications.

Step 1 Manually disable all platform agents and applications verified by Cisco (such as Cisco AVVID partner applications) that run on the servers in the cluster. Disabling platform agents and services—for example, performance monitoring (such as NetIQ), antivirus services (such as McAfee services, which are approved by Cisco), intrusion detection, and remote management services—ensures that the upgrade completes.

Step 2 Manually remove previous versions of the Cisco IP Telephony Applications Backup by using the **Add/Remove Programs** application in the Windows 2000 Control Panel. The upgrade does not prompt you to perform this task.

Step 3 Manually install the Cisco IP Telephony Applications Server Backup. The upgrade CD-ROM contains the Setup.exe file that you must use to install the application in the \backup directory.

Step 4 Back up the data on the publisher database server to either a network directory or local tape drive. Only data contained on the publisher database service is restored. For example, if Cisco TFTP does not reside on the publisher database server, the restoration at the end of the upgrade erases all customized TFTP information, such as specific IP Phone or gateway loads. If you want to retain this information, you must reconfigure the system so that the loads exist on the publisher database server, or you must manually save this data before the restoration.

Step 5 Using the operating system installation and recovery CD-ROMs, install the operating system. Make sure that you choose **Same Server Recovery** from the options during the operating system installation. Choosing this option ensures that the server retains the current network configuration data.

Caution Before you install the operating system, Cisco strongly recommends that you configure the server hardware (such as mirrored hard drives) to the state of the original configuration. A nonstandard server hardware configuration causes the CCM installation to fail and data or configuration settings from drive mirroring to be lost.

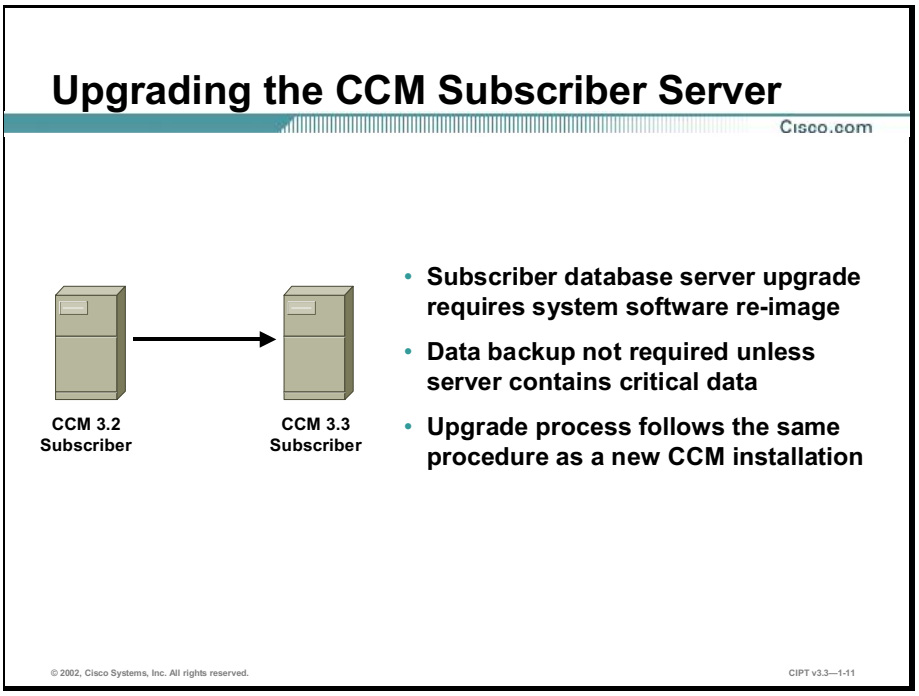
Note To avoid dormant domain system accounts, Cisco strongly recommends that you remove the server from any Windows-based domain during the upgrade. In addition, do not install any operating support packs until you complete the upgrade on every server in the cluster.

Step 6 Install CCM 3.3. Choose to perform a **Complete** installation when prompted by the wizard-based setup program.

Note While new CCM installations reboot with all CCM-based services disabled, the CCM upgrade process keeps running the services that were active before you performed the upgrade process.

Step 7 Restore the data that you backed up before you upgraded the CCM. The restore utility should open automatically after you install the CCM software and reboot your server.

Reference For all CCM installation and upgrade guides, refer to the following URL (requires CCO login and password): http://www.cisco.com/en/US/customer/products/sw/voicesw/ps556/prod_installation_guides_list.html.



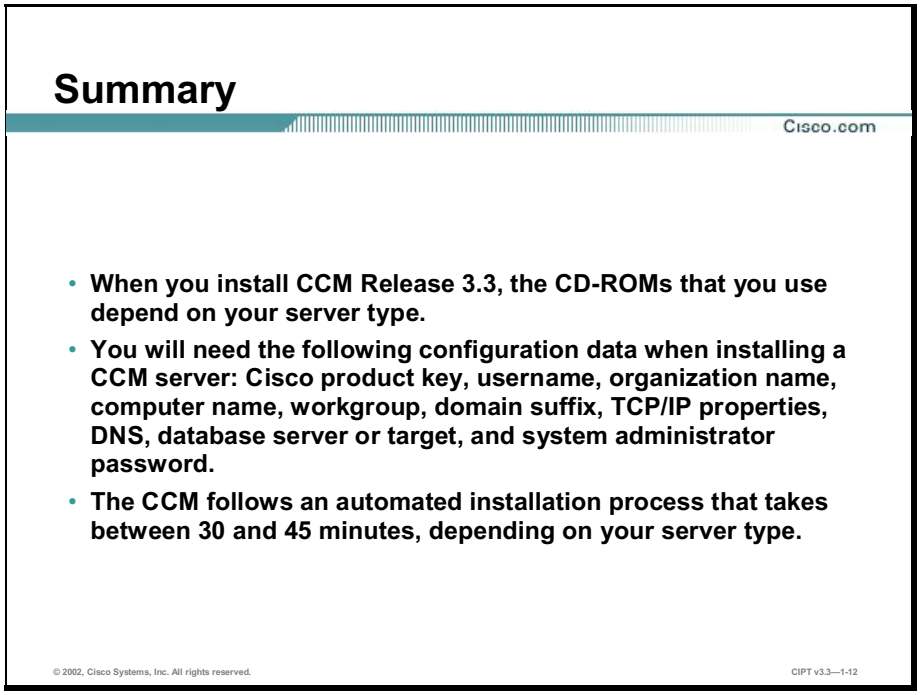
Because the foundation operating system changes to support CCM 3.3, you must also re-image the subscriber servers running a prior CCM version. Because the subscriber servers do not typically contain critical data, you should not need to perform a complete server backup. If your subscriber server acts as the TFTP server, you may want to manually back up custom files, such as IP Phone firmware images or ring files, before performing the server upgrade.

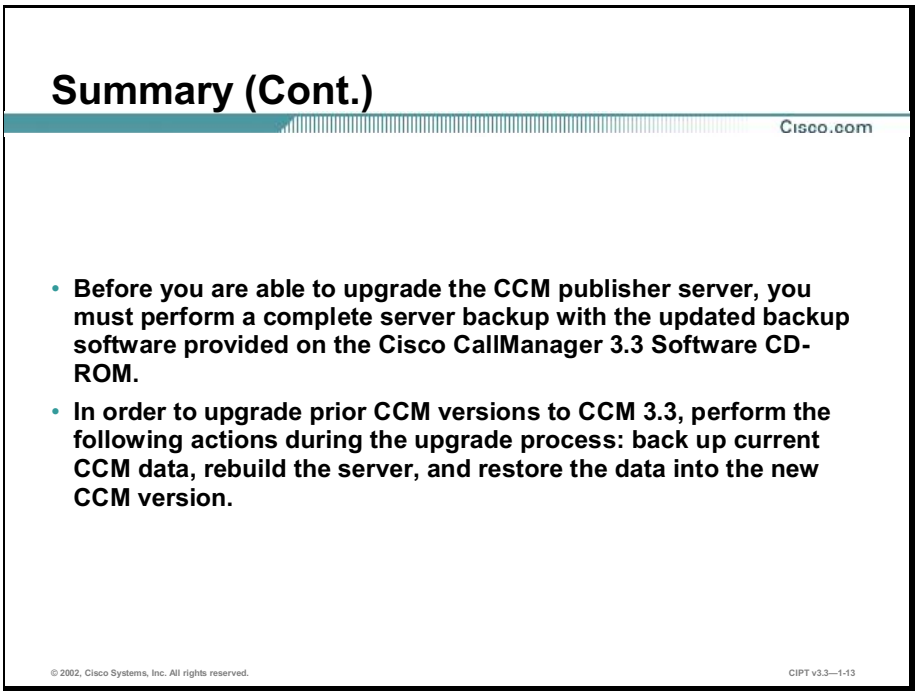
The installation process for the subscriber server follows the same procedure as a new installation of CCM. After you build the server and install the CCM software, the subscriber will receive a fresh copy of the Microsoft SQL database from the publisher.

Caution	Before installing the subscriber server, ensure that the server has network connectivity to the publisher database. The CCM installation will fail if you do not provide this connectivity.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Devices module

References

For additional information, refer to these resources:

- CCM documentation: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm, 25 November 2002.
- *Cisco CallManager Compatibility Matrix*: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm, 25 November 2002.
- CCM installation and upgrade guides (requires CCO login and password): http://www.cisco.com/en/US/customer/products/sw/voicesw/ps556/prod_installation_guides_list.html, 25 November 2002.
- Smith, A., Chris Peace, Delon Whetton, and John Alexander. *Cisco CallManager Fundamentals: A Cisco AVVID Solution.* San Jose, California: Cisco Press; 2001.

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which two of these services does Cisco recommend that you stop on a subscriber server? (Choose two.)

A) FTP Publishing Service

B) CCM Service

C) IIS Admin Service

D) World Wide Web Publishing Service

Q2) What function does the Cisco Messaging Service provide?

A) supports Cisco Unity

B) allows CCM to interface with SMDI-compliant messaging systems

C) allows CCM to interface with any external messaging system

D) all of the above

Q3) If you are not using DNS, what must be configured to resolve NetBIOS server names?

A) DHCP

B) backup server

C) lmhost file

D) DNS reverse lookup

Q4) What is the total number of CD-ROMs needed to install CCM?

A) 1

B) 2

C) 3

D) 4

E) 5

F) 6

Q5) What is the first step required when upgrading the CCM publisher server?

A) back up the server data

B) upgrade the backup utility

C) reboot the server using the Hardware Detection CD-ROM

D) run the automated script on the Cisco CallManager 3.3 Software CD-ROM

2

Devices

Overview

This module teaches you the common devices used in a Cisco IP telephony solution, including Cisco IP Phones, Cisco Catalyst switches, and Cisco access gateways. You will learn the configuration and support of these devices.

Upon completing this module, you will be able to:

- Install and configure a Cisco IP Phone
- Configure Cisco CallManager to support IP Phones
- Configure Cisco Catalyst switches for single port multiple VLANs and inline power
- Configure Cisco CallManager to support Cisco access gateways for off-net telephony access

Outline

The module contains these lessons:

- Cisco IP Phones
- Configuring Cisco CallManager to Support IP Phones
- Cisco Catalyst Switches
- Cisco Access Gateways

Cisco IP Phones

Overview

This lesson will teach you the various models of Cisco IP Phones and how they work within a Cisco IP telephony solution. You will learn the configuration, registration, and call-processing processes of Cisco IP Phones and Cisco CallManager (CCM). You will also learn the H.323 audio coders-decoders (codecs) supported by each of these Cisco IP Phones and the advantages and disadvantages of each codec.

Importance

You should be able to distinguish between the various Voice over IP (VoIP) end-user devices created by Cisco and describe their functions in the IP telephony network. In addition, you must understand the communication between a Cisco IP Phone and CCM, during registration and call processing, to baseline normal voice network operations, and for troubleshooting purposes.

Objectives

Upon completing this lesson, you will be able to:

- Describe the common features of Cisco VoIP end-user devices
- List the entry-level Cisco IP Phones and their features
- List the midrange and upper-end Cisco IP Phones and their features
- Describe the features and benefits of the additional IP telephony devices
- Create a flowchart of the boot-up and registration process of a Cisco IP Phone to CCM
- Identify and define the benefits of the H.323 audio codecs supported by Cisco IP Phones

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of how network devices obtain subnet and IP addressing information
- An understanding of the relationship between servers in a CCM cluster

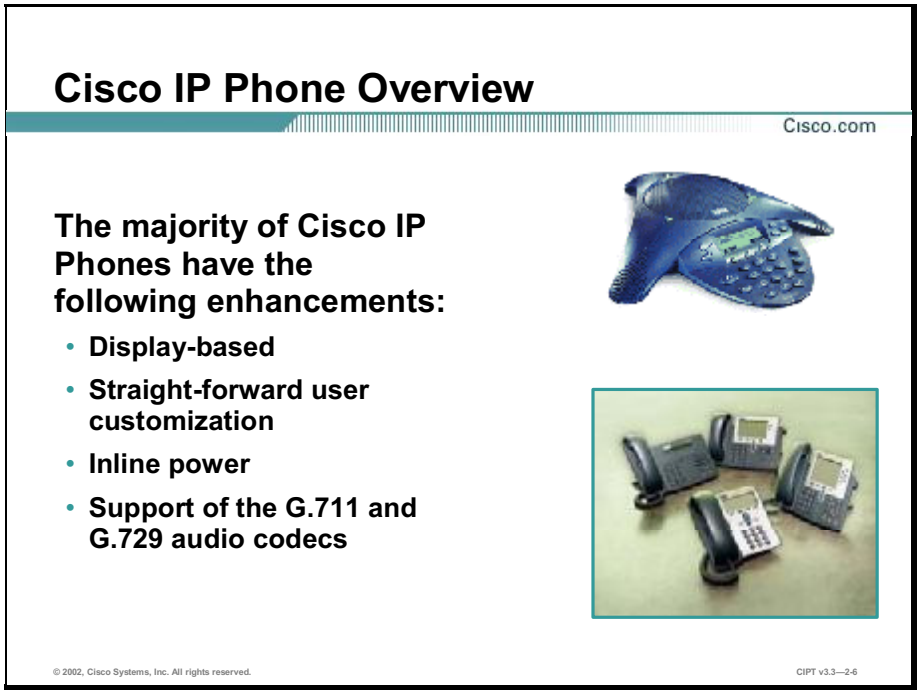
Outline

This lesson includes these topics:

- Overview
- Cisco IP Phone Overview
- Entry-Level Cisco IP Phones
- Midrange and Upper-End Cisco IP Phones
- Additional Cisco VoIP Devices
- IP Phone Registration Process
- Cisco IP Phone Codec Support
- Summary
- Lesson Review

Cisco IP Phone Overview

This topic provides an overview of Cisco IP Phones and features common to all Cisco Voice over IP (VoIP) end-user devices.



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

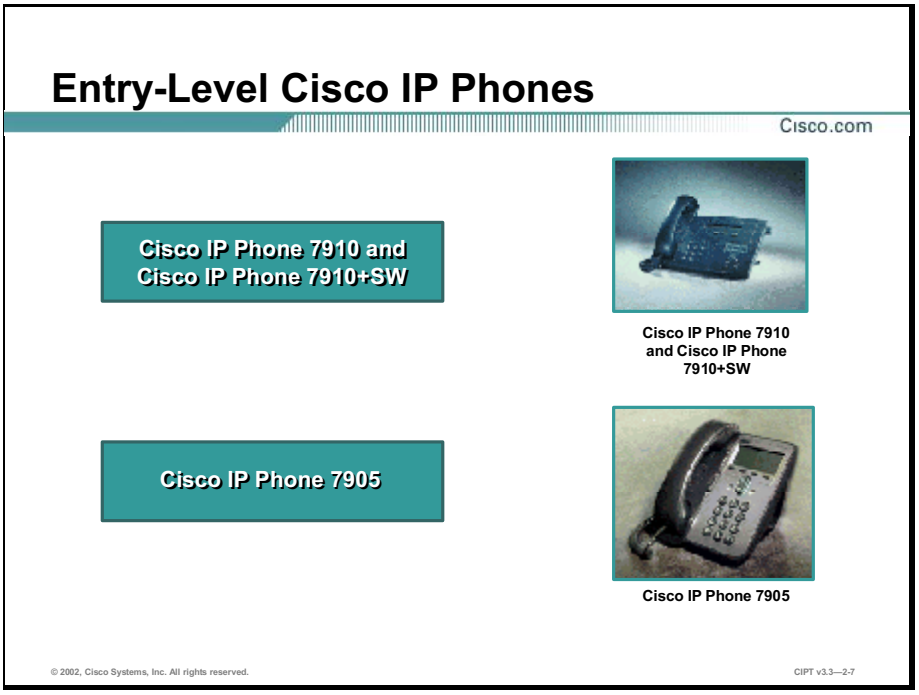
The majority of Cisco IP Phones possess these enhancements:

- Display-based
- Straight-forward user customization
- Inline power
- Support of 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 a Cisco IP Phone 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 available and a brief overview of their features.



Cisco has produced a number of entry-level IP Phones for a variety of functions. Depending on user functionality requirements, these IP Phones may function well for normal employees or for use only in public areas, such as lobbies or break rooms. You can also use these IP Phones in a lab environment to test simulated Cisco CallManager (CCM) deployments at a relatively low cost.

- **Cisco IP Phone 7910 and 7910+SW:** The Cisco IP Phone 7910 and 7910+SW are IP Phones 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 Cisco two-port switch, making it suitable for worker applications where you require basic IP Phone functionality and a collocated PC. The following is a brief description of the major features of these IP Phones:
  - Provide G.711 and G.729a codec support
  - Have a single 10BaseT RJ-45 connection (the 7910+SW provides two 10/100 Ethernet ports)
  - Support all standard IP Phone features

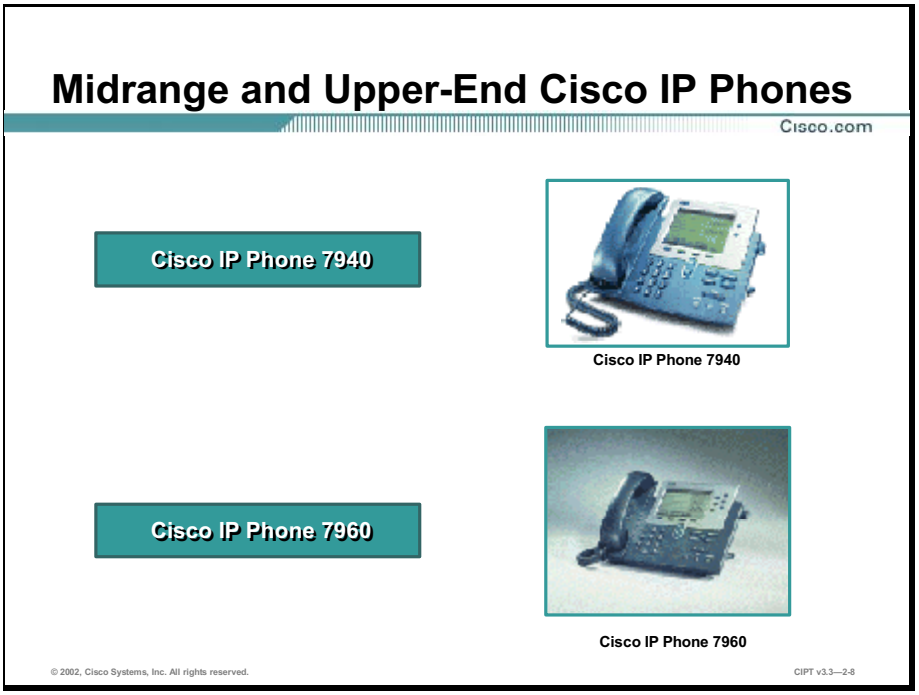
- Support local and inline power

- **Cisco IP Phone 7905:** The Cisco IP Phone 7905 provides single-line access and four interactive on-screen buttons or softkeys, which guide a user through call features and functions via the pixel-based liquid crystal display (LCD) screen. Use this IP Phone for employees that do not require a feature rich IP Phone or for public areas. Here is a brief description of the major features of the Cisco IP Phone 7905:

  - Has G.711 and G.729a codec support
  - Includes a single 10BaseT RJ-45 connection
  - Supports all standard IP Phone features through on-screen softkeys
  - Supports limited Extensible Markup Language (XML) script processing
  - Supports local and inline power
  - Supports H.323, Media Gateway Control Protocol (MGCP), and Skinny Station Protocols through firmware upgrades

Midrange and Upper-End Cisco IP Phones

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



Cisco designed the IP Phones 7940 and 7960 to meet the demand for a corporate-level IP Phone. The Cisco IP Phone 7940 meets the majority of employee needs because it supports all standard telephone features, two directory numbers, and XML services. The Cisco IP Phone 7960 meets the executive requirements by expanding the number of supported directory numbers to six. In addition, this model is compatible with the Cisco IP Phone 7914 expansion module, which adds 14 line or speed dial buttons through a module that attaches to the side of the IP Phone. A description of the Cisco IP Phone 7940 and the Cisco IP Phone 7960 follows:

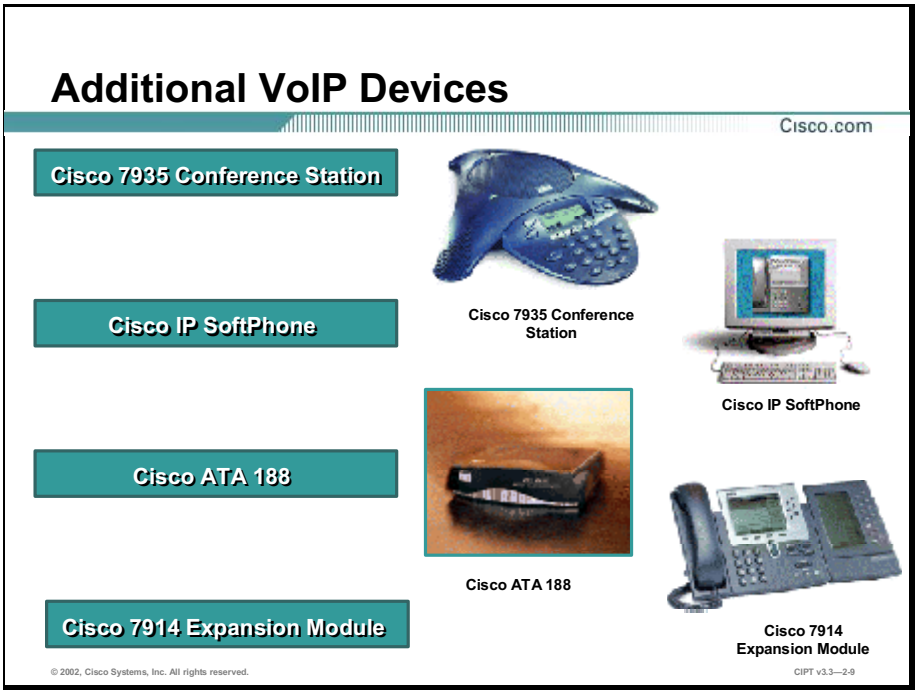
- **Cisco IP Phone 7940:** The Cisco IP Phone 7940 is for low-to-medium traffic users who need minimal directory numbers. This IP Phone operates with IP telephony systems based on CCM technology, H.323, or session initiation protocol (SIP). The 7940 IP Phone features include:
  - Two programmable line and/or feature buttons and four interactive softkeys
  - Two 10/100 Mbps RJ-45 ports
  - A minimum of 24 user-adjustable ring tones
  - G.711 and G.729a codec support
  - XML service support

- an EIA/TIA-232 port for options, such as line expansion and security access
- Skinny Station Protocol, MGCP, and SIP support through software image upgrade

- **Cisco IP Phone 7960:** The Cisco IP Phone 7960 is designed primarily for managers and executives. This IP Phone operates with IP telephony systems based on CCM technology, H.323, or SIP. Features of the this IP Phone include:
  - Six programmable line and/or feature buttons and four interactive softkeys
  - Two 10/100 Mbps RJ-45 ports
  - A minimum of 24 user-adjustable ring tones
  - G.711 and G.729a codec support
  - XML service support
  - EIA/TIA-232 port for options, such as line expansion and security access
  - Skinny Station Protocol, MGCP, and SIP support through software image upgrade

Additional Cisco VoIP Devices

This topic describes other Cisco VoIP devices that are available and a brief overview of their features.



Cisco continues to create additional IP telephony devices to meet the needs of businesses. These four devices meet specific business needs for the voice network:

- **Cisco 7935 conference station:** The Cisco IP conference station 7935 voice instrument is a full-featured, IP-based, full-duplex, hands-free conference station for use on desktops and offices and in small to medium-sized conference rooms. By integrating Polycom speakerphone technology, the Cisco IP conference station 7935 delivers high-quality audio through the VoIP network.

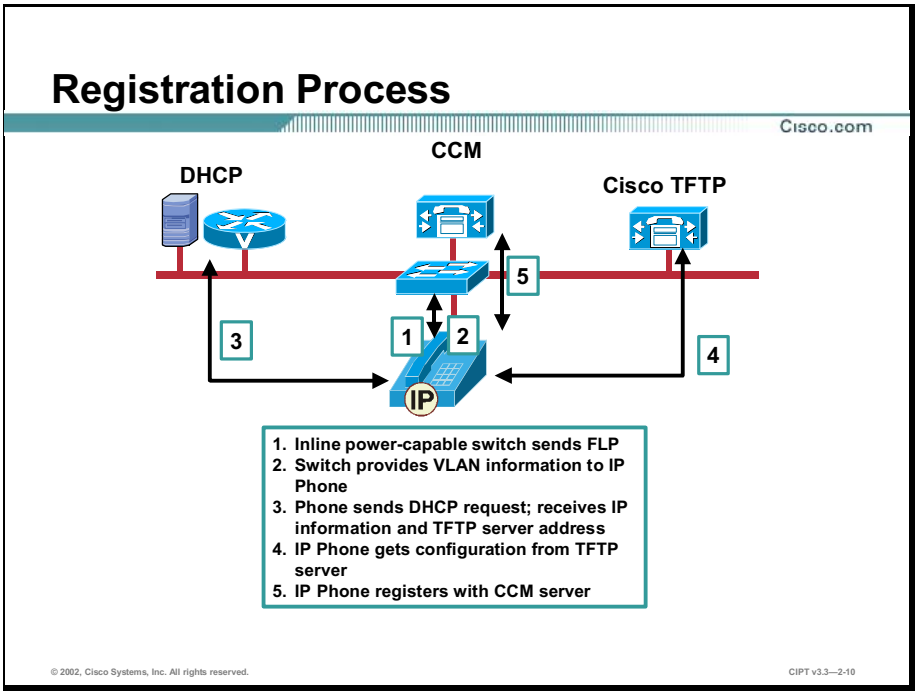
- **Cisco IP SoftPhone:** Cisco IP SoftPhone is a Windows-based application for the PC. Cisco IP SoftPhones allow you to integrate a software-based telephone with the IP telephony network. You can use a headset with an attached microphone to communicate, or some manufacturers are currently producing universal serial bus (USB)-based handsets, which are compatible with Cisco IP SoftPhones. Cisco IP SoftPhones integrate with Microsoft NetMeeting and Lightweight Directory Access Protocol (LDAP) directories, which provide video conferencing capabilities and the ability to drag and drop usernames from an LDAP directory list to dial or create larger conference calls. You can use the Cisco IP SoftPhone as a standalone telephone or to control an existing IP Phone, such as the Cisco IP Phone 7960.

- **Cisco Analog Telephone Adaptor (ATA) 188:** The Cisco ATA 188 interfaces regular telephones with your IP-based telephony network. This adapter is useful for customers that have existing legacy devices, such as fax machines or telephones, which they do not want to replace after they have migrated to VoIP. The ATA 188 provides two legacy voice connections, allowing you to attach two devices with distinct directory numbers. The equipment also supplies two 10/100 Mbps Ethernet connections, allowing you to collocate a network device with the legacy voice equipment.

- **Cisco 7914 expansion module:** The Cisco IP Phone expansion module 7914 extends the capabilities of the Cisco IP Phone 7960 with additional buttons and an LCD display. 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.

IP Phone Registration Process

This topic describes the registration process for a Cisco IP Phone.



This figure provides an overview of the registration process for a Cisco IP Phone. Each time an IP Phone boots, it uses this process:

1. If you are using a Cisco switch that is capable of providing inline power, the switch will send a Fast Link Pulse (FLP) signal. The switch uses the FLP to determine if the attached device is an unpowered Cisco IP Phone. In the unpowered state, a Cisco IP Phone loops back to the FLP, signaling the switch to send -48V DC power down the line.

2. After the IP Phone receives power and boots up, the switch sends a Cisco Discovery Protocol (CDP) packet to the IP Phone. This CDP packet provides the IP Phone with voice VLAN information, if that feature has been configured.

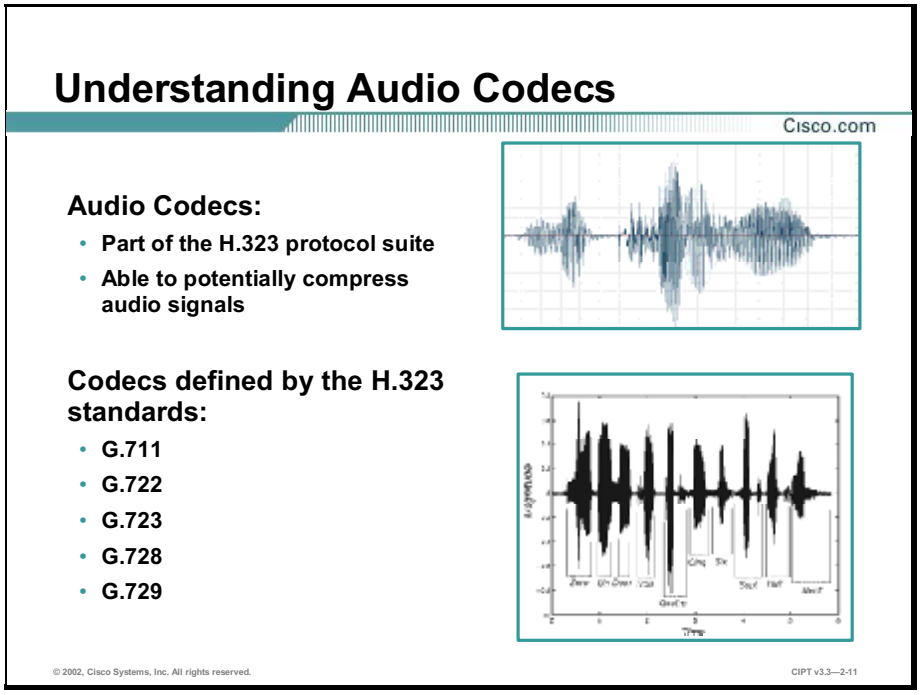
3. The IP Phone then broadcasts a request to a Dynamic Host Control Protocol (DHCP) server. The DHCP server responds to the IP Phone with a minimum of an IP address, a subnet mask, and the IP address of the Cisco TFTP server.

4. The IP Phone then contacts the Cisco TFTP server. The TFTP server sends the configuration information for that IP Phone, which contains an ordered list of up to three CCMs.

5. The IP Phone then attempts to register with the first CCM in the list provided by the TFTP server.

Cisco IP Phone Codec Support

This topic defines audio coders/decoders (codecs) and describes the codecs supported by most Cisco IP Phones.

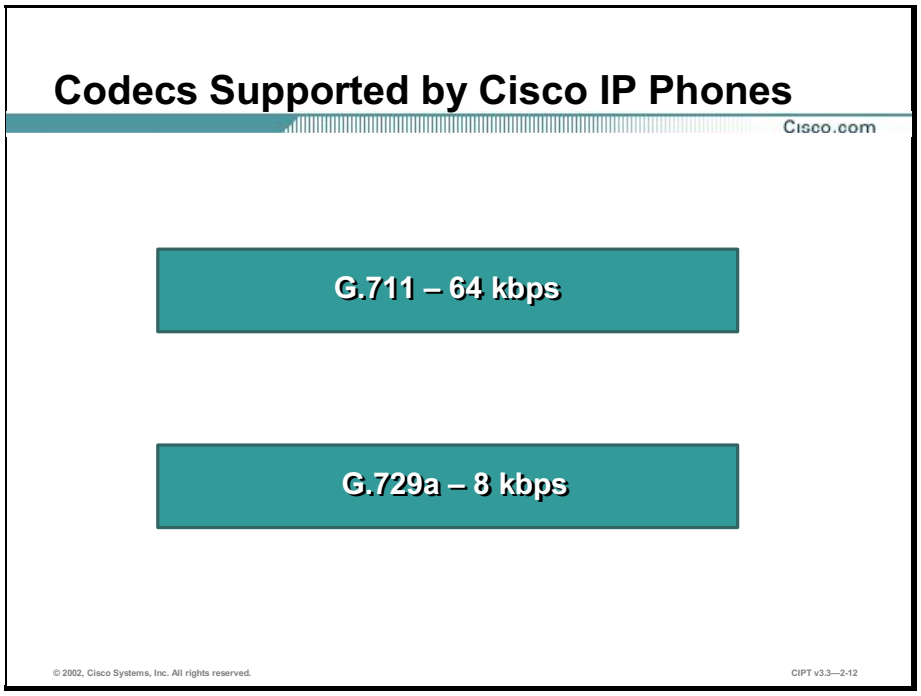


Before a VoIP device is able to stream audio, the device must convert audio into a generic format. For this purpose, the H.323 standards committee created multiple audio codecs. These codecs function at the presentation layer of the Open System Interconnection (OSI) Model. Their primary function is to convert voice signals into a generic standard that any H.323-compatible device can understand. 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 amount of bandwidth an audio stream consumes. Compression can cause degraded voice quality, which is why the different audio codecs offer different levels of compression.

The H.323 protocol suite defines the following audio codecs:

- **G.711:** Audio codec for 56/64 kbps
- **G.722:** Audio codec for 48/56/64 kbps
- **G.723:** Speech codec for 5.3 and 6.4 kbps
- **G.728:** Speech codec for 16 kbps
- **G.729:** Speech codec for 8/13 kbps

All H.323-compliant devices must support, at a minimum, the G.711 audio codec.



Cisco IP Phones natively support two primary codecs: G.711 and G.729a. While you are able to convert between other codecs through transcoding, Cisco recommends that you design your VoIP network around these two codecs.

The G.711 and G.729a codecs deliver relatively equal sound quality, with the G.711 scoring slightly higher than G.729a in a mean opinion score (MOS) test. Because of this equality, some network administrators choose to operate an entirely G.729a native network. Others choose to implement G.729a over the WAN and keep G.711 on the LAN.

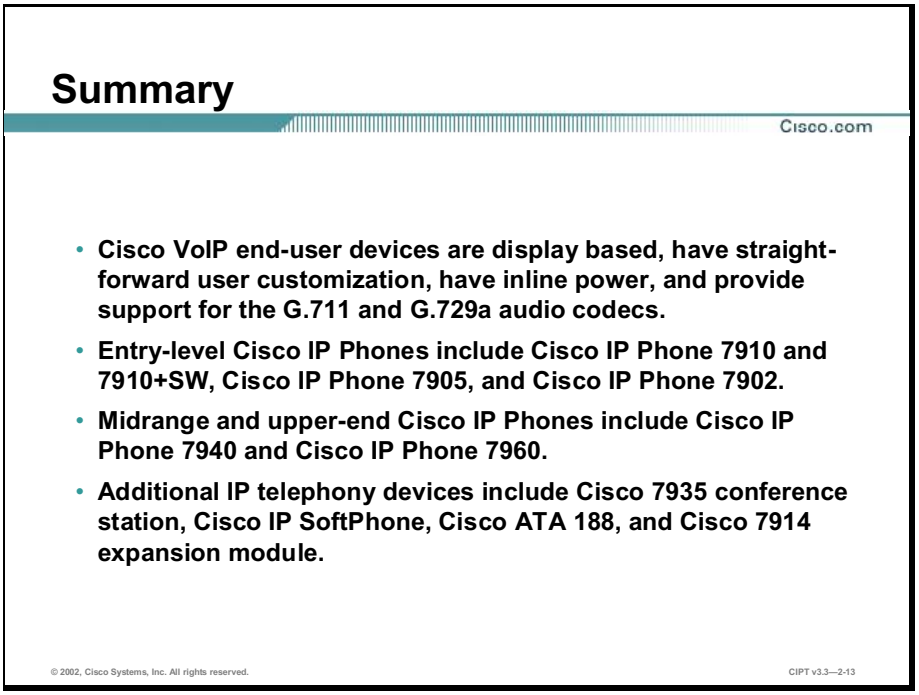
Note	The G.729a is a derivative of the original G.729 codec. While they are compatible, G.729a provides simpler algorithmic calculations.

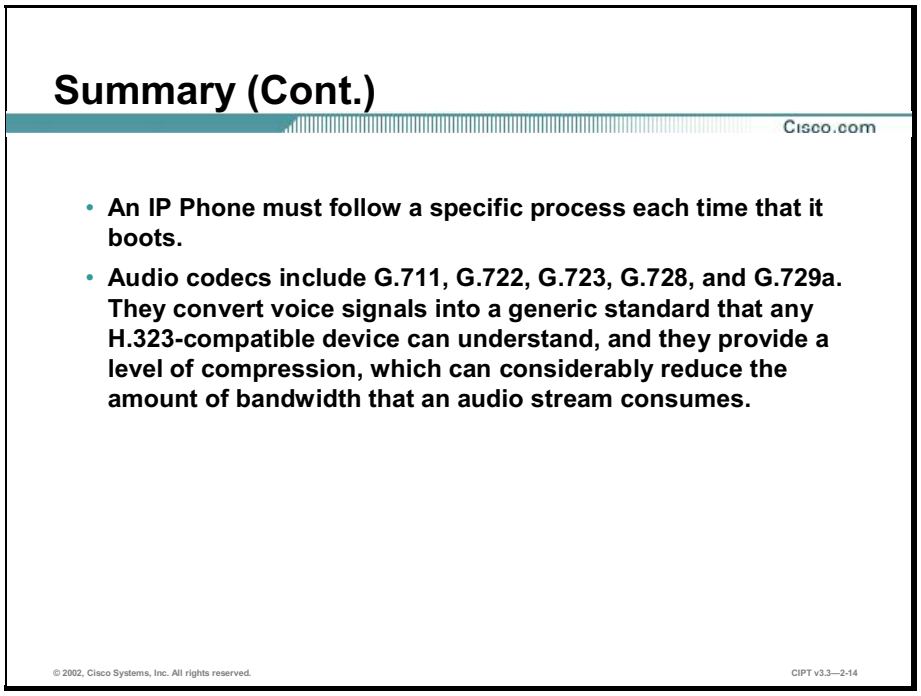
While this configuration is ideal for many network environments, you may eventually encounter a codec mismatch. A codec mismatch occurs when two devices cannot negotiate a common codec or when the network administrator has forbidden the use of their common codec, such as using G.711 over the WAN. Regardless of the cause, you now have a need for transcoding. Transcoding resources perform conversions between the H.323 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.

Note	Some first generation Cisco IP Phones, such as the 12SP+ and 30VIP, support the G.723 codec rather than G.729a. These IP Phones are no longer in production.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Configuring Cisco CallManager to Support IP Phones lesson

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which compressed codec do Cisco second-generation IP Phones support?

A) G.723

B) G.728

C) G.729

D) G.729a

Q2) Which item does a Cisco IP Phone NOT obtain from the DHCP server?

A) CDP

B) IP address

C) TFTP server IP address

D) subnet mask

Q3) A company wants to migrate to a VoIP network, but it has an expensive all-in-one voice/fax/copier device. Which device would you recommend?

A) Cisco 7936 Conference Station

B) Cisco IP SoftPhone

C) Cisco ATA 188

D) Cisco 7914 Expansion Module

Q4) A company is deploying a VoIP network for their call center of 120 employees. The call center employees require an IP Phone that is capable of supporting two directory numbers. In addition, the network administrator would like to run a single cable for the IP Phone and the computer that are collocated in each employee cubical. Which IP Phone will meet this requirement for the least expense?

A) Cisco IP Phone 7910+SW

B) Cisco IP Phone 7910

C) Cisco IP Phone 7940

D) Cisco IP Phone 7960

Q5) 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 meet these requirements?

A) Cisco IP Phone 7902

B) Cisco IP Phone 7905

C) Cisco IP Phone 7910

D) Cisco IP Phone 7912

Q6) Which of the following H.323 codecs do most Cisco end-user devices support?

A) G.711

B) G.723

C) G.711 and G.723

D) G.711 and G.729a

Configuring Cisco CallManager to Support IP Phones

Overview

Cisco CallManager (CCM) is the call-routing and signaling component for the Cisco IP telephony solution. This lesson describes the CCM configuration to support Cisco IP Phones. This lesson will teach you manual configuration and voice network configuration for auto-registration. You will learn how to configure device pools, which are responsible for configuring IP Phone redundancy, date or time zone, coder/decoder (codec) use, and other functionalities.

Importance

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

Objectives

Upon completing this lesson, you will be able to:

- Eliminate IP Phone reliance on the Domain Name System
- Configure a device pool
- Configure IP Phone button templates
- Manually configure IP Phones and directory numbers
- Configure CCM to support IP Phone auto-registration

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of the IP Phone registration process
- An understanding of the relationship between CCM clusters and device registration

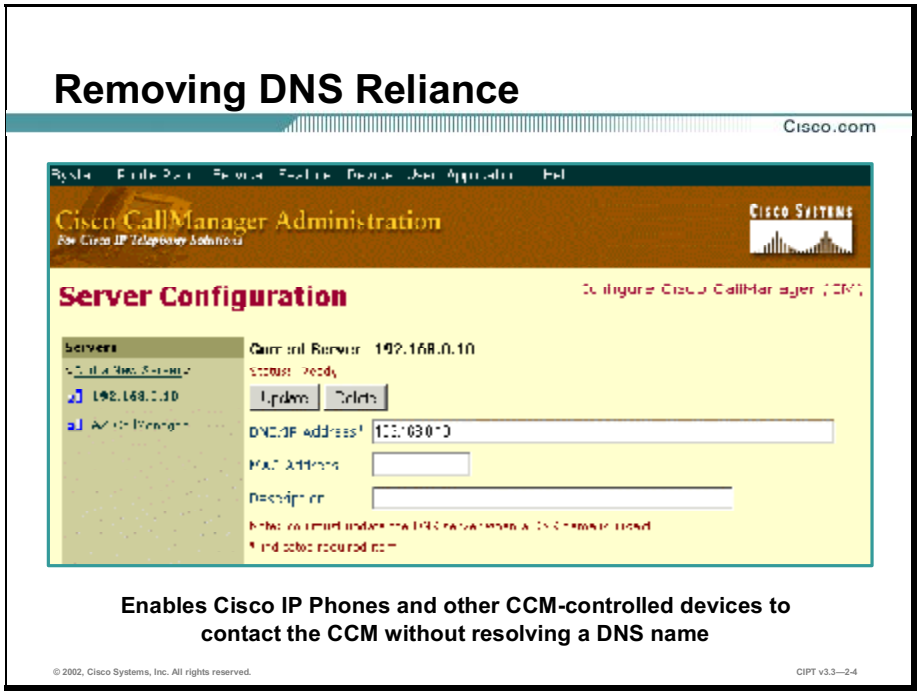
Outline

This lesson includes these topics:

- Overview
- Server Configuration
- Configuring Device Pools
- IP Phone Button Templates
- Manual IP Phone and Directory Number Configuration
- Configuring IP Phone Auto-Registration
- Summary
- Lesson Review

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 (CCM) to support IP Phones.

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

- It allows devices, such as Cisco IP Phones, to find CCM on the network without having to query the Domain Name System (DNS) server to help resolve the server name to an IP address.
- It prevents the IP telephony network from failing if the IP Phones lose connection to the DNS server.
- It decreases the amount of time required when a device attempts to contact CCM.

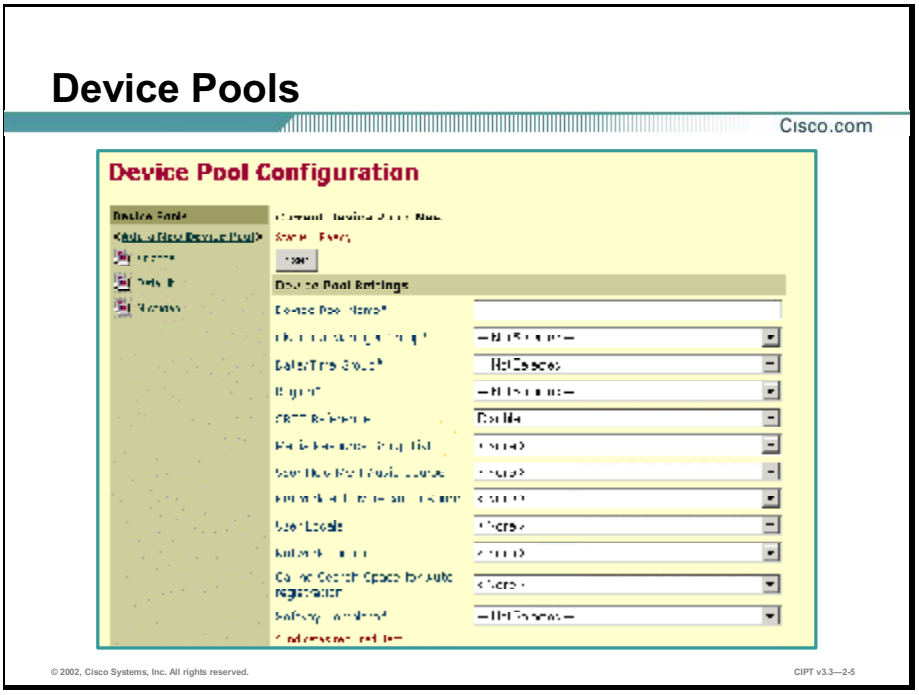
Perform these steps to eliminate DNS reliance:

Step 1 In Cisco CallManager Administration, choose **System**>**Server**. The Configuration window appears.

Step 2 Choose a server name from the left column, and enter the IP address for the server in the DNS/IP Address field; click **Update**.

Configuring Device Pools

This topic describes device pool configuration, which is essential to the functionality and performance of a voice network.



You must configure the device pool for IP Phones before adding them to the network. Cisco created the device pool configuration to eliminate excessive redundant configurations between devices. Device pools are responsible for assigning many key configuration items to Voice over IP (VoIP) devices.

Example

Configuring 100 different 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, which 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 five critical configuration items are:

- CCM group configuration
- Date/time group configuration
- Region configuration
- Softkey template configuration
- Device pool configuration

The configuration table shown gives a brief description of each device pool field.

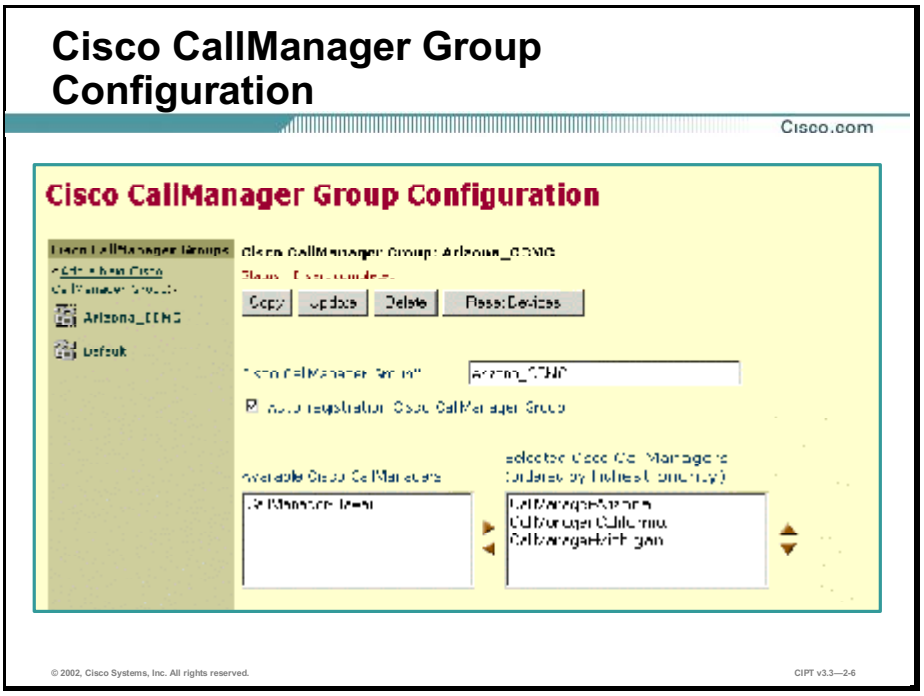
Table: Device Pool Configuration Items

Field	Description
Device Pool Name*	Describes a name for the device pool
CCM Group*	Selects a redundancy group for the device pool (This redundancy group can contain a maximum of three redundant CCM servers.)
Date/Time Group*	Assigns the correct time zone to the device
Region*	Determines codec selection when used by the device
SRST[1] Reference	Configures SRST and selects the gateway that will support a device if the connection to the CCM is lost
Media Resource Group List	Assigns media resource support to a device for functions such as conferencing, transcoding, or MOH
User Hold MOH Audio Source	Selects the audio that CCM should play when a user presses the **Hold** button on the IP Phone
Network Hold MOH Audio Source	Selects the audio that CCM should play when a user presses the **Transfer** or **Conference** button on the IP Phone
User Locale	Defines the language that the device uses
Network Locale	Defines the tones and cadences that the device uses
Calling Search Space for Auto-registration	Defines who an IP Phone is able to call if it auto-registers with the CCM
Softkey Template*	Defines the type and order of the softkeys displayed on the LCD[2] of a Cisco IP Phone

* indicates a required field.

1. SRST = Survivable Remote Site Telephony

2. LCD = liquid crystal display



A CCM group specifies a prioritized list with a maximum of three CCMs. The first CCM in the list serves as the primary CCM for devices assigned to that group. The other members of the group serve as secondary and tertiary backup CCMs. Changes to the CCM group affect the configuration file given to IP Phones by the TFTP server when they initially boot up.

Example

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

Checking the **Auto-registration Cisco CallManager Group** check box enables the CCM to place any new IP Phones that auto-register (IP Phones added to the network without manual administrative configuration) into this group by default. Unless you change its configuration, this default CCM group will only have the first CCM installed in the selected network.

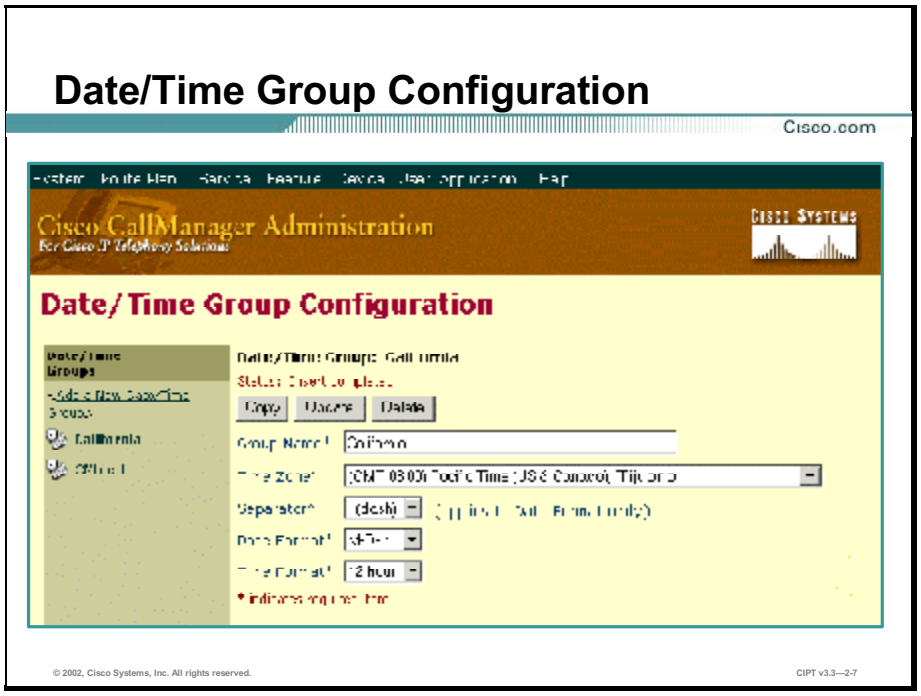
Perform these steps to configure a CCM group:

Step 1 Choose **System>Cisco CallManager Group**; the default group created by CCM during the installation appears.

Step 2 Choose **Add New Cisco CallManager Group** to create a new CCM group.

Step 3 Move the existing CCMs using the left and right arrows, and change the order of CCMs using the up and down arrows.

Note A CCM is often a member of multiple CCM groups.



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

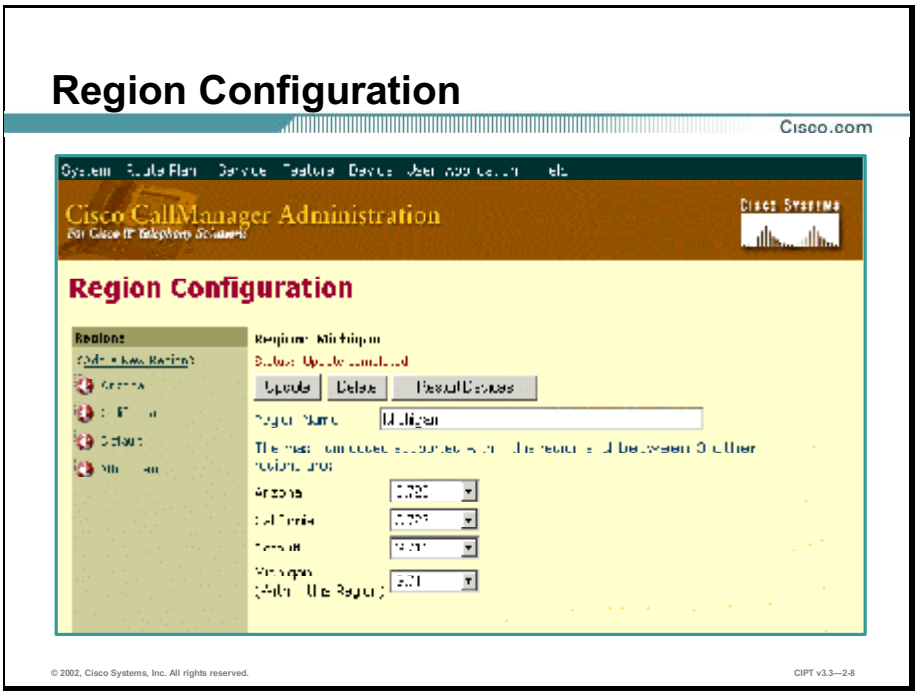
CCM has a default date/time group called CMLocal. The CMLocal date/time group synchronizes to the active date and time of the operating system on the CCM server. You can change the settings for CMLocal after installing CCM.

Perform 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.



CCM regions determine the audio codec that an IP Phone uses when communicating with other devices on the network. 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 CCM is G.711. If you do not plan to use any other voice codec, you do not need to use regions.

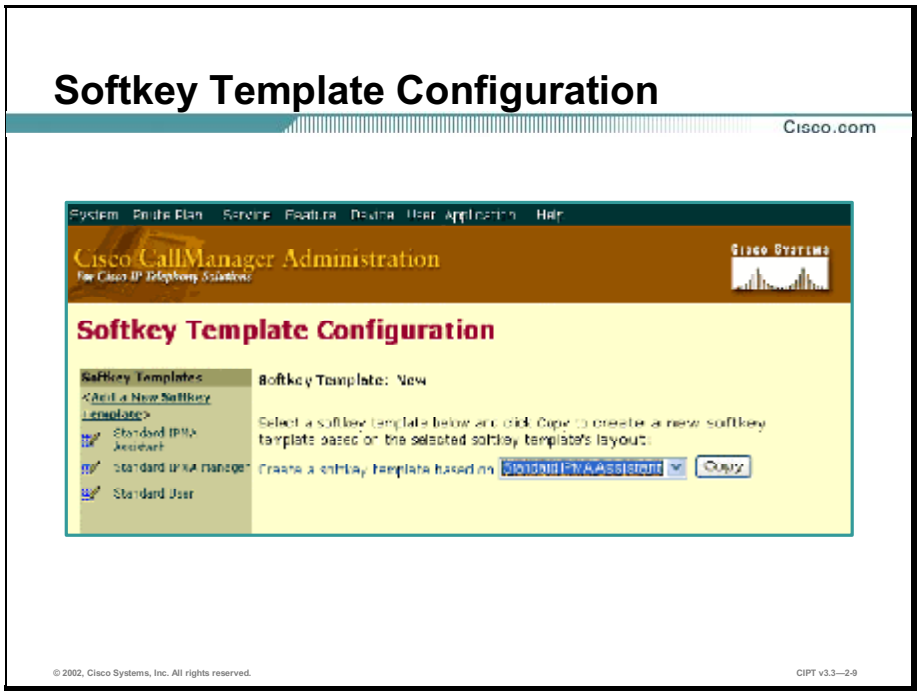
Example

In the figure shown here, there are four regions: Arizona, California, Default, and Michigan, with the configuration of the Michigan region displayed. If a device assigned to the Michigan region calls another device in the Michigan region, the devices will use the G.711 codec. However, if a device assigned to the Michigan region calls a device assigned to the Arizona region, the devices will use the G.729 codec. CCM creates the Default region during the installation process. Rename the Default region to a more logical name to avoid confusion.

Perform these steps to configure a region:

Step 1 Choose **System**>**Region**, and the default region created during the CCM installation appears.

Step 2 Choose **Add a New Region** to configure the regions, and choose the codec used between the regions.



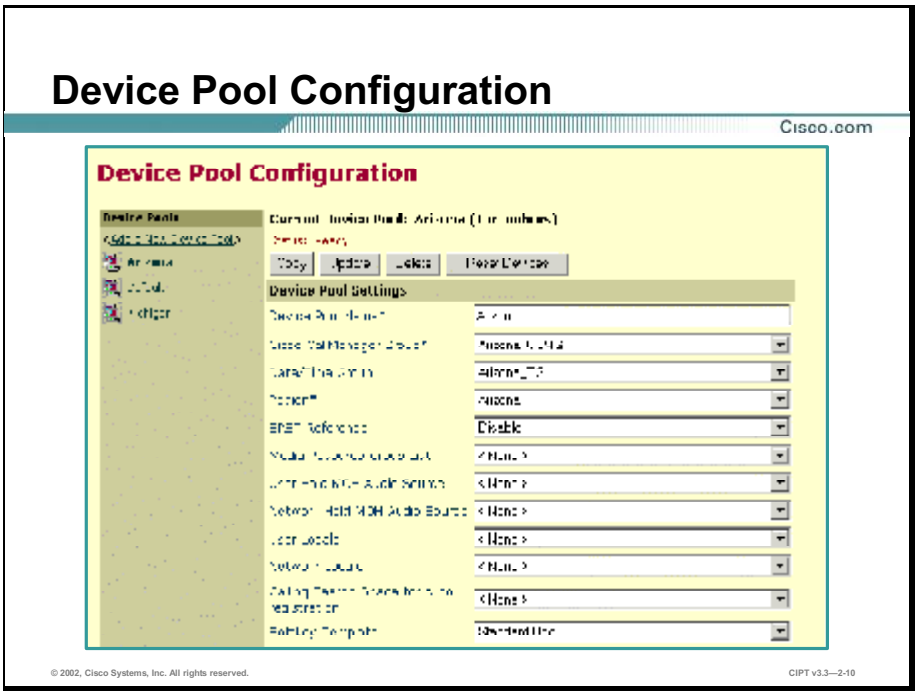
The Softkey Template Configuration window allows the administrator to manage the on-screen softkeys on Cisco IP Phone 7960 and 7940 models. You can configure these softkeys with many CCM functions and features.

CCM includes three default softkey templates; you cannot delete or modify the following standard templates:

- Standard IP Manager Assistant (IPMA)
- Standard IPMA Manager
- Standard User

Note The *Features Plus* module provides information about softkey template configuration. For now, use the Standard User softkey template during your device pool configurations.

Device Pool Configuration



After creating the minimal mandatory components of a device pool, you can create the device pool itself. The device pool combines all of the individual configurations you created into a single entity. You will eventually assign this entity to an individual device, such as an IP Phone. This process will configure that device with most of the configuration elements that it needs to operate efficiently in your IP telephony network.

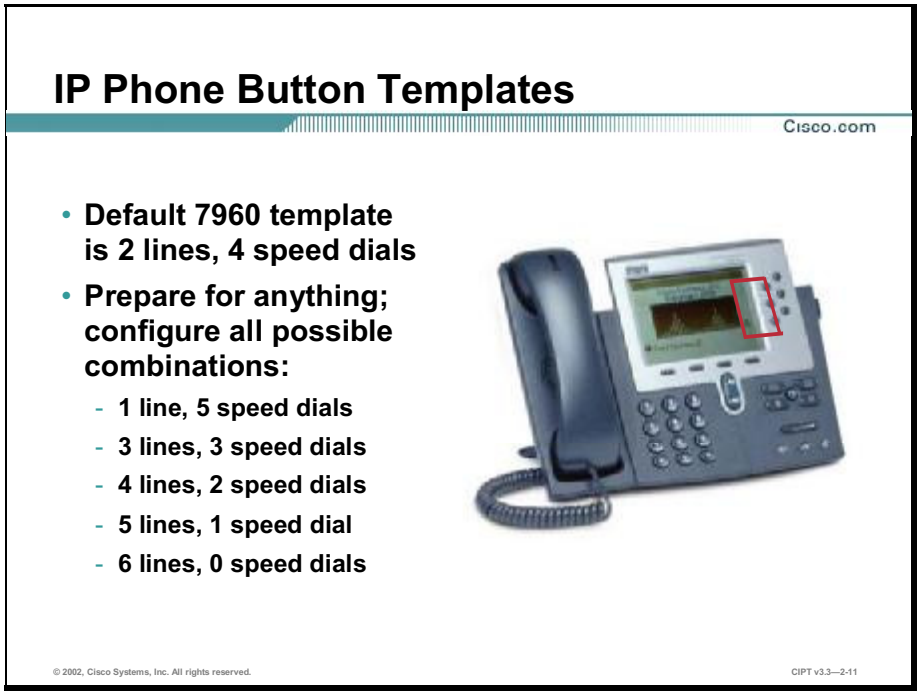
Perform these steps to create the device pool:

Step 1 Choose **System**>**Device Pool**.

Step 2 When the Device Pool Configuration window opens, click **Add a New Device Pool**, and choose, at a minimum, the CCM group, date/time group, region, and the softkey template that you created.

IP Phone Button Templates

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



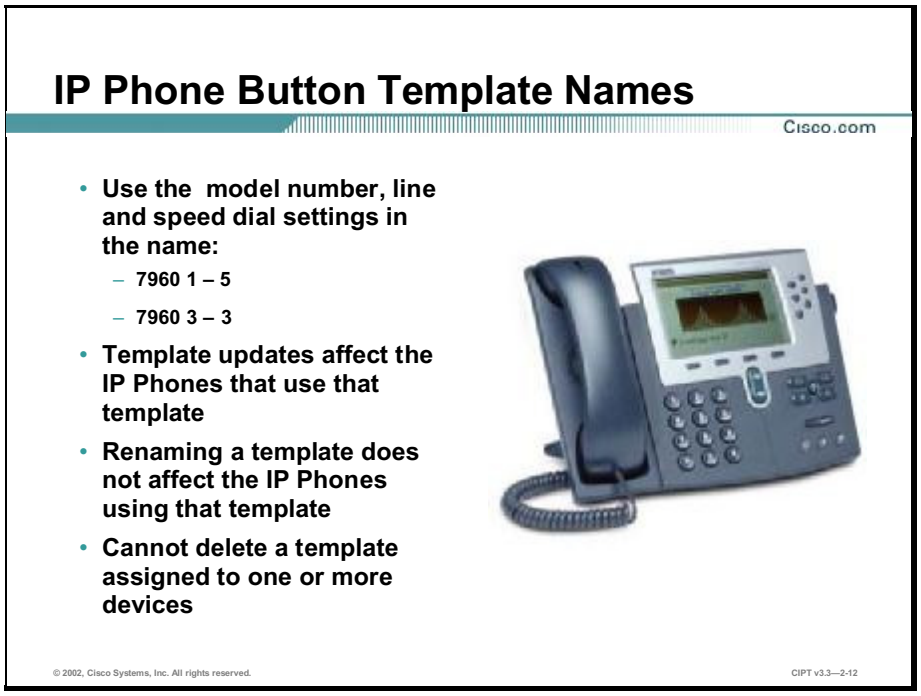
Creating and using templates provides a fast way to assign a common button configuration to a large number of IP Phones. CCM includes several default IP Phone button templates. When adding IP Phones, you can assign one of these templates to each IP Phone or create a new template.

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 IP 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 can use these IP Phone button template combinations:

- 1 line, 5 speed dials
- 2 lines, 4 speed dials (default)
- 3 lines, 3 speed dials
- 4 lines, 2 speed dials
- 5 lines, 1 speed dial

- 6 lines, 0 speed dials



Create easily recognizable naming conventions for the IP Phone button template.

Example

If you have a Cisco IP Phone 7960 that has three lines and three speed dials, you can use “7960 3-3” for the IP Phone button template name. If you have a special request or only a limited number of users that need three lines and three speed dials, you can quickly assign “7960 3-3” to the IP Phone, rather than creating a template for each IP Phone and then assigning the template to the IP Phone.

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

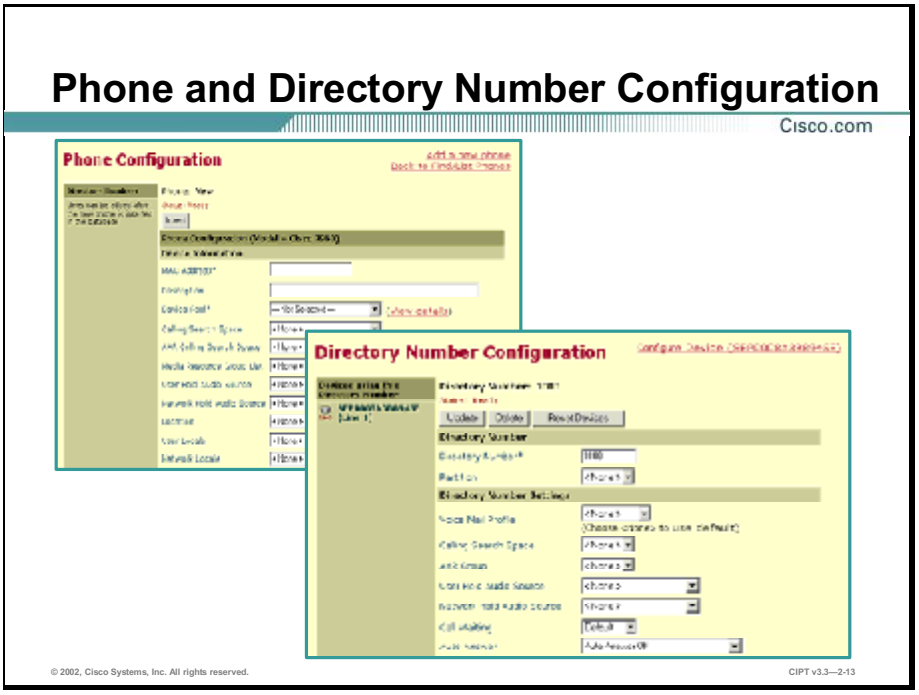
You can rename existing templates and modify them to create new ones. You can also update custom templates to add or remove features, lines, or speed dials. When you update a template, the change affects all of the IP Phones that use it.

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 use this feature to create a copy of an existing template that you can modify.

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 if 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 IP Phone button template.

Manual IP Phone and DN Configuration

This topic discusses manual IP Phone and directory number (DN) configuration in Cisco CallManager Administration.



Manually adding new IP Phones to the network is often tedious, but it can comprise 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 CCM database at once, but BAT is not appropriate for adding or modifying a single IP Phone for a new employee.

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

- You can find the MAC address in the text and usage parameter control (UPC) form, imprinted on the shipping box for the IP Phone. Some administrators use bar code scanners to simplify the process of adding multiple IP Phones.
- You can find the MAC address in the text and UPC form on the back of the IP Phone, on a sticker near the bottom.
- If you boot up the IP Phone, you can press the **Settings** button on the face of the IP Phone. Use the arrow keys to navigate, and choose **Network Configuration**. The MAC address displays on line three of the network configuration.

You can continue the CCM configuration after you have the MAC address of the IP Phone. Perform these steps to configure the IP Phone:

Step 1 In Cisco CallManager Administration, choose **Device** > **Phone**.

Step 2 Open the Find and List Phones Configuration window; 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 list, and click **Next**.

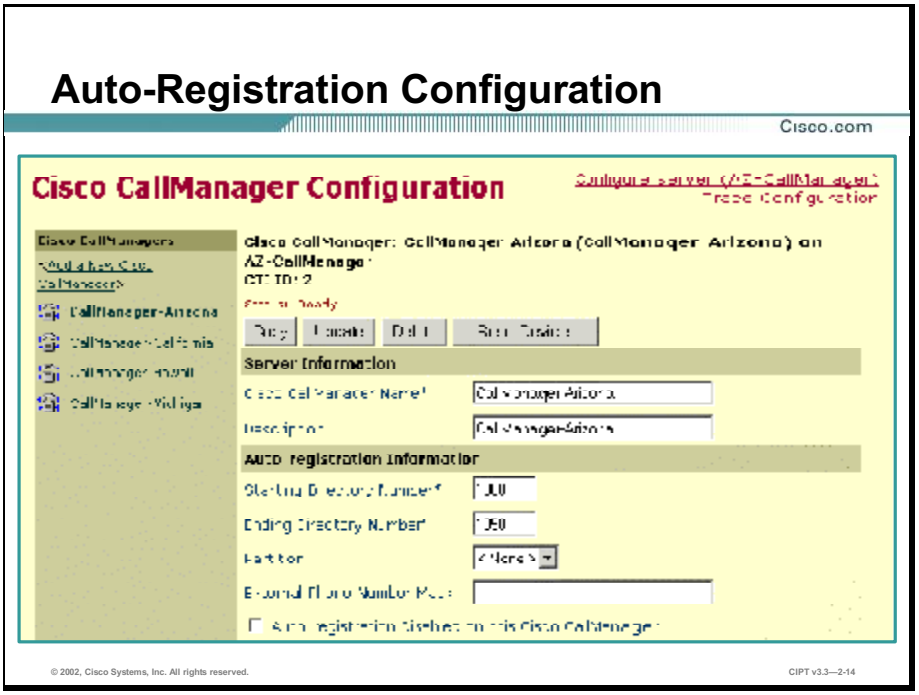
Step 4 At a minimum, you must configure the MAC Address and Device Pool fields, then click **Insert**.

Step 5 CCM prompts you to add a DN for line one, then click **OK**.

Step 6 When the Directory Number Configuration window appears, type the DN of the IP Phone in the appropriate field, and click **Insert**.

Configuring IP Phone Auto-Registration

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



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

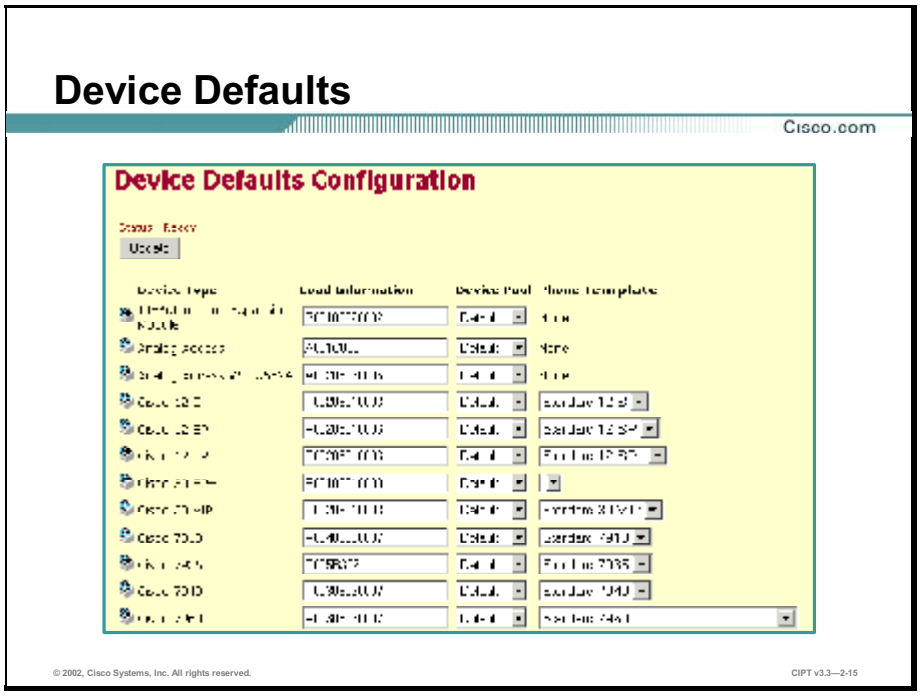
Although auto-registration simplifies the process of deploying a new IP telephony network, it is an option available only in some new IP telephony deployments. Because administrators deploy most IP telephony networks as a migration from a PBX environment, users have existing telephone extensions. These 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 over auto-registration. Perform these steps to configure the CCM server to support auto-registration:

Step 1 From Cisco CallManager Administration, choose **System>Cisco CallManager**.

Step 2 From the column on the left, select the CCM server that you want to support auto-registration.

Step 3 Under the Auto-registration Information Configuration section, type 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.



When devices auto-register in a CCM cluster, they use the Device Default Configuration window. The Load Information field provides the firmware version for the devices; the Device Pool field provides the configuration information, and the Phone Template field provides the correct IP Phone button template for the Cisco IP Phones.

If devices auto-register and are not registering to the intended CCM, check the device defaults window to ensure that you have chosen the correct device pool.

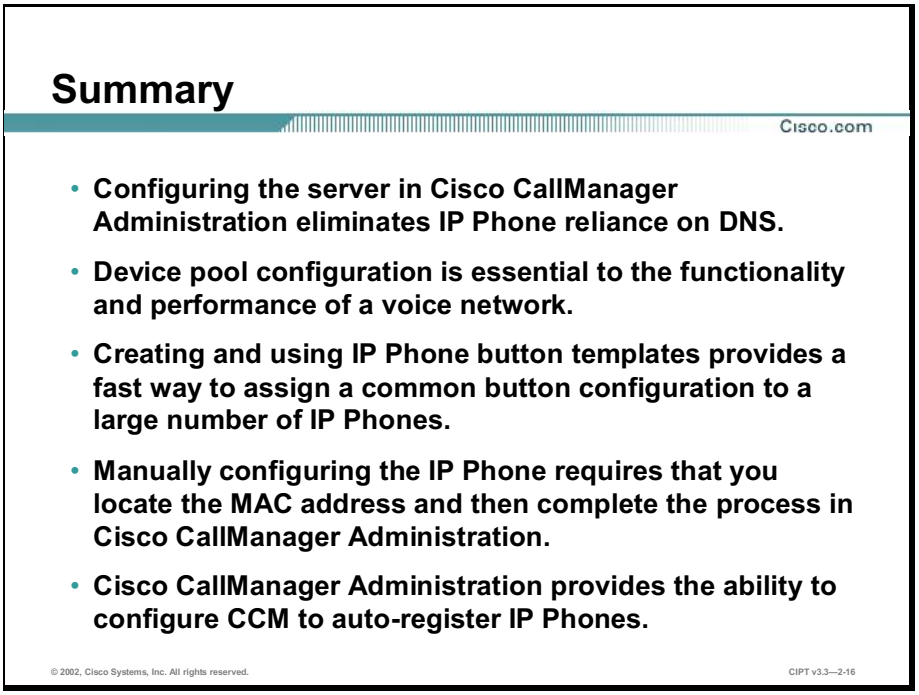
Perform these steps to confirm the device auto-registration setup:

Step 1 In Cisco CallManager Administration, choose **System**>**Device Defaults** to open the device Defaults Configuration window.

Step 2 Scroll to the Cisco IP Phone device or devices that will auto-register, and select the device pool from the drop-down list.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Cisco Catalyst Switches lesson

References

For additional information, refer to these resources:

- *Cisco IP Telephony Network Design Guide:* http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network
- *Cisco IP Telephony Quality of Service (QoS) Design Guide:* http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos
- Johnathan Davidson.*Voice over IP Fundamentals*. San Jose, California: Cisco Press; 2000, ISBN: 1-57870-168-6
- Anne Smith, Chris Pearce, Delon Whetton, John Alexander. *Cisco CallManager Fundamentals: A Cisco AVVID Solution.* San Jose, California, Cisco Press; 2001, ISBN: 1-58705-008-0

- Kelly McGrew, Steve McQuerry. *Cisco Voice over Frame Relay (VoFR), ATM (VoATM), and VoIP*. San Jose, California: Cisco Press, ISBN: 1-57870227-5

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which setting is NOT required for a device pool?

A) media resource group list

B) CCM group

C) date/time group

D) region

Q2) How does CCM tie configuration information to the IP Phones in the Microsoft SQL database?

A) with an IP address

B) through a unique GUID

C) with a hostname

D) none of the above

Q3) Which IP Phone button template is the default for a Cisco IP Phone 7960?

A) 1 line, 5 speed dials

B) 2 lines, 4 speed dials

C) 3 lines, 3 speed dials

D) 6 lines, 0 speed dials

Q4) Terry is a network administrator for ATTC Inc. Terry wants to configure the Cisco IP telephony network to use only the G.729 codec. Outline the general steps that Terry needs to take to complete this process. Use a minimum number of steps to complete the process.

Q5) What do you choose to view the area of Cisco CallManager Administration that eliminates DNS reliance by changing the CCM server name to an IP address?

A) **System**>**Server**

B) **System**>**Cisco CallManager**

C) **Service**>**Service Parameters**

D) **Device**>**Phone**

Cisco Catalyst Switches

Overview

This lesson describes the Cisco Catalyst switch models in an IP telephony solution. This lesson will teach you to use the Cisco Catalyst switch models that support powering Cisco IP Phones, powering single-port multiple VLANs, and extending class of service (CoS) to a Cisco IP Phone. You will also learn the fundamentals of configuring a Cisco Catalyst switch.

Importance

This lesson provides information about how to identify Cisco Catalyst switch models that provide power to the IP Phone, how to configure multiple VLANs on a single port, and how to extend CoS so that voice packets have priority on the network. This configuration allows you to support a single port to the desktop to save on wiring cost.

Objectives

Upon completing this lesson, you will be able to:

- Identify the Cisco Catalyst switches used in a Cisco IP telephony solution
- Identify how Cisco Catalyst switch models supply power to the IP Phones
- Describe the options for powering Cisco IP Phones
- Configure dual VLANs on a single port on a Cisco Catalyst switch
- Configure CoS on the Cisco Catalyst switch models to extend to the device beyond the Cisco IP Phone so that voice packets have priority over data packets

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- VLAN routing and configuration
- TCP/IP networking skills

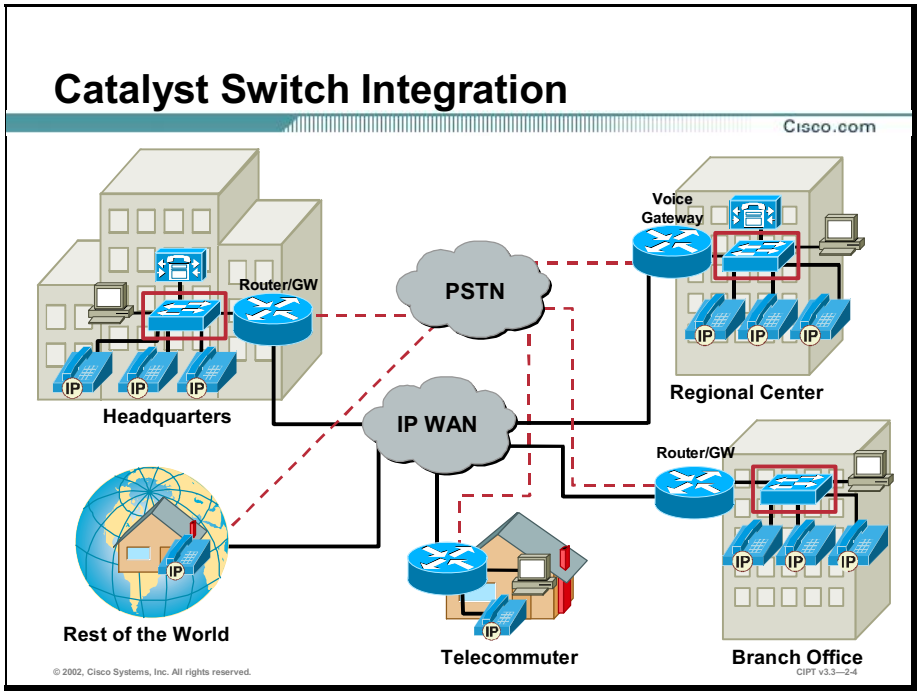
Outline

This lesson includes these topics:

- Overview
- IP Telephony Infrastructure
- Cisco Voice over IP Catalyst Switch Models
- Powering the Cisco IP Phone
- Dual VLAN Configuration
- Configuring CoS
- Summary
- Lesson Review

IP Telephony Infrastructure

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



Cisco Catalyst switches play a key role in your IP telephony rollout. Upgrading the network infrastructure to switches, which support voice features, is often beneficial when dealing with issues such as quality of service (QoS) or powering your Cisco IP Phones.

Cisco voice-capable switches support three primary feature sets that can assist you with your IP telephony deployment:

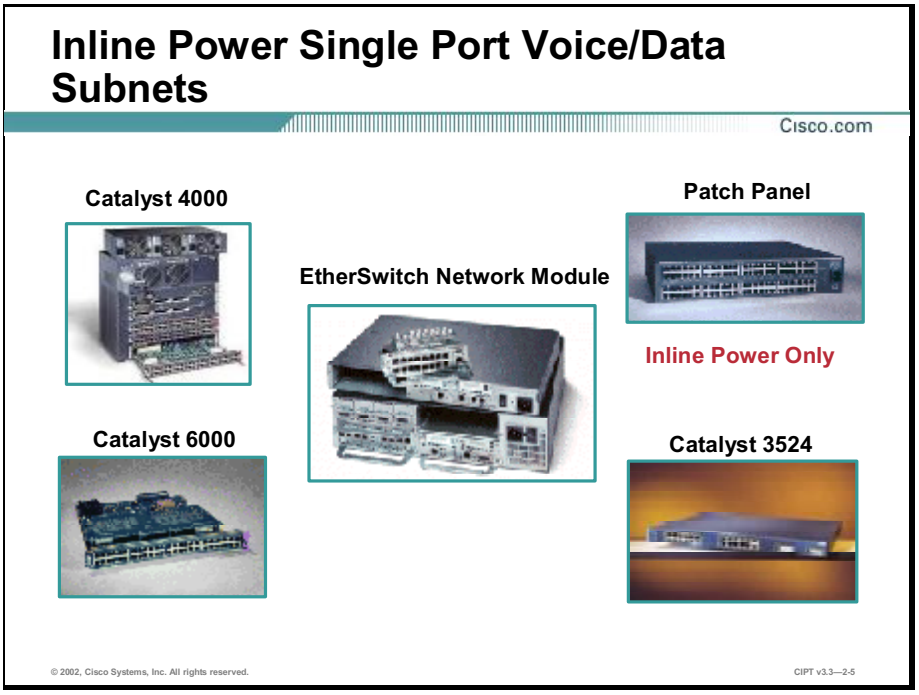
- **Inline power:** Inline power capabilities allow a Cisco Catalyst switch to send -48 VDC of power through Category 5 cable pins 1, 2, 3, and 6. The switch can now power the Cisco IP Phone or other inline-power compatible devices (such as wireless access points) without the need for an external power supply.

- **Auxiliary VLANs:** 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 attached through the IP Phone, on separate VLANs.

- **Class of service (CoS):** CoS is a data link layer (Layer 2) marking and allows you to prioritize certain traffic types over other traffic types. This feature is critical in IP telephony networks. Data traffic can easily overwhelm voice traffic, causing poor voice quality. You can achieve end-to-end prioritization of your voice traffic by using CoS markings along with type of service (ToS) markings at the network layer (Layer 3).

Cisco Voice over IP Catalyst Switch Models

This topic identifies the Cisco Voice over IP (VoIP) Catalyst switch models that support inline power and multiple VLANs on a single port.



This family of inline power switches extends the Cisco IP telephony networking capabilities of the Catalyst backbone to the enterprise wiring closet and branch office. The inline-power Fast Ethernet module enables the modular wiring closet infrastructure to provide centralized power for Cisco IP telephony networks. The module prepares the network infrastructure for IP-based converged business applications, which provide seamless communications and collaboration between branch and corporate sites. Some of these switches support single-port multiple VLANs (voice and data subnets) while providing inline power. Here is a description of these inline power switches:

- **Catalyst 4000 series switch**: The inline power 10/100BaseT Ethernet switching module supports up to 48 ports per module (RJ-45 interfaces). These modules support autosensing and/or autonegotiation, along with telephone discovery to determine the speed and duplex mode of the attached device. The Catalyst 4003 Ethernet switch uses the Catalyst inline-power patch panel to provide inline power. The Catalyst 4006 Ethernet switch provides inline power with support for up to 240 multiservice ports. Cisco developed a new auxiliary direct current (DC) power shelf to support the new demand for IP Phone power on the Catalyst 4006 Ethernet switch. This power shelf supplies the Catalyst Ethernet 4006 switch with the 48 Vdc needed for inline power. The Catalyst 4500 chassis will support inline power without additional power supplies.

- **Catalyst 6000 series switch:** Cisco uses the Catalyst 6000 series switch to lead its customers to campus convergence. Fast Ethernet enhancements, delivered by the new 48-port inline power 10/100BaseT Ethernet switching module, are the first product features introduced. The new Fast Ethernet modules support the inline power feature, which is 48-VDC power, provided over standard Category 5 unshielded twisted-pair (UTP) cable up to 100 meters (m). Terminal devices, such as IP Phones, utilize power provided from the Catalyst 6000 series switch instead of using wall power. This capability gives you centralized power control, which translates into greater network availability. You can ensure that building power outages will not affect network telephony connections by deploying the Catalyst 6000 series switches with uninterruptible power supply (UPS) systems in secured wiring closets.

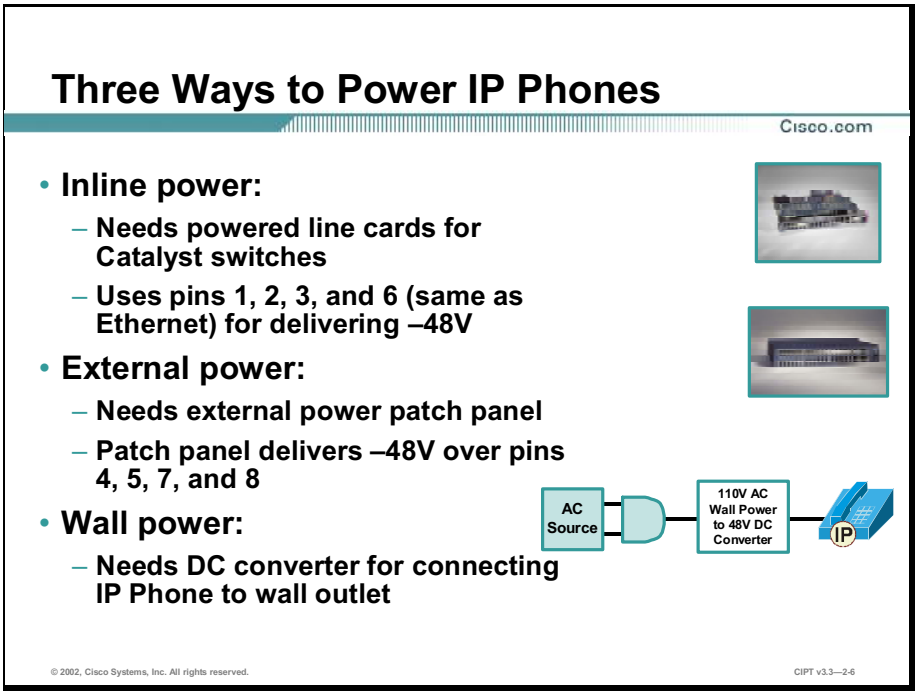
- **Catalyst 3524-PWR XL Ethernet switch:** The Catalyst 3524-PWR XL Ethernet switch has 24 10/100 switched ports with integrated inline power and two Gigabit Interface Converter (GBIC)-based Gigabit Ethernet ports. Integrated inline power provides DC to devices that can accept power over traditional UTP cabling, for example, Cisco 7900 family of IP Phones. The dual GBIC-based Gigabit Ethernet implementation provides customers with tremendous deployment flexibility. This flexibility currently allows customers to implement one type of stacking and uplink configuration, while preserving the option to migrate that configuration in the future.

- **Patch panel:** The Catalyst inline-power patch panel enables inline power for Cisco multiservice enabled Catalyst switches. This product supports a new feature called inline power. Inline power is 48-VDC power provided over standard Category 5 UTP cable up to 100m. Terminal devices, such as IP Phones, can utilize power provided from the Catalyst inline-power patch panel instead of requiring wall power. This capability gives you centralized power control, which translates into greater network availability. You can ensure that building power outages will not affect network telephony connections by deploying Catalyst gear with UPS systems in secured wiring closets.

- **16-Port 10/100 Ethernet Switch Module for Cisco 2600/3600 Routers:** This network module offers branch office customers the option to integrate switching and routing in a single platform. The Cisco EtherSwitch network module has 16 10/100 switched Ethernet ports, with options for inline power and a single Gigabit Ethernet port. In order to supply inline power, the network module requires a daughter-card and an external power supply, which attaches directly to the module using a custom cable. The EtherSwitch network module also supports QoS configurations and VLANs using the 802.1P and 802.1Q standards.

Powering the Cisco IP Phone

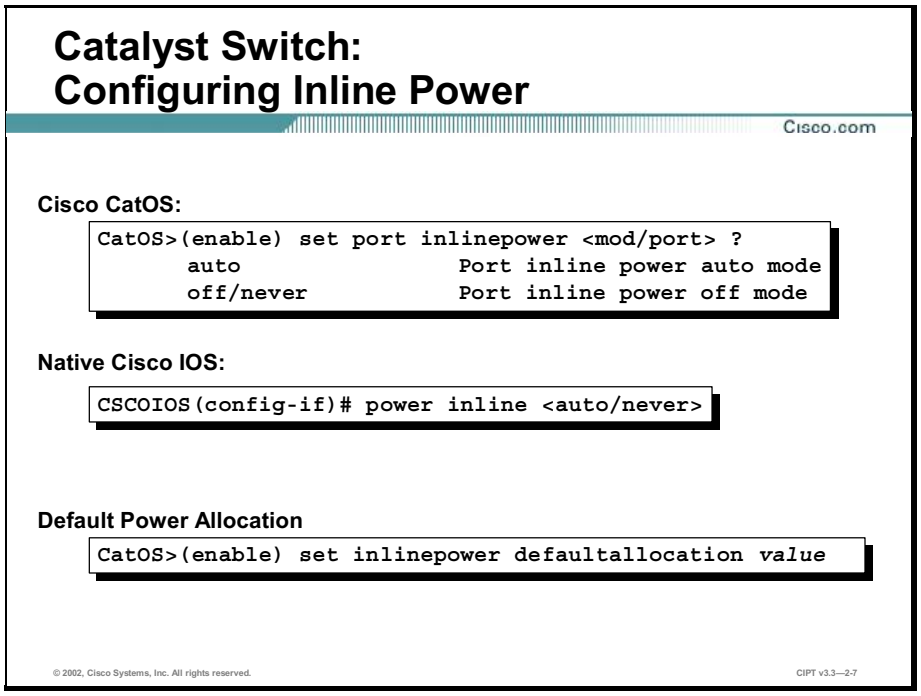
This topic describes the options for powering Cisco IP Phones.



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

- Inline power
  - Inline power needs powered line cards for the Catalyst switches.
  - The Catalyst will use pins 1, 2, 3, and 6 (same as Ethernet) for delivering –48V.
- External power
  - External power needs an external power patch panel.
  - The patch panel delivers –48 V over pins 4, 5, 7, and 8.
- Wall power
  - Wall power needs a DC converter for connecting to a wall outlet.

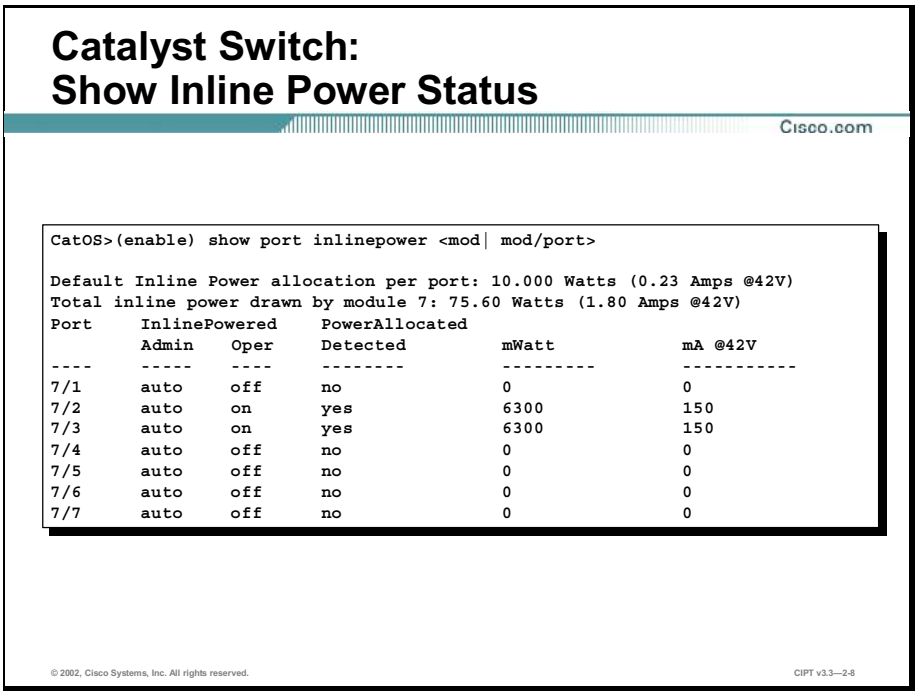
Note	You must order the wall power supply separately for the Cisco IP Phone.



Use the Cisco Catalyst software command syntax to set a port to provide inline power on the Cisco Catalyst 6000 and 4000 series switches. Use the native Cisco IOS command syntax to provide inline power on an interface for the Catalyst 2900 series XL switch and the Catalyst 3524 switch.

The two modes are either “auto” or “off/never.” The telephone-discovery algorithm is operational in the “auto” mode. The telephone-discovery algorithm is disabled in the “off/never” mode.

The Catalyst 4000 and 3524 switches have enough power to supply all of their ports, so only Catalyst 6000 series switches track the allocation of power to the IP Phone. Use the default power allocation command shown in the figure to supply 7 watts (W) of power to an IP Phone instead of the default setting of power (10W) on the Catalyst 6000 series switches.



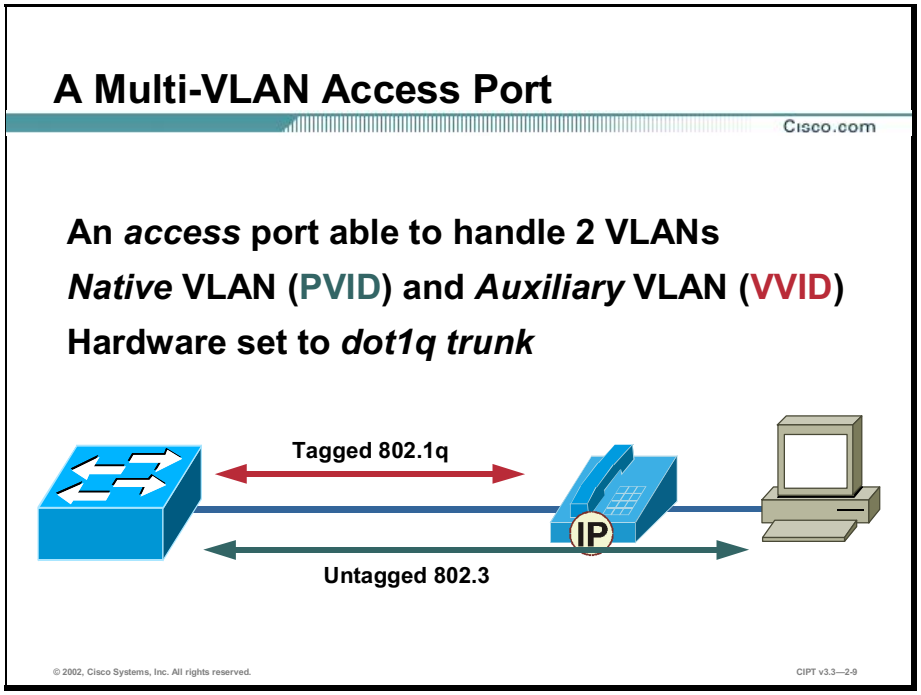
Use the command in the figure shown here to display a view of the power allocated on Catalyst 6000 series switches. The switch shows the default allocated power as 10W in addition to the inline power status of every port. The Inline Power Syntax Descriptions table provides a brief description of the syntax output.

Table: 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]**
Oper	Identifies if the inline power is operational
Power Allocated	
Detected	Identifies if power is detected
mWatt	Identifies the mW supplied on a given port
mA @42V	Identifies the mA @ 42 V supplied on a given port

Dual VLAN Configuration

This topic describes the concept and 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 Catalyst software command-line interface (CLI) refers to this new voice VLAN as the auxiliary VLAN for configuration purposes. You can use the new auxiliary VLAN to represent other types of devices. Currently, the device is an IP Phone, so you can think of it as a voice VLAN. In the future, other types of nondata devices will reside in the auxiliary VLAN.

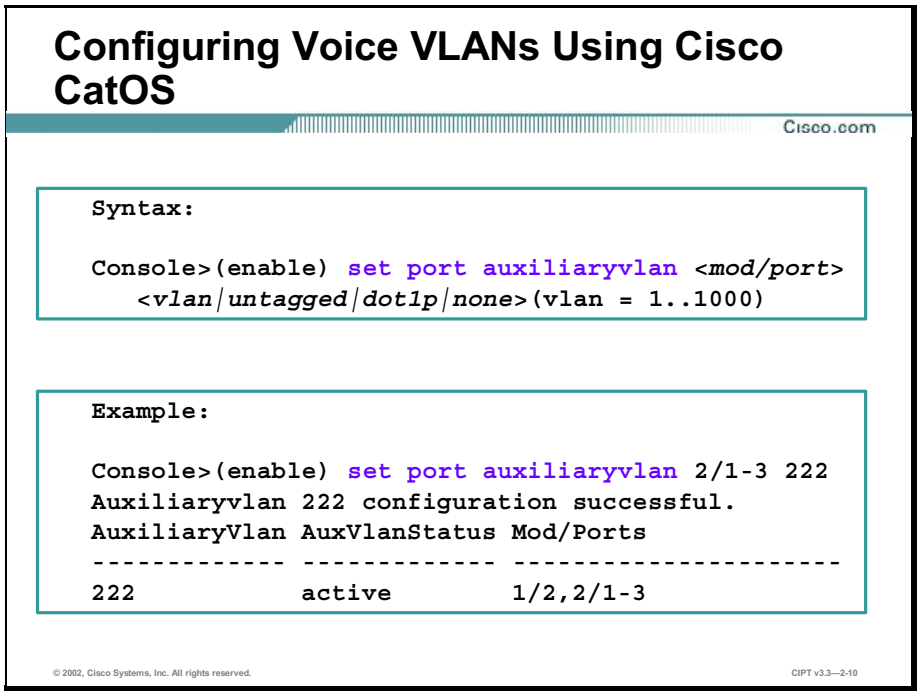
These nondata devices (such as IP Phones) should reside in a separate VLAN (auxiliary VLAN), which will make it easier for customers to automate the process of deploying IP Phones. IP Phones will boot up and reside in the auxiliary VLAN if you configure the switch to support them, just as data devices come up and reside in the native VLAN (also referred to as the default VLAN) of the switch. The IP Phone communicates with the switch via Cisco Discovery Protocol (CDP) when it powers up. The switch will provide the telephone with the appropriate VLAN ID, known as the Voice VLAN ID (VVID). This VVID is analogous to the data VLAN ID, known as Port VLAN ID (PVID).

These are some of the advantages of this solution:

- This solution allows 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 an introduction of a large number of new devices, such as IP Phones, in the network without extensive modifications to the IP addressing scheme.

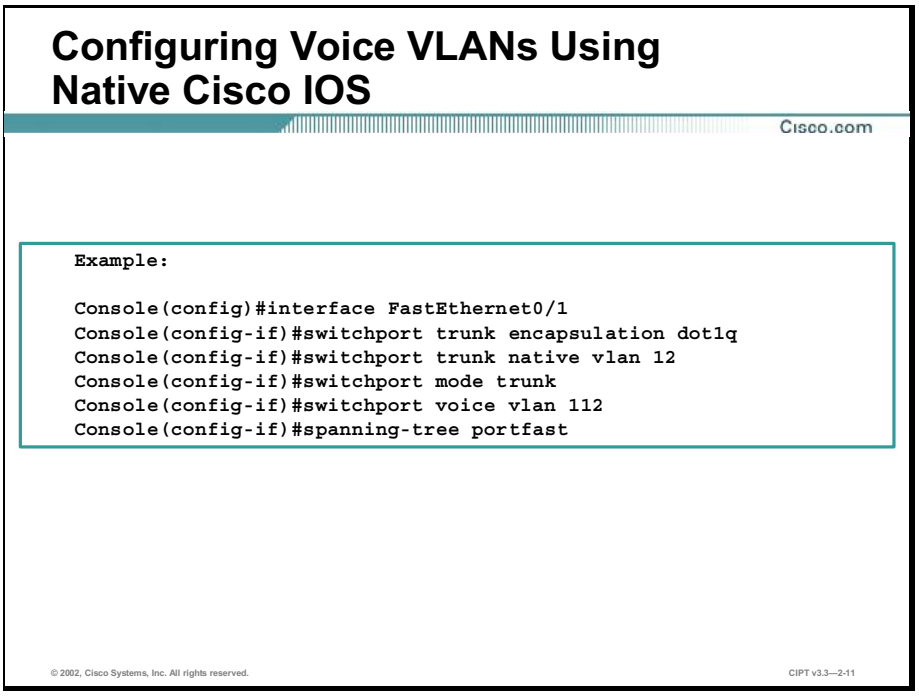
- This solution allows the logical separation of data and voice traffic that have different characteristics. This separation allows the network to individually handle each of these traffic types.

- 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 and/or PC location.

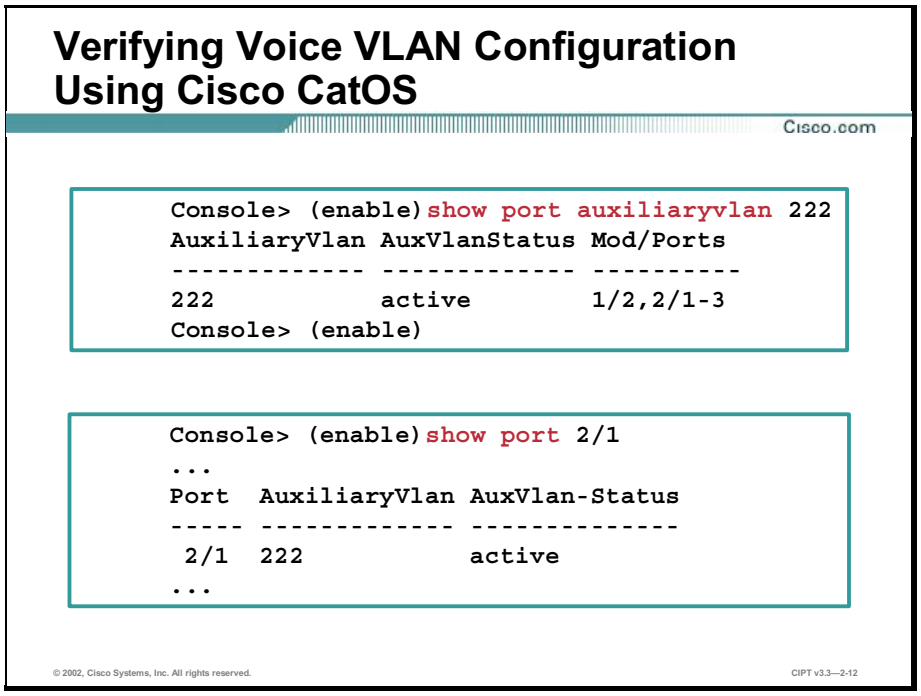


You can configure the VVID in Cisco Catalyst 5.5 and above using the **set port auxiliaryvlan <mod/port>** command.

The VVID 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 VVID on a per port basis, range of ports, or for an entire module.



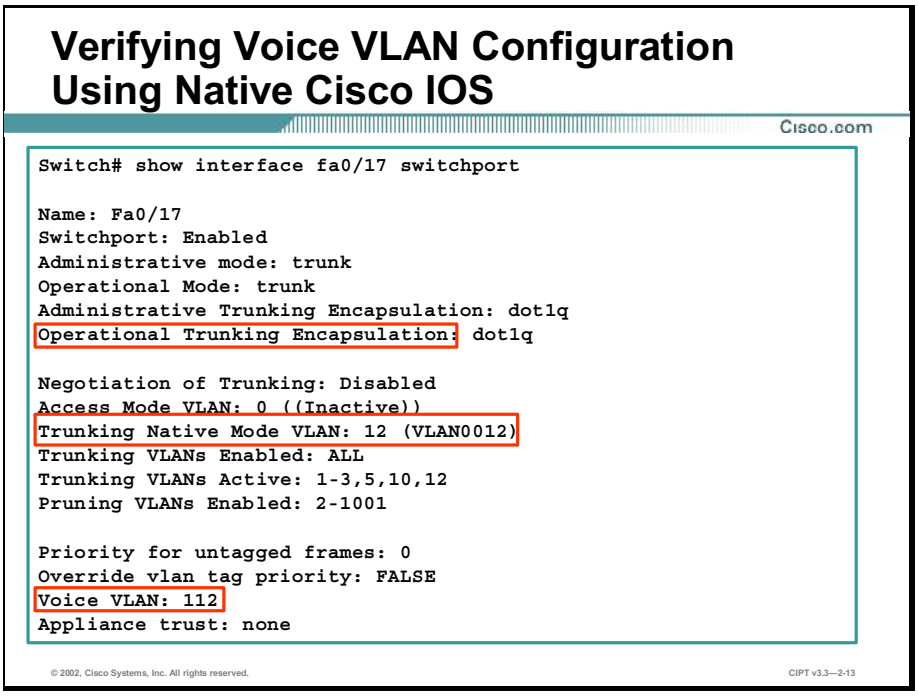
Use the commands in the figure shown to configure the voice and data VLAN on a single-port interface of a Catalyst 3524 switch or Catalyst 2900 XL switch. These commands apply the same functionality as setting a port to use an auxiliary VLAN on a Catalyst 6000 or 4000 switch.



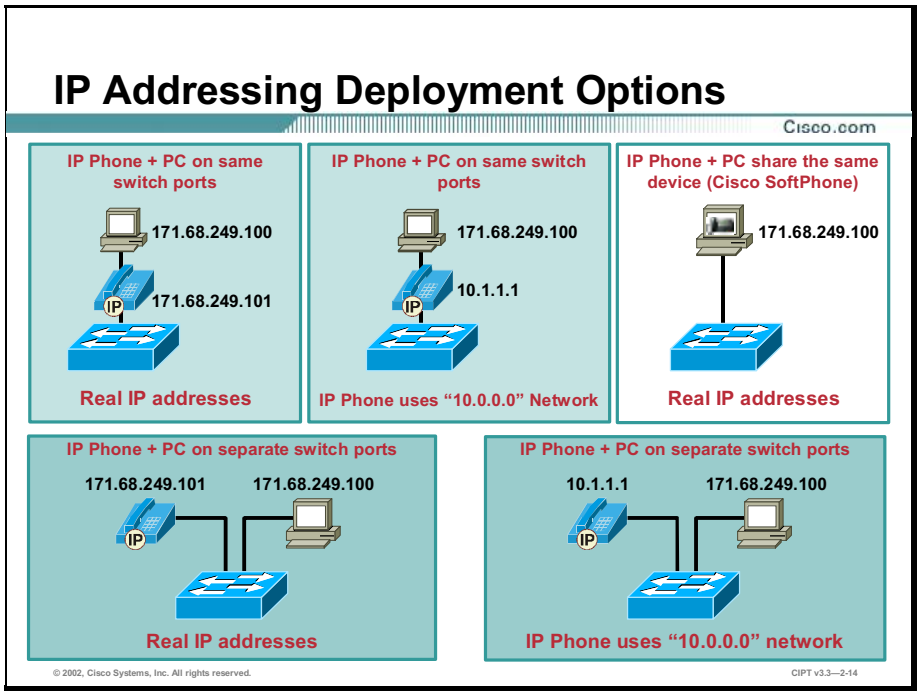
You can check the status of the auxiliary VLAN on a port or module in one of two ways:

- 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.
- 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



You can verify your voice VLAN configuration on the Catalyst 2900 series XL switch and Catalyst 3524 switch by using the **show interface <mod/port> switchport** command. The Catalyst 4000 and 6000 series switches may display a more convenient output, but using this syntax will display the voice and data VLAN configuration on any interface.



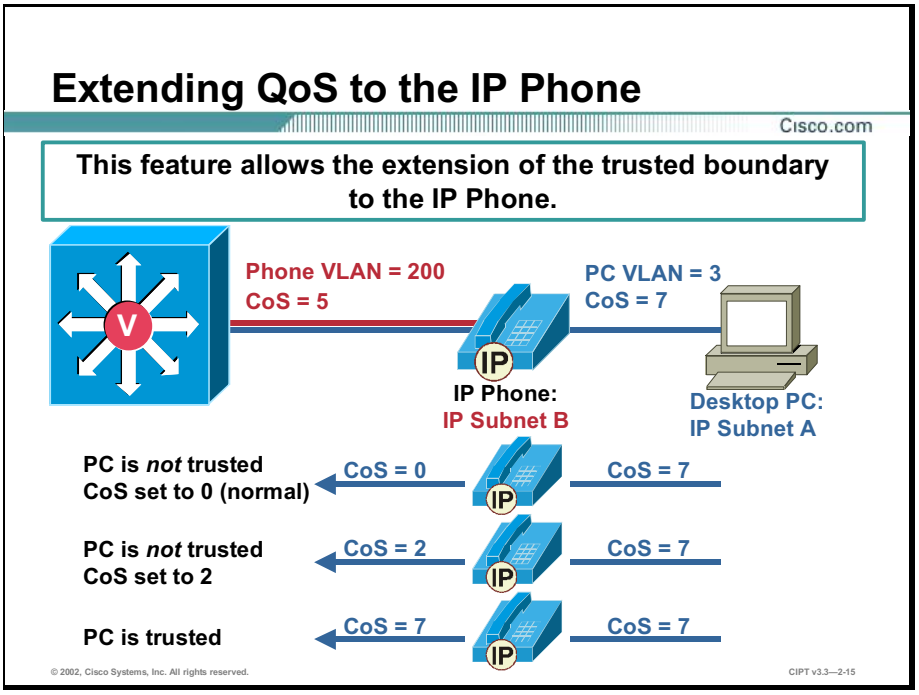
Cisco IP Phones require network IP addresses. Cisco makes the following recommendations for IP addressing deployment:

- Continue to use existing addressing for data devices (PCs, workstations, and so forth).
- Add IP Phones with Dynamic Host Configuration Protocol (DHCP) as the mechanism for obtaining addressees.
- Use subnets for IP Phones if they are available in the existing address space.
- Use private addressing (network 10 or network 172.16 – 172.20) if subnets are not available in existing address space.

LAN and private IP WAN will carry these routes between both of the address spaces. The WAN gateway to the Internet should block private addresses, which data devices currently block.

Configuring CoS

This topic describes configuring the CoS values when a PC and an IP Phone are sharing the same switch port.



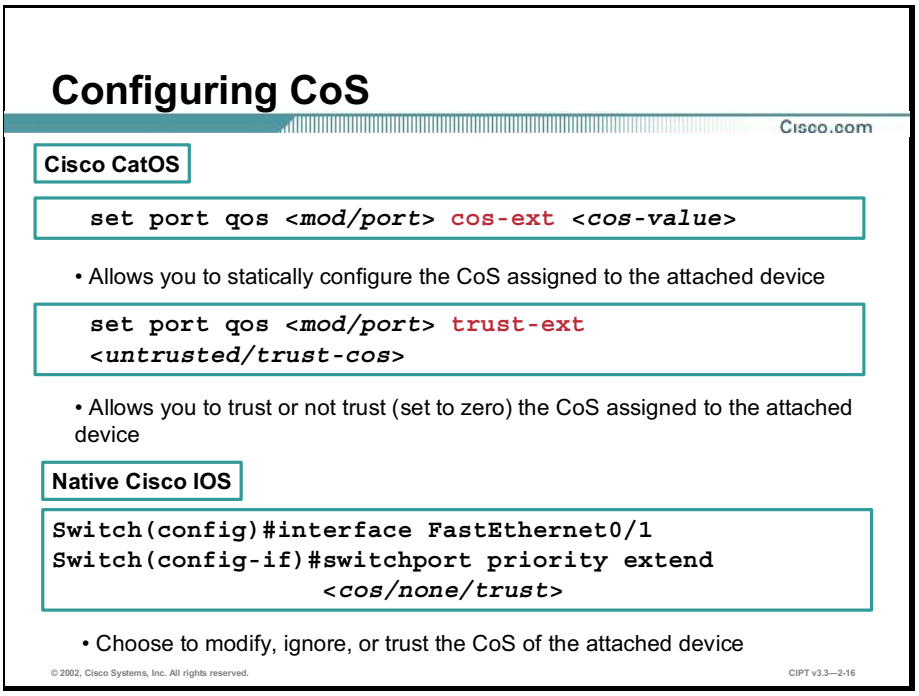
CoS is a data link layer marking that you can use to classify traffic as it passes through a switch. You should ensure that voice traffic has priority as it travels throughout your network because it is extremely sensitive to delay. Cisco IP Phones send all voice packets tagged with CoS 5 by default, which is the highest level of CoS recommended for user traffic. The multi-VLAN port also receives packets from the devices (PC and/or workstation) connected to the access port of the IP Phone. The attached device can send packets with a CoS equal to or higher than the packets sent by the IP Phone, which can cause severe voice quality problems on your IP telephony network.

Catalyst switches have the ability to extend the boundary of trust to the IP Phone. The attached data device (for example, a PC and/or workstation) can set the CoS to any value you determine, as traffic passes from the device through the IP Phone. You can choose not to trust the attached device and set the CoS to zero or set the CoS to a configured value that you determine, or you can trust the attached device and allow the CoS to remain unchanged.

The Catalyst switch uses CDP to send this configuration information to the IP Phone. The switch sends an additional CDP 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 frames before sending them to the switching engine. You use input queuing only when there is congestion. The switch will use the CoS value(s) to place the frames in appropriate queues. CoS 5 frames go into the priority queue, which is serviced before other queues.

Reference	The *Deploying Quality of Service* (DQoS) course provides more information about voice QoS theory and configuration.



You can configure the switch with different QoS settings on a per port basis. Use **set port qos <mod/ports> trust <untrusted|trust-cos>** command from the CLI.

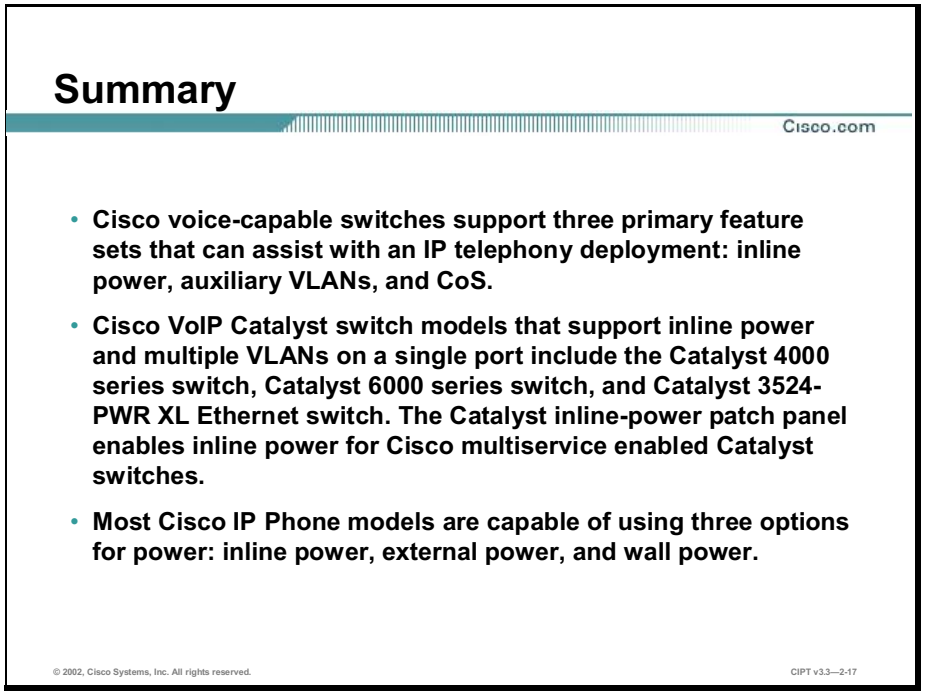
You may want to trust the PC CoS if sending tagged packets or give it a value other than zero. Use the **set port qos 2/1 trust-ext trust-cos** command to extend trust out to the PC.

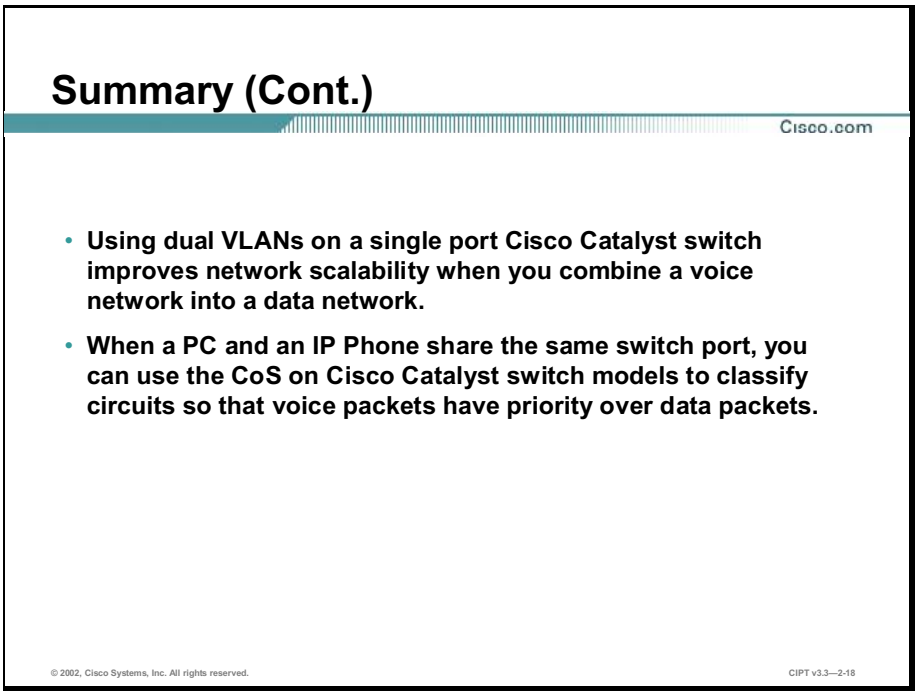
Use the **set port qos 2/1 cos-ext 2** command if you want to set the CoS to 2 on packets that the device, attached to the IP Phone, sends.

Use the other commands shown in the figure to set the trust boundaries if a Catalyst switch uses Cisco IOS; for example, use the commands for the Cisco 3524 switch or the Cisco 2900 series XL switch.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Cisco Access Gateways lesson

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) What is the default CoS value setting of a Cisco IP Phone?

A) CoS = 0

B) CoS = 2

C) CoS = 5

D) CoS = 7

Q2) What is the recommended IP addressing scheme for a Cisco IP telephony solution?

A) The IP Phones and PCs reside on the same port and use real IP addresses.

B) The IP Phones and PCs reside on the same port as the IP Phones and use a 10.0.0.0 network.

C) The IP Phones and PCs reside on the different ports and use real IP addresses.

D) The IP Phones and PCs reside on the different ports, and the IP Phones use a 10.0.0.0 network.

Q3) How much power does a Cisco 7960 IP Phone use without any expansion modules attached?

A) 5W

B) 7W

C) 10W

D) 12W

Q4) Which device does not support a single port with multiple VLANs?

A) Cisco Catalyst 3524 switch

B) Cisco Catalyst 4224 switch

C) Cisco Catalyst 6000 series switch

D) Cisco power patch panel

Q5) Which item is a network layer QoS marking?

A) CoS

B) ToS

C) QoS

D) DoS

Cisco Access Gateways

Overview

This lesson will teach you about the Cisco access gateways in a Cisco IP telephony solution. You will learn about analog and digital gateways, gateway protocols, recommended gateway requirements, and configuration basics for adding a Cisco access gateway to a Cisco IP telephony solution.

Importance

Your IP telephony solution will need a gateway to connect to the Public Switched Telephone Network (PSTN). This lesson provides information about choosing a Cisco access gateway and integrating Cisco gateways in a Cisco CallManager (CCM)-based solution.

Objectives

Upon completing this lesson, you will be able to:

- Describe the IP telephony infrastructure
- Compare analog and digital gateways
- Describe common access gateways
- Identify and describe gateway protocols
- Describe core gateway requirements

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- General navigation in Cisco CallManager Administration
- Prerequisite Cisco Voice over Frame Relay, ATM, and IP (CVOICE) course or equivalent experience

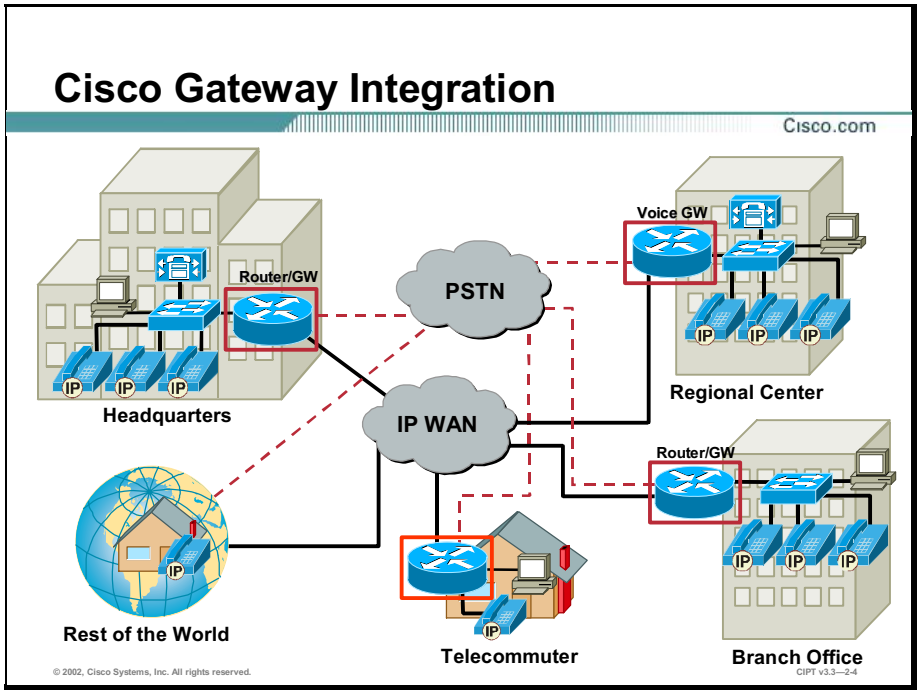
Outline

This lesson includes these topics:

- Overview
- IP Telephony Infrastructure
- Analog Versus Digital
- Cisco Access Gateways
- Gateway Protocols
- Core Gateway Requirements
- Summary
- Lesson Review

IP Telephony Infrastructure

This topic introduces the importance of Cisco access gateways in the overall design of the IP telephony infrastructure.

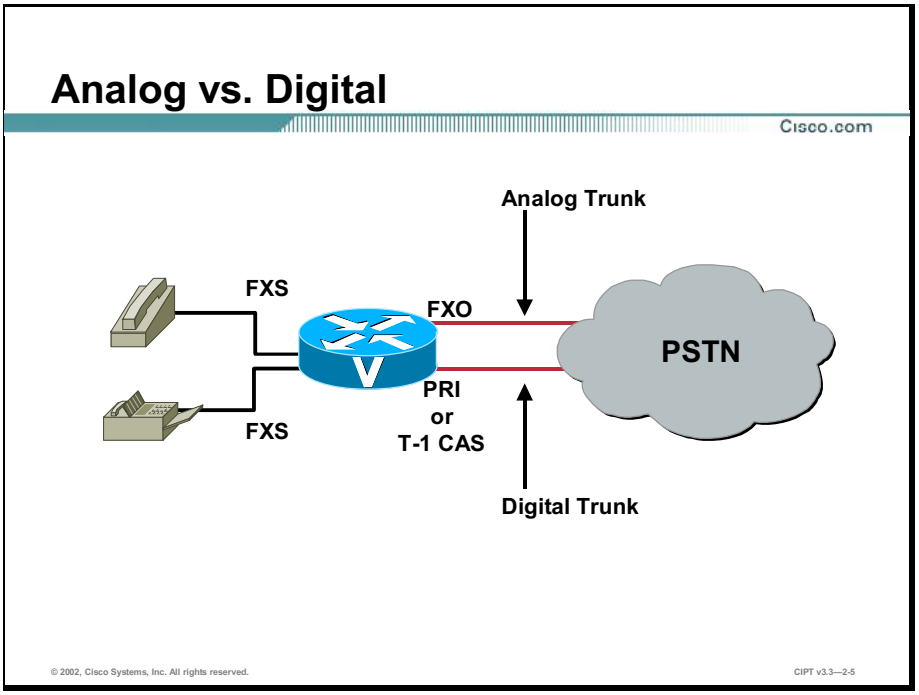


When you are designing an IP telephony solution, it is important to choose and configure the correct gateway. These gateways are the routers that bind the discontinuous pieces of your network into a fully operational system. Voice gateways provide a path to reach other voice networks, including H.323-based voice networks, individual analog devices (for example, fax machines or legacy telephone equipment), or the Public Switched Telephone Network (PSTN).

Note This lesson provides an overview of the voice gateways that you can use with the Cisco CallManager (CCM) system. For information on configuring the voice gateways, refer to the *Cisco Voice over IP, Frame Relay, and ATM (CVOICE)* course.

Analog Versus Digital

This topic describes analog and digital access gateways.

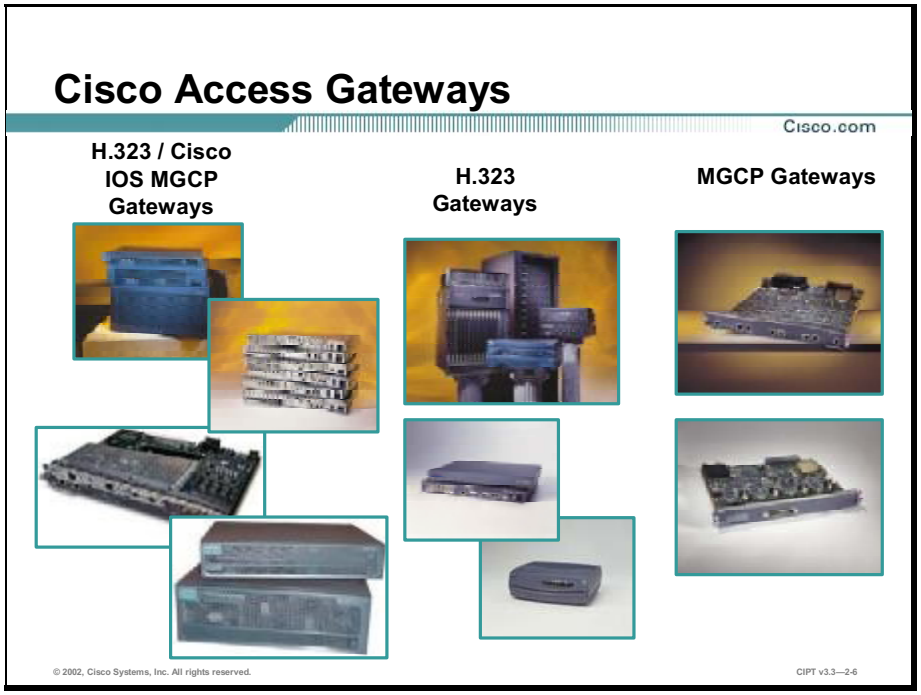


There are two types of Cisco access gateways: analog and digital. Here is a description of these gateways:

- **Cisco access analog gateways:** There are two categories of Cisco access analog gateways:
  - **Access analog station gateways:** Access analog station gateways connect CCM to plain old telephone service (POTS) analog telephones, interactive voice response (IVR) systems, fax machines, and voice-mail systems. Station gateways also provide Foreign Exchange Station (FXS) ports.
  - **Access analog trunk gateways:** Access analog trunk gateways connect CCM to PSTN central office (CO) or PBX trunks. Trunk gateways provide Foreign Exchange Office (FXO) ports for PSTN or PBX access and recEive and transMit (E&M) ports for analog trunk connection to a legacy PBX. To minimize any answer and disconnect supervision issues, use digital gateways when possible. Analog Direct Inward Dialing (DID) is also available for PSTN connectivity.
- **Cisco access digital trunk gateways:** A Cisco access digital trunk gateway connects CCM to the PSTN or to a PBX via digital trunks, such as PRI or T1 channel-associated signaling (CAS). Digital T1 PRI trunks may also connect to certain legacy voice-mail systems.

Cisco Access Gateways

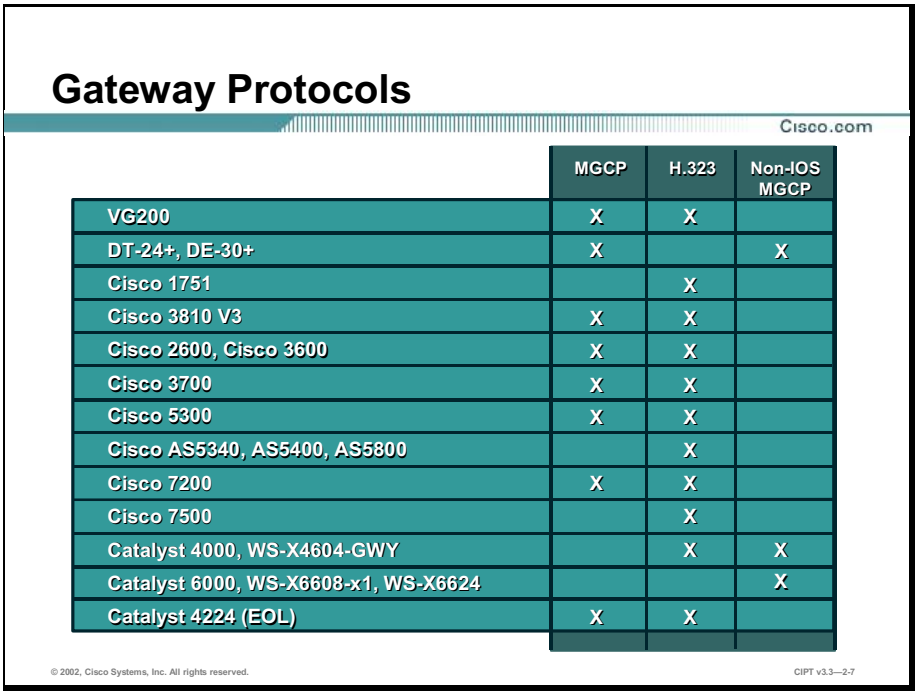
This topic highlights the Cisco access gateways used in a Cisco IP telephony solution.



This figure shows the most common Cisco access gateways. You can group these gateways into analog and digital categories or by the protocols used to communicate with CCM.

Gateway Protocols

This topic describes the gateway protocols that Cisco access gateways support.



CCM 3.0 and greater support these three types of gateway protocols:

- **H.323:** Peer-to-peer protocol, with voice-routing intelligence residing in the gateway
- **Media Gateway Control Protocol (MGCP):** Server/client protocol, with voice-routing intelligence residing in CCM
- **Non-IOS MGCP:** Server/client protocol, with voice-routing intelligence residing in CCM

Cisco IP Phones and integrated switch gateways, such as the Catalyst 6000 gateway modules, allow you to use a lighter weight protocol, MGCP. MGCP and Non-IOS MGCP use a master or slave model, where the voice-routing intelligence resides in CCM. The H.323 gateways utilize a peer-to-peer model where the voice-routing intelligence resides in the gateway. This model offers more redundancy if CCM connection is lost, but it requires a more complicated configuration.

Selecting the protocol to use depends on site-specific requirements and the installed base of equipment for the customer; for example, most remote branch locations have Cisco 1750, 2600, or 3600 series routers installed. These routers support H.323. With Cisco IOS software release 12.2(XA) and CCM 3.05(a) or later, the Cisco 2600 and 3600 series products support MGCP for analog FXS and/or FXO interfaces. A future release will provide CCM 3.1, MGCP support for T1 CAS, and T1/E1 PRI on the Cisco 2600 and 3600 series. The figure shown here provides a summary of the protocols supported by the different Cisco access gateways.

For an analog gateway configuration, you may prefer MGCP to H.323 due to its simpler configuration or support for call survivability during a CCM switchover from a primary to a secondary CCM. In other gateway configurations, you may prefer H.323 to Non-IOS MGCP or MGCP because of the robustness of the interfaces supported.

The Supported Gateway Protocols and Cisco IP Telephony Gateway table shows a detailed list of the gateways and the protocols that they support.

Table: Supported Gateway Protocols and Cisco IP Telephony Gateway

Gateway	MGCP	H.323	Non-IOS MGCP
VG200	Yes, supported with FXS and/or FXO T1 CAS with CCM 3.1 and Cisco IOS software release 12.2.XN* (E&M Wink Start and Delay Dial only)	Yes, supported with Cisco IOS software release 12.1(5)XM1. The VG-200 uses H.323 to support a wider range of digital and analog interfaces.	No
DE-30+, DT-24+	Yes, supported with CCM 3.1	No	Yes
Cisco 827	No	Yes, supported with FXS	No
Cisco 1751	Future support with Cisco IOS 12.2.7T	Yes	No
Cisco 3810 V3	Yes, supported with Cisco IOS software release 12.1(3)T and CCM 3.0(5)	Yes	No
Cisco 2600	Yes, supported with 12.2(XA) and CCM 3.0(5) FXO interfaces only, no E&M interface T1 CAS/T1/E1 PRI - Cisco IOS software release 12.2.9T** Q.931 PRI Backhaul – Cisco IOS software release 12.2.9T**	Yes	No
Cisco 3600	Yes, supported with 12.2(XA) and CCM 3.0(5) FXO interfaces only, no E&M support T1 CAS/T1/E1 PRI - Cisco IOS software release12.2.9T** Q.931 PRI Backhaul – Cisco IOS software release12.2.9T**	Yes	No
Cisco 3700	Yes, supported with Cisco IOS software release 12.2T	Yes	No
Cisco 5300***	Yes, supported with Cisco IOS software release 12.1(1)T***	Yes	No
Cisco AS5350*** Cisco AS5400***	Future support***	Yes, supported with Cisco IOS software release 12.1(5)/12.2(2)XA	No
Cisco AS5800	No	Yes	No
Cisco AS5850***	Future support***	Future support	No
Cisco 7200***	Yes, supported with Cisco IOS software release 12.2.(1)T***	Yes	No
Cisco 7500	No	Yes, supported with Cisco IOS software release 12.1.5	No
Catalyst 4000 WS-X4604-GWY Gateway Module	Future support with Cisco IOS software release and Cisco CCM 3.1*	Yes, supported with PSTN interfaces	Yes, supported with conferencing, MTP, and/or transcoding services

Gateway	MGCP	H.323	Non-IOS MGCP
Catalyst 6000 WS-X6608-x1 Gateway Module and FXS Module WS-X6624	Yes, supported with CCM 3.1, T1/E-1 module supporting PRI and CAS and FXS module	No	Yes, with FXS module and T1/E1 prior to CCM 3.1
Catalyst 4224 (End of Life [EOL])	Yes, supported with 12.2.2XN and CCM 3.1*	Yes	No
Cisco ICS7750-MRP	No	Yes	No
Cisco ICS7750-ASI	No	Yes	No

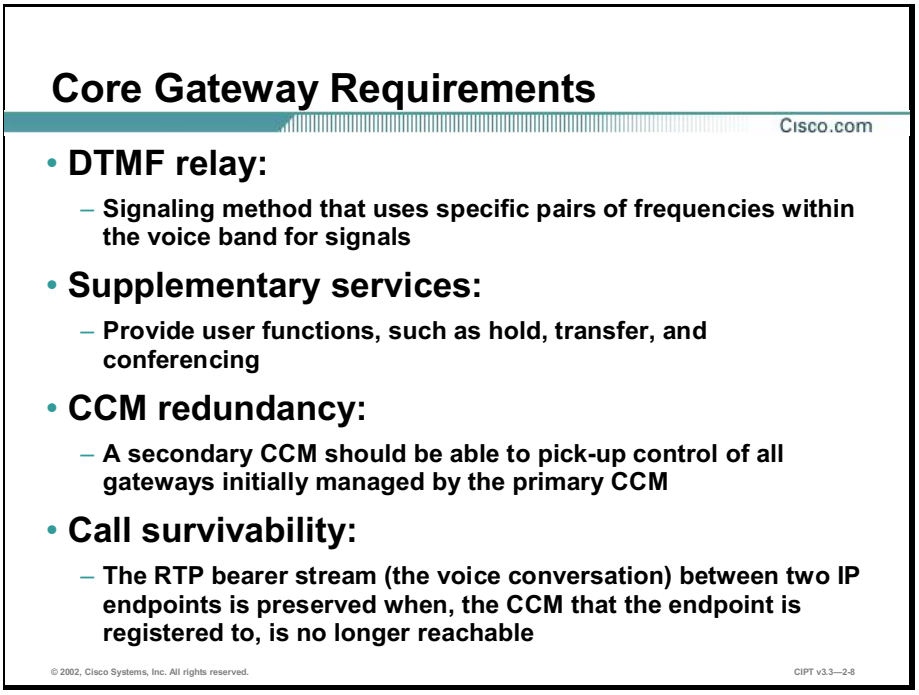
*There is a special Cisco IOS software release attached to CCM 3.1.

**The 12.2.2T PRI backhaul support for Cisco 2600 and 3600 series products uses Reliable User Data Protocol (RUDP) and is not compatible with CCM. CCM 3.1 provides PRI backhaul since the Call Agent is scheduled for Cisco software release 12.2.9T and uses TCP as the transport.

***While the Cisco 5300, Cisco AS5350, Cisco AS5400, CiscoAS5850, and Cisco 7200 supports MGCP, RUDP is used, which is not supported in CCM.

Core Gateway Requirements

This topic provides an overview of the core requirements for a gateway to support an IP telephony network.



The IP telephony gateway selection includes common or core requirements, site, and implementation specific features. IP telephony gateway must meet these core requirements:

- **Dual Tone Multi-Frequency (DTMF) relay capabilities:** DTMF relay capabilities, specifically out-of-band DTMF, separate DTMF digits from the voice stream. It then sends them as signaling indications through the gateway protocol (H.323, Cisco IOS MGCP, and MGCP) signaling channel instead of as part of the voice stream or bearer traffic. The gateway requires out-of-band support when using a low bit rate coder-decoder (codec) for voice compression because the potential exists for DTMF signal loss or distortion.

- **Supplementary services support:** These services are typically basic telephony functions, such as hold, transfer, and conferencing.

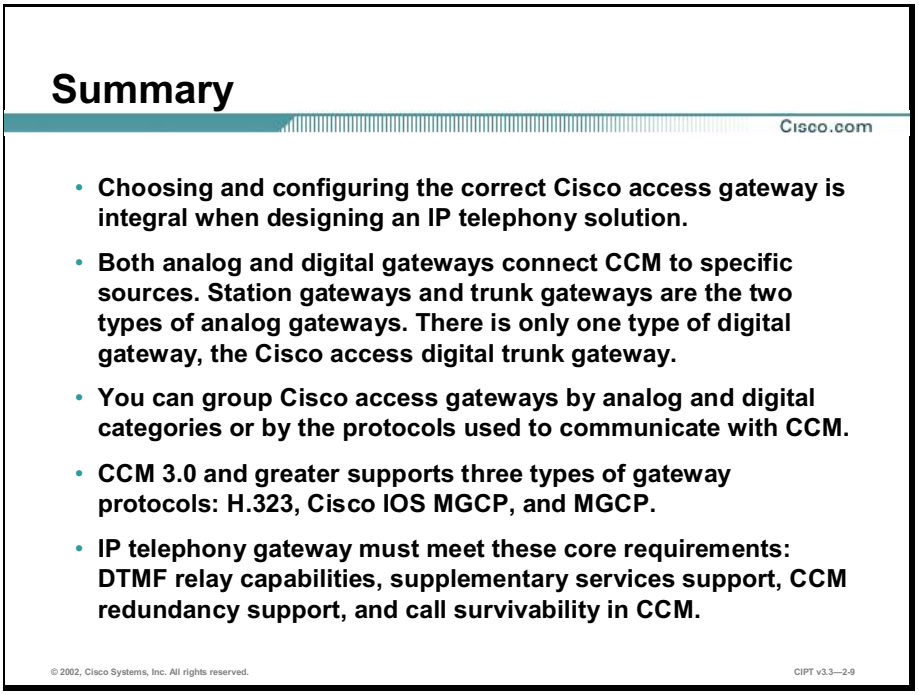
- **CCM redundancy support:** CCM clusters provide for CCM redundancy. The gateways must support the ability to rehome to a secondary CCM in the event of a primary CCM failure, which differs from call survivability in the event of a CCM or network failure.

- **Call survivability in CCM:** The voice gateway preserves the RTP bearer stream (the voice conversation) between two IP endpoints when the CCM that the endpoint is registered to is no longer reachable.

Any IP telephony gateway that you select for an enterprise deployment should support these three core requirements. Additionally, every IP telephony implementation has its own site-specific feature requirements, such as analog or digital access, DID, and capacity requirements.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Route Plan module

References

For additional information, refer to these resources:

- Cisco IP Telephony Gateways Overview: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/config/overvw.htm
- WAN Switching Products website: http://www.cisco.com/warp/public/779/largeent/select_products/wan/WAN_ms.html

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) What type of voice network connects a Cisco access gateway?

A) H.323

B) the PSTN

C) PBX systems

D) all of the above

Q2) What type of interface is on a digital voice gateway?

A) FXO

B) T1

C) E&M

D) FXS

Q3) Which two switch series are capable of supporting a voice network? (Choose two.)

A) Catalyst 1900

B) Catalyst 4000

C) Catalyst 2800

D) Catalyst 6000

Q4) Which two protocol types can the VG200 gateway support? (Choose two.)

A) H.323

B) MGCP

C) Skinny

D) Non-Cisco IOS MGCP

Q5) Which item is a core gateway requirement?

A) support for DTMF relay

B) support for inline power

C) support for multiple VLANs on single port

D) support for disconnect supervision

3

Route Plan

Overview

This module discusses basic and advanced route plan concepts. It also discusses the application of a telephony class of service (CoS) using partitions and calling search spaces in Cisco CallManager (CCM).

Upon completing this module, you will be able to:

- Describe how to create a basic route plan
- Apply advanced route plan components in order to customize a basic route plan
- Configure partitions and calling search spaces in a Cisco IP telephony solution
- Configure CAC and SRST

Outline

The module contains these lessons:

- Route Plan Basics
- Advanced Route Plan
- Telephony Class of Service
- Call Admission Control and Survivable Remote Site Telephony

Route Plan Basics

Overview

This lesson discusses the basics of a route plan within Cisco CallManager (CCM). Basic components of a route plan include route groups, route lists, and route patterns. This lesson provides background knowledge regarding route plans in order for you to better understand the actual flow of a call, as it is routed throughout a Cisco IP telephony network.

Importance

In order to successfully implement and/or support a Cisco IP telephony environment, you must be able to configure CCM to route internal and external calls appropriately.

Objectives

Upon completing this lesson, you will be able to:

- Describe the necessary elements for creating external route plans
- Describe the devices used when implementing route plans
- Describe route groups
- Create route lists
- Create route patterns
- Describe the CCM digit analysis process
- Describe a basic route plan

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

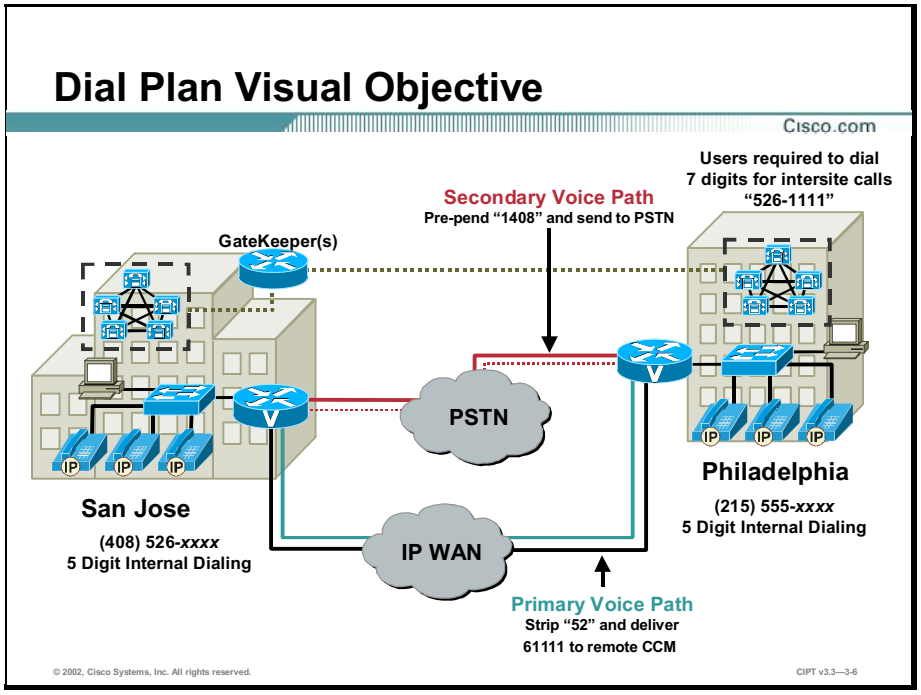
- Familiarity with the North American Dialing Plan
- Familiarity with Cisco IOS

Outline

This lesson includes these topics:

- Overview
- External Call Routing
- Devices
- Route Groups
- Route Lists
- Route Pattern
- Digit Analysis
- Call Routing Summary
- Summary
- Lesson Review

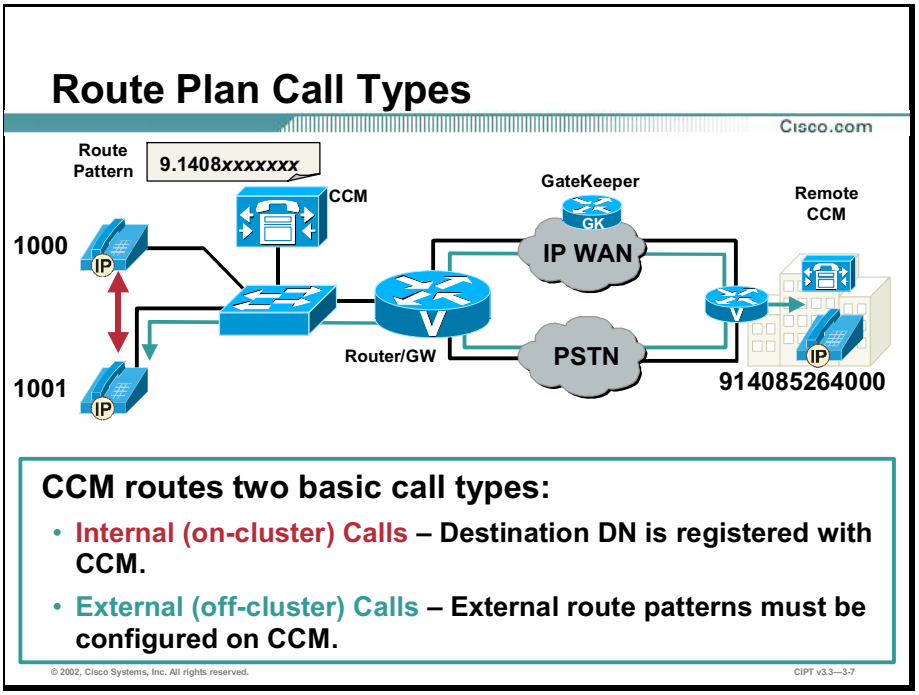
Visual Objective



The figure shown depicts the goal of a well-designed route plan. In this scenario, the caller does not know whether the CCM uses toll bypass and routes the call across the IP WAN or uses Public Switched Telephone Network (PSTN) Fallback to route the call over the PSTN (because the IP WAN is unavailable for some reason). You should complete route plan design before you create the actual route plan configuration.

External Call Routing

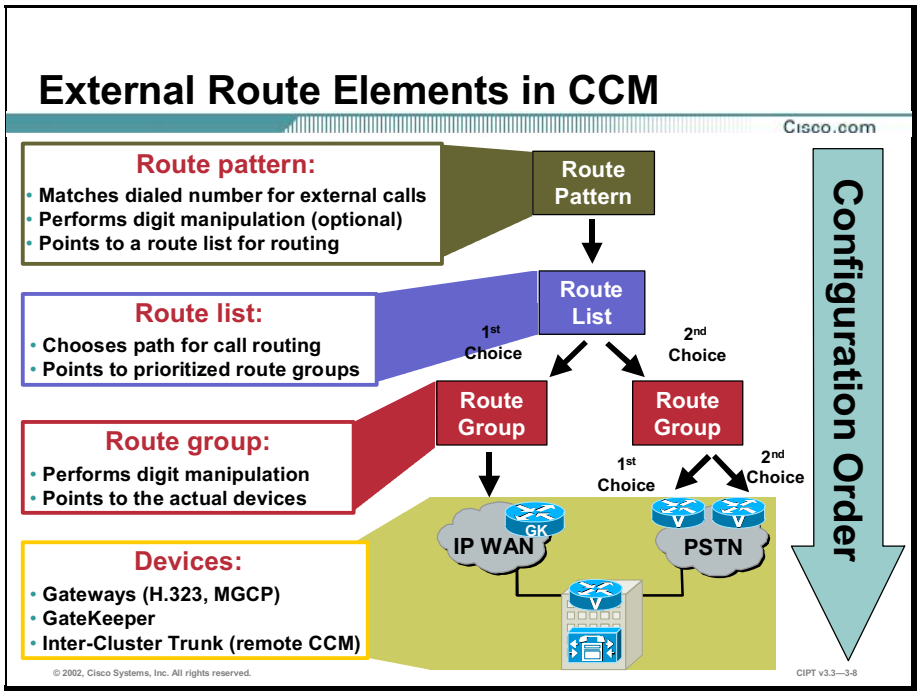
This topic explains external call routing in a basic route plan.



When you place a call from a Cisco IP Phone, Cisco CallManager (CCM) analyzes the dialed digits. If the dialed number matches a directory number (DN) that is registered with the CCM cluster, CCM enables you to route the call to the destination Cisco IP Phone associated with the matching DN. This type of call is an internal (or on-cluster) call. CCM allows you to handle the call internally without the need to route the call to an external gateway.

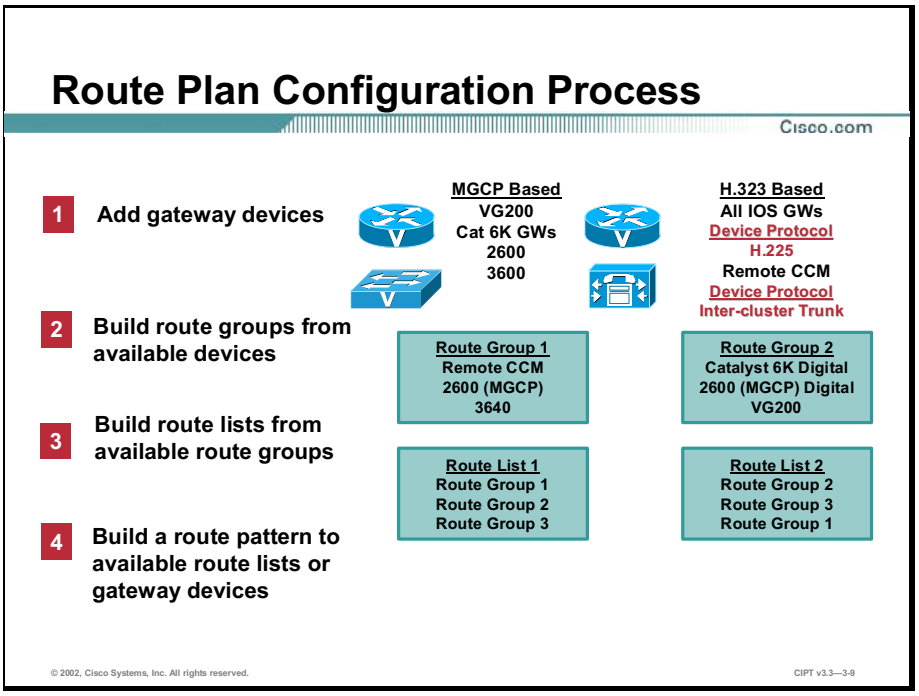
IP Phones are not the only devices that can place and receive internal calls; any device that registers a DN with CCM can place and receive internal calls. Examples of other devices include the Cisco IP SoftPhone and analog telephones attached to Media Gateway Control Protocol (MGCP) or Skinny-based gateways.

When an IP Phone dials a number that does not match a registered DN, it assumes that the call is an external (or off-cluster) call. CCM will then search its external route table to determine where to route the call. CCM uses the concept of route and translation pattern tables to determine where and how to route an external call. The route pattern and translation pattern tables are very similar to the routing table that a Cisco router maintains for routing data.



You can create external route plans based on a three-tiered architecture that allows multiple layers of call routing as well as digit manipulation. Route patterns match external dial strings, in which a corresponding route list will select available paths for the outbound call based on priority. Cisco refers to these paths as “route groups,” which are very similar to the Trunk Group concept in traditional PBX terminology. You can think of a route pattern as a static route with multiple paths that you can prioritize. The figure shown depicts the three-tiered route plan architecture.

In addition to facilitating multiple prioritized paths for a given dialed number, the route plan can also provide unique digit manipulation for each path, based on the external network requirements. Digit manipulation involves adding or subtracting digits from the original dialed number to accommodate user dial habits and to ensure that the external network or Public Switched Telephone Network (PSTN) receives the correct digits to place a call.



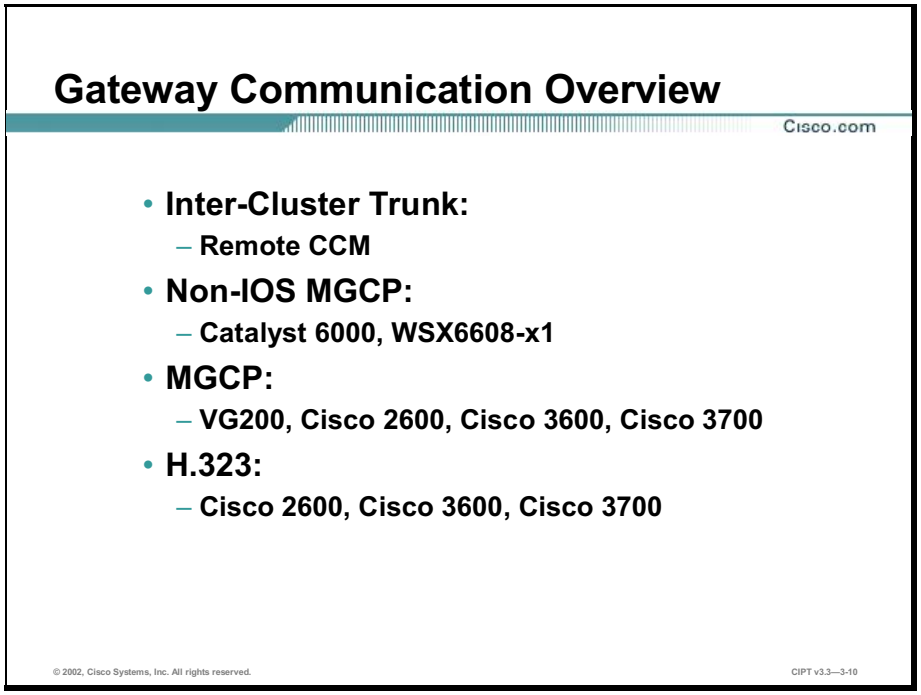
Shown here is the *general* process for route plan configuration. You can construct a route plan using this process:

- Add gateway devices. You can create gateway devices using the Device menu selection.
- Build route groups from available devices. You can select and place gateway devices in an ordered list to build a route group.
- Build route lists from available route groups. Select and order route groups in a route list.
- Build a route pattern and associate it with an available route list or gateway device.

The route pattern is the key component in a route plan. The route pattern matches an external dial string and routes the outgoing call to the appropriate gateway. When the dialed digits match a route pattern, CCM routes the call to the assigned route list or gateway.

Devices

This topic describes the gateway devices used in a Cisco IP telephony solution.



Gateway devices allow CCM to communicate with non-IP networks, such as the PSTN. Cisco created two main categories of gateway devices: analog gateways and digital gateways.

Analog gateways can be either station gateways or trunk gateways. Station gateways use Foreign Exchange Station (FXS) ports to connect to end-user devices such as fax machines and analog telephones. You can also use station gateways to connect to legacy systems, such as voice mail and interactive voice response (IVR) systems. Trunk gateways use Foreign Exchange Office (FXO) ports to connect to either the PSTN or PBXs and provide connectivity to other telephone systems through analog lines.

Digital gateways provide the same type of connectivity to the PSTN or PBX. However, digital gateways use digital technology such as PRI common channel signaling (CCS) and T1 channel-associated signaling (CAS) trunks. You can also use digital T1 PRI trunks to connect to certain legacy voice-mail systems.

The figure shows the grouping of voice gateway devices into three categories: MGCP, H.323, and Non-IOS MGCP gateways. CCM supports only these three gateway protocols. This list depicts the major advantages and disadvantages of each gateway protocol.

- **MGCP:** Uses a master-slave (Server-Client) model in which the CCM controls the gateway. MGCP gateways provide full support for CCM supplementary services (hold, transfer, and conference features), CCM redundancy, and call survivability. Ease of configuration is another advantage of MGCP.

- **Non-IOS MGCP:** Uses a master-slave (Server-Client) model in which the CCM controls the gateway. Non-IOS MGCP gateways provide full support for CCM supplementary services (hold, transfer, and conference features) and CCM redundancy, but do not support call survivability.

- **H.323:** Uses a peer-to-peer model. You perform most of the configuration through Cisco IOS on the voice gateway device. With the peer-to-peer model, CCM does not have control over the gateway, which limits the CCM feature support on H.323 gateways. For example, H.323 gateways do not support call survivability and only devices that support H.323 v2 can take advantage of CCM supplementary services, such as hold, transfer, and conference features. However, H.323 gateways support additional Cisco IOS features outside of CCM that the other gateways do not, such as Call Admission Control (CAC) and survivable remote site telephony (SRST).

In addition to the different gateway devices listed, another type of gateway, called an inter-cluster trunk, exists. The inter-cluster trunk is a logical gateway used for inter-cluster communication between two CCM clusters.

Selecting the protocol to use depends on site-specific requirements and the customer's installed base of equipment. For example, most remote branch locations have Cisco 1750, 2600, or 3600 series routers installed. These routers support H.323. With Cisco IOS software release 12.2(XA) and CCM 3.05(a) or later, the Cisco 2600 and 3600 series products support MGCP for analog FXS and FXO interfaces. MGCP support for T1 CAS and T1/E1 PRI on the Cisco 2600 and 3600 series will be available in a future Cisco IOS release.

For analog gateway configuration, you may prefer MGCP to H.323 due to simpler configuration or support for call survivability during a CCM switchover from a primary to a secondary CCM. Additionally, you may prefer H.323 to MGCP due to interface robustness or to use with CAC or SRST.

Most gateway devices support multiple gateway protocols. This table shows a detailed list of the gateways and supported protocols.

Table: Supported Gateway Protocols and Cisco IP Telephony Gateway

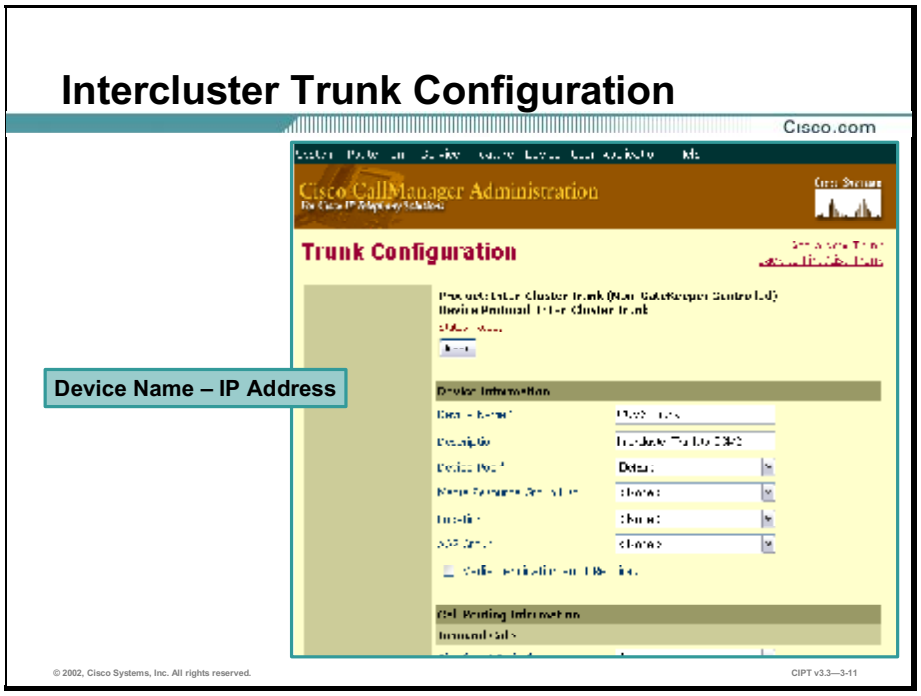
Gateway	MGCP	H.323	Non-IOS MGCP
VG200/248	Yes Supported with: FXS/FXO T1 CAS with CCM 3.1 and Cisco IOS software release 12.2.XN* (E&M Wink Start; Delay Dial only)	Yes Supported with Cisco IOS software release 12.1(5)XM1. The VG-200/VG-248 uses H.323 to support a wider range of digital and analog interfaces.	No
DE-30+, DT-24+	Yes, supported with CCM 3.1	No	Yes
Cisco 827	No	Yes, supported for FXS	No
Cisco 1751	Future support with Cisco IOS 12.2.7T	Yes	No
Cisco 3810 V3	Yes, supported with Cisco IOS software release 12.1(3)T and CCM 3.0(5)	Yes	No
Cisco 2600	Yes, supported with 12.2(XA) and CCM 3.0(5) FXO interfaces only, no E&M interface T1 CAS/T1/E1 PRI - Cisco IOS software release 12.2.9T** Q.931 PRI Backhaul – Cisco IOS software release 12.2.9T**	Yes	No
Cisco 3600	Yes, supported with 12.2(XA) and CCM 3.0(5) FXO interfaces only, no E&M support T1 CAS/T1/E1 PRI - Cisco IOS software release12.2.9T** Q.931 PRI Backhaul – Cisco IOS software release12.2.9T**	Yes	No
Cisco 3700	Yes, supported with Cisco IOS software release 12.2T	Yes	No
Cisco 5300***	Yes, supported with Cisco IOS software release 12.1(1)T***	Yes	No
Cisco AS5350*** Cisco AS5400***	Future support***	Yes, Cisco IOS software release 12.1(5)/12.2(2)XA	No
Cisco AS5800	No	Yes	No
Cisco AS5850***	Future support***	Future support	No
Cisco 7200***	Yes, supported with Cisco IOS software release 12.2.(1)T***	Yes	No
Cisco 7500	No	Yes, supported with Cisco IOS software release 12.1.5	No

Gateway	MGCP	H.323	Non-IOS MGCP
Catalyst 4000 WS-X4604-GWY Gateway Module	Future support with Cisco IOS software release and CCM 3.1*	Yes, for PSTN interfaces	Yes, for conferencing and MTP/ transcoding services
Catalyst 6000 WS-X6608-x1 Gateway Module & FXS Module WS-X6624	Yes, supported with CCM 3.1, T-1/E-1 module supporting PRI and CAS and FXS module	No	Yes, for FXS module and T1/E1 prior to CCM 3.1
Catalyst 4224	Yes, supported with 12.2.2XN and CCM 3.1*	Yes	No
Cisco ICS7750-MRP	No	Yes	No
Cisco ICS7750-ASI	No	Yes	No

*Special Cisco IOS software release tied to CCM 3.1.

**12.2.2T PRI Backhaul support for Cisco 2600 and 3600 series products uses RUDP and is not compatible with CCM. PRI backhaul with CCM 3.1 as the Call Agent is scheduled for Cisco software release 12.2.9T and uses TCP as the transport.

***While the Cisco 5300, Cisco AS5350, Cisco AS5400, CiscoAS5850, and Cisco 7200 supports MGCP, RUDP is used, which is not supported in CCM.



Use these steps to configure an inter-cluster trunk:

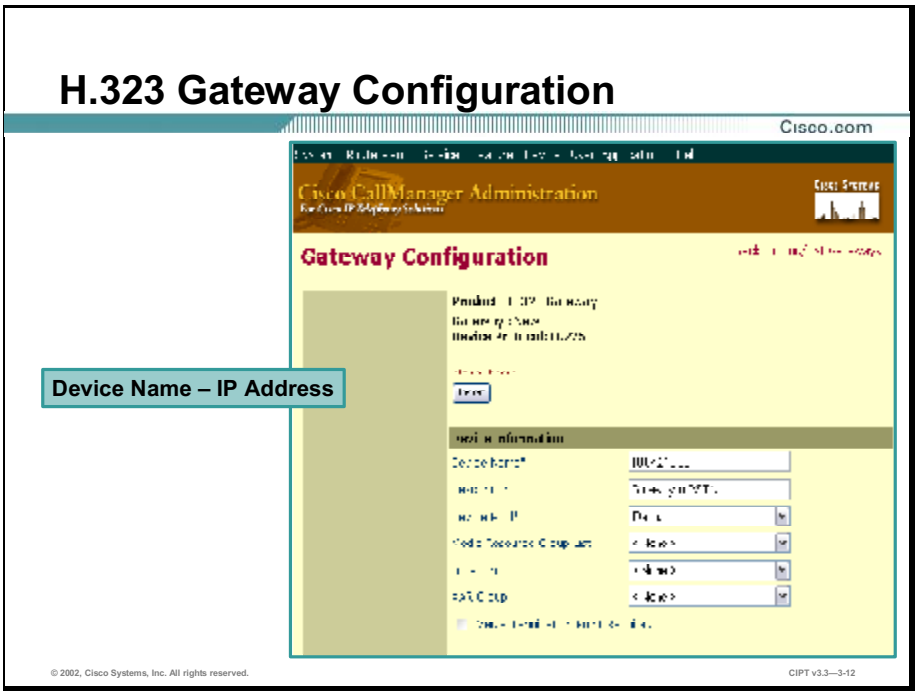
Step 1 Select **Trunk** from the Device menu on the Cisco CallManager Administration page.

Step 2 Click the **Add a New Trunk** hyperlink and select the appropriate Inter-Cluster Trunk type (GateKeeper Controlled or Non-GateKeeper Controlled).

Step 3 CCM populates the Device Protocol field with the appropriate protocol. Click **Next** to continue.

If you are configuring a Non-GateKeeper Controlled Inter-Cluster Trunk, you can enter the IP addresses of up to three CCMs in the remote cluster. If you are configuring a GateKeeper Controlled Inter-Cluster Trunk, you will enter the gatekeeper information, such as the gatekeeper's name, prefix, and zone.

Note The Trunk Configuration page has other configurations. Search the CCM Help option for inter-cluster trunk configuration to obtain additional information regarding these settings.



Use these steps to configure an H.323 gateway:

Step 1 Select **Gateway** from the Device menu on the Cisco CallManager Administration page.

Step 2 Click the **Add a New Gateway** hyperlink and select **H.323 Gateway** from the Gateway Type menu.

Step 3 CCM automatically populates the Device Protocol field with H.225. Click **Next**. For the device name, enter the IP address of the Cisco router that will be acting as the gateway.

Note	The Gateway Configuration page has other configuration settings. Search the CCM Help option for gateway configuration to obtain additional information regarding these settings.

Because H.323 is a peer-to-peer protocol, you must configure most of the gateway configuration using Cisco IOS on the gateway itself. The table lists the Cisco IOS commands used to configure a voice gateway.

Table: Cisco IOS Commands

Command	Description
H323_GW(config)# **voice class** h323 *<tag>*	Creates an H.323 voice class that is used to configure a TCP time-out duration.
H323_GW(config-class)# **h225 tcp timeout** *<seconds>*	Configures the H.225 TCP time-out duration in seconds. Possible values are 0 to 30. The default is 15. If you specify 0, the H.225 TCP timer is disabled. When the duration (seconds) of the H.225 TCP is exceeded, the voice gateway will use the next ordered dial peer (controlled via the **preference** command), which points to a backup CCM.
H323_GW(config)# **dial-peer voice** *<tag>* voip	Creates a Voice over IP dial-peer.
H323_GW(config-dial-peer)# **voice class h323** *<tag>*	Assigns the previous created voice class to this dial-peer.
H323_GW(config-dial-peer)# **destination-pattern** *<dial-string>*	Configures the dial string that this dial-peer matches.
H323_GW(config-dial-peer)# **session target ipv4**:*ccm ip address*	Identifies the IP address to route a call to when the destination pattern above is matched. The IP address is the address of the CCM on an H.323 gateway.
H323_GW(config-dial-peer)# **preference** *<0 – 10>*	Assigns a preference to a dial-peer when multiple dial-peers contain the same destination pattern, but different session targets. 0 is the highest, 10 is the lowest (used to configure CCM redundancy on H.323 gateways).
H323_GW(config-dial-peer)# **dtmf-relay h245-alphanumeric**	Configures the gateway to use out-of-band DTMF relay. DTMF relay sends DTMF across the signaling channel, instead of part of the voice stream. DTMF relay is needed when you are using a low-bit-rate codec for voice compression, because the potential exists for DTMF signal loss or distortion.

Example

Here is an example configuration of an H.323 gateway configured for CCM redundancy.

Table: H.323 Gateway Configuration for CCM Redundancy

Command	Description

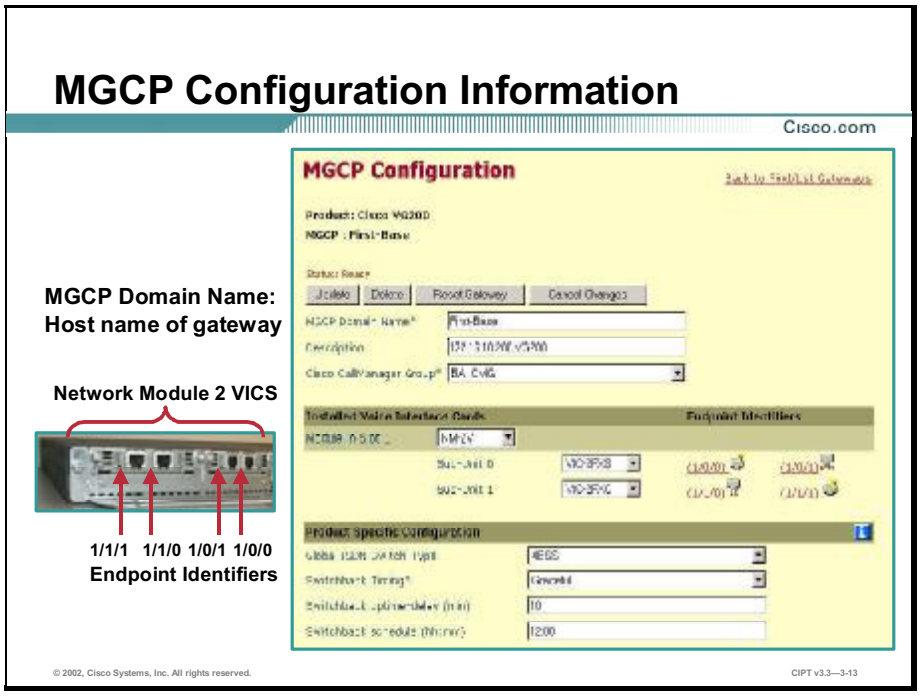
`dial-peer voice 101 voip`
`destination-pattern 1111`
`session target ipv4:10.1.1.101`
	IP address of the primary CCM

`preference 0`	Specifies this dial-peer as the connection to the primary CCM

`dtmf-relay h245-alphanumeric`
`dial-peer voice 102 voip`
`destination-pattern 1111`
`session target ipv4:10.1.1.102`
	IP address of the secondary CCM

`preference 1`	Specifies this dial-peer as the connection to the secondary CCM

Note The Cisco Voice over IP (CVOICE) course discusses the complete configuration of the H.323 gateway.



Use these steps to configure an MGCP Gateway:

Step 1 Select **Gateway** from the Device menu on the Cisco CallManager Administration page.

Step 2 Click the **Add a New Gateway** hyperlink and select one of the various MGCP capable devices from the Gateway Type menu.

Step 3 CCM automatically populates the Device Protocol field. Click **Next**.

Step 4 For the domain name, enter the unique host name of the Cisco device that will be acting as the gateway. You must also select a CCM Group for redundancy. You must then select the type of network modules (NMs) and voice interface cards (VICs) that are used in the sub-unit slots of the MGCP gateway.

Note The MGCP Configuration page has other configuration settings. Search the CCM Help option for MGCP gateway configuration to obtain information regarding these additional settings.

After you configure the general gateway settings, you must then configure the endpoint identifiers via Cisco IOS on the MGCP gateway device.

The table shown here lists commands to help configure endpoint identifiers.

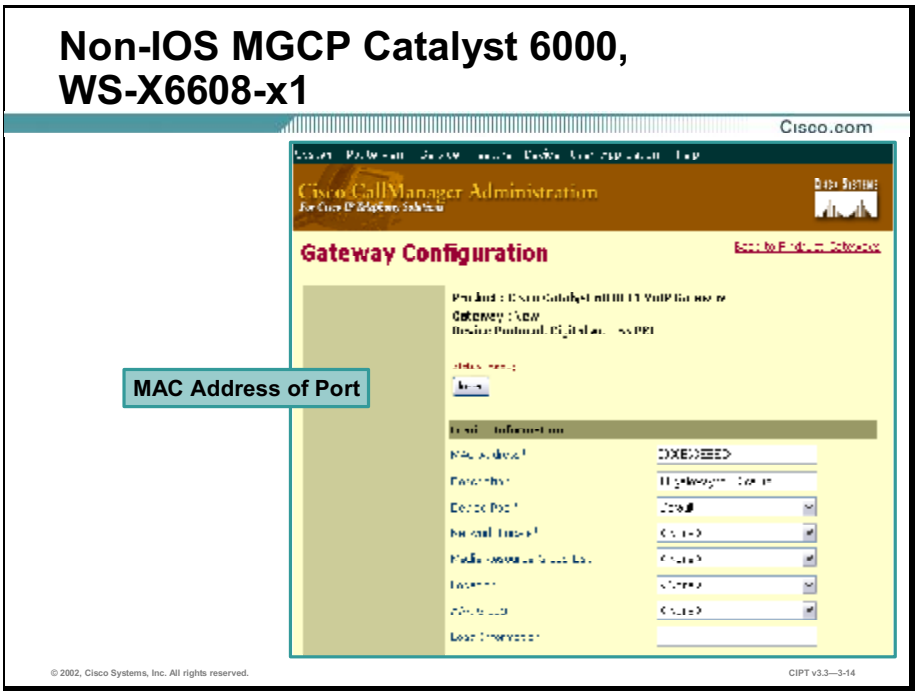
Table: Cisco IOS Commands

Command	Description
Router(config)# **host MGCP_GW**	Assigns a unique name to the voice gateway so that the CCM server can identify it. This name must be unique throughout the network.
MGCP_GW(config)# **mgcp**	Enables MGCP on the voice gateway.
MGCP_GW(config)# **mgcp call-agent** *<ip address>*	Identifies the primary CCM for the gateway.
MGCP_GW(config)# **ccm-manager mgcp**	Indicates to the gateway that the CCM is using MGCP.
MGCP_GW(config)# **ccm-manager redundant-host** *<ip address1> <ip address2>*	Specifies the secondary and tertiary CCMs used for CCM redundancy.
MGCP_GW(config)# **ccm-manager switchback** {**graceful** | **immediate** | **schedule-time** *hh:mm* | **uptime-delay** *minutes*}	Specifies how the gateway behaves if the primary server becomes unavailable and later becomes available again. The keywords and arguments are as follows: ■ **graceful**: Completes all outstanding calls before returning the gateway to the control of the primary CCM server. ■ **immediate**: Returns the gateway to the control of the primary CCM server without delay, as soon as the network connection to the server is reestablished. ■ **schedule-time *hh:mm***: Returns the gateway to the control of the primary CCM server at the specified time, where *hh:mm* is the time according to a 24-hour clock. If the gateway re-establishes a network connection to the primary server after the configured time, the switchback will occur at the specified time on the following day. ■ **uptime-delay *minutes***: Returns the gateway to the control of the primary CCM server when the primary server runs for a specified number of minutes after a network connection is re-established to the primary server. Valid values are from 1 to 1440 (from 1 minute to 24 hours).
MGCP_GW(config)# **mgcp dtmf-relay voip codec all mode out-of-band**	Configures the gateway to use out-of-band DTMF relay for all codecs. If this command is not configured, DTMF tones will be not be regenerated correctly on remote endpoints.
MGCP_GW(config)# **mgcp sdp simple**	Configures the voice gateway to use the simple desktop messaging protocol.
MGCP_GW(config)# **dial-peer voice** *<tag>* **pots**	Creates a POTS dial-peer.
MGCP_GW(config-dial-peer)# **application MGCP**	Configures the dial-peer to use the MGCP application.
MGCP_GW(config-dial-peer)# **port 1/1/1**	Associates the dial-peer with a voice-port.

Example

```
MGCP_GW#show running-config
mgcp

mgcp call-agent 172.20.71.30

mgcp dtmf-relay codec all mode out-of-band

mgcp sdp simple

!

ccm-manager switchback graceful

ccm-manager redundant-host 172.20.71.26 172.20.71.47

ccm-manager mgcp

!

voice-port 1/1/1

!

dial-peer voice 4 pots

application MGCPAPP
```

Note The Cisco Voice over IP (CVOICE) course discusses the complete configuration of the MGCP gateway itself.



Use these steps to configure a Non-IOS MGCP Gateway:

Step 1 Select **Gateway** from the Device menu on the Cisco CallManager Administration page.

Step 2 Click the **Add a New Gateway** hyperlink and select one of the various Non-IOS MGCP devices from the Gateway Type menu. If you have selected the Catalyst 6000 WS-X6608 module, The Device Protocol field provides you with the option of either Digital Access PRI or Digital Access T1. After you have made your selection, click **Next**.

CCM associates with a Non-IOS MGCP gateway (such as the 6608 blade) through the MAC address of the port. The **<mod> show port** command from enable mode on the Catalyst 6000 is a quick way to identify and list the MAC addresses of each digital gateway port on the Voice T1/E1 and Services (WS-X6608) module.

```
Cat6000(enable)show port 3
Port      DHCP     MAC-Address        IP-Address      Subnet-Mask
--------- -------- ------------------ --------------- ---------------
 3/1      disable  00-30-b6-3e-8e-c4  172.16.10.121   255.255.255.0
 3/2      disable  00-30-b6-3e-8e-c5  172.16.20.122   255.255.255.0
 3/3      disable  00-30-b6-3e-8e-c6  172.16.30.123   255.255.255.0
 3/4      disable  00-30-b6-3e-8e-c7  172.16.40.124   255.255.255.0
 3/5      disable  00-30-b6-3e-8e-c8  172.16.1.125    255.255.255.0
 3/6      disable  00-30-b6-3e-8e-c9  172.16.1.126    255.255.255.0
 3/7      disable  00-30-b6-3e-8e-ca  172.16.1.127    255.255.255.0
 3/8      disable  00-30-b6-3e-8e-cb  172.16.1.128    255.255.255.0
```


Note To display detailed information about a specific port on the module use the **<mod/port> show port** command.

Cisco recommends that you statically configure T1/E1 ports that are used as digital gateways. In order to ensure that a particular port registers with the correct CCM, confirm that the TFTP server IP address is the same address as the server that you want the port to register within the CCM cluster.

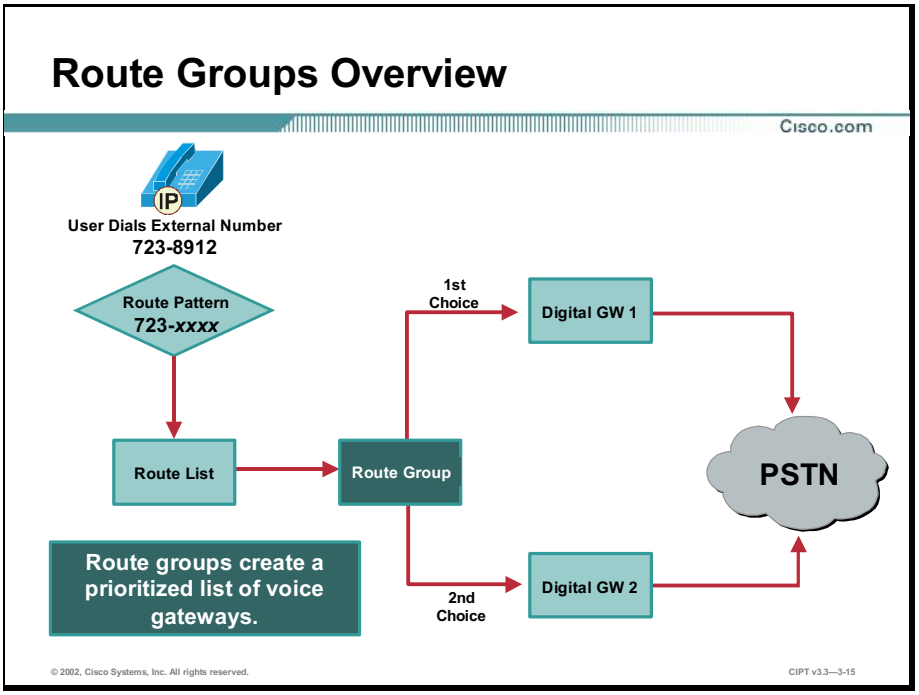
After you add the gateway to the database, CCM creates a configuration file in the cluster on the Cisco TFTP server, and this is where the T1/E1 port downloads its configuration details, which include an ordered list of CCMs. The following command disables DHCP and statically configures the following voice port settings: IP address, subnet mask, VLAN ID, TFTP server IP address, and default gateway.

```
Cat6000 (enable) set port voice in 3/1 dhcp disable 172.16.1.121
255.255.255.0 vlan 1 tftp 172.16.1.5 gateway 172.16.1.1
```

Note When a port resets, the module has the ability to reset the adjoining port because all eight ports on the WS-X6608 module share the same XA processor. This creates a domino effect, and all of the ports on the module reset. If you are not going to use a port, you should either disable the port or configure and register it to Cisco, so that it does not continuously perform an asynchronous reset.

Route Groups

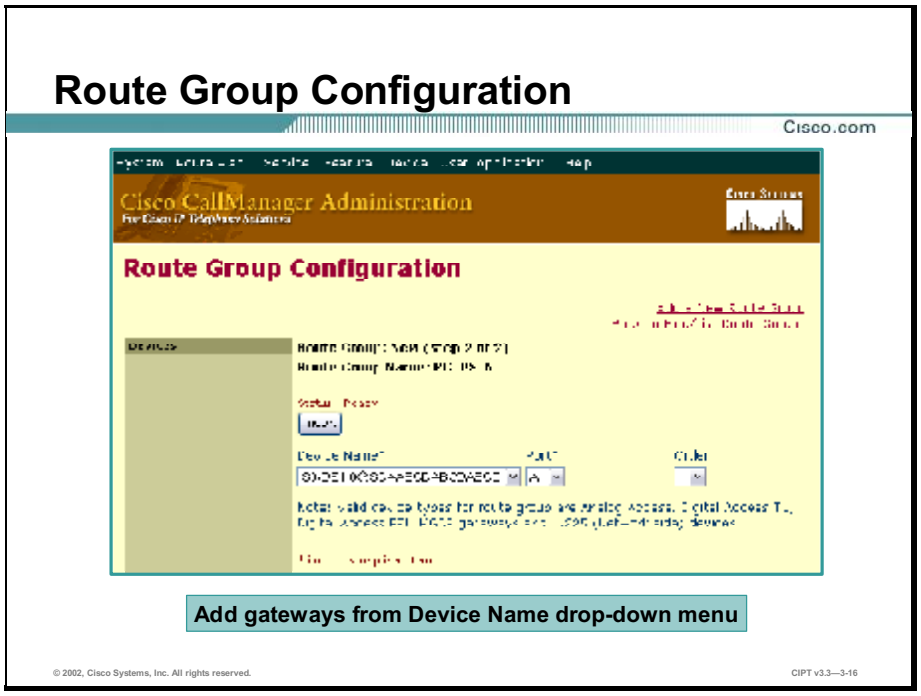
This topic describes the functions and configuration of route groups.



Route groups and route lists work together to control and enhance external call routing. They also help with implementing cost savings and redundancy, which are some of the common features of a Cisco IP telephony network.

Route groups are a logical grouping of device gateways. Prioritizing these device gateways allows you to send external calls out of a preferred gateway (usually across the IP WAN for toll savings) and keep a backup path for external calls (usually the PSTN) if the primary gateway is down or unable to route the call.

You may encounter a scenario that requires multiple route groups, such as multiple long-distance carriers. Each long-distance carrier offers different rates for long-distance calls on their network. You can use route groups to prioritize the use of the cheaper carrier over the others and retain redundancy if the cheaper carrier cannot route the call for some reason.



Use these steps to configure a route group:

Step 1 Select **Route Group** from the Route Plan menu on the Cisco CallManager Administration page.

Step 2 Click the **Add a New Route Group** hyperlink. Give the new route group a name and click **Continue**.

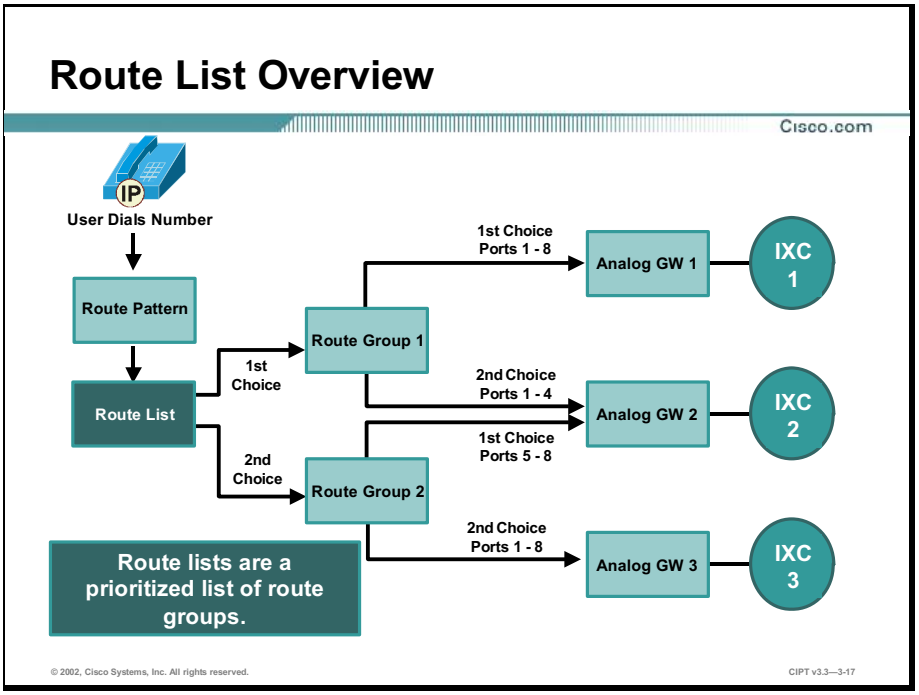
Step 3 Select a gateway from the Device Name menu to add that gateway to the route group.

The method you use to configure route groups depends on the gateway types that you plan to include in the group. Each gateway is an entity; you group H.323 gateways as a whole by device. However, you can group MGCP gateways by ports, which means that individual ports on MGCP gateways can be entities in a route group. The Order menu allows you to control the priority of the gateways within a route group.

You should configure route groups by function. For example, all gateways to the PSTN can belong to one route group, all gateways to long-distance carriers can belong to another (with the cheapest carrier having priority), and all gateways across the IP WAN can belong to another route group. If you want to control routing per gateway instead of groups of gateways or ports, a route group can contain only one gateway.

Route Lists

The topic describes the functions and configuration of route lists.



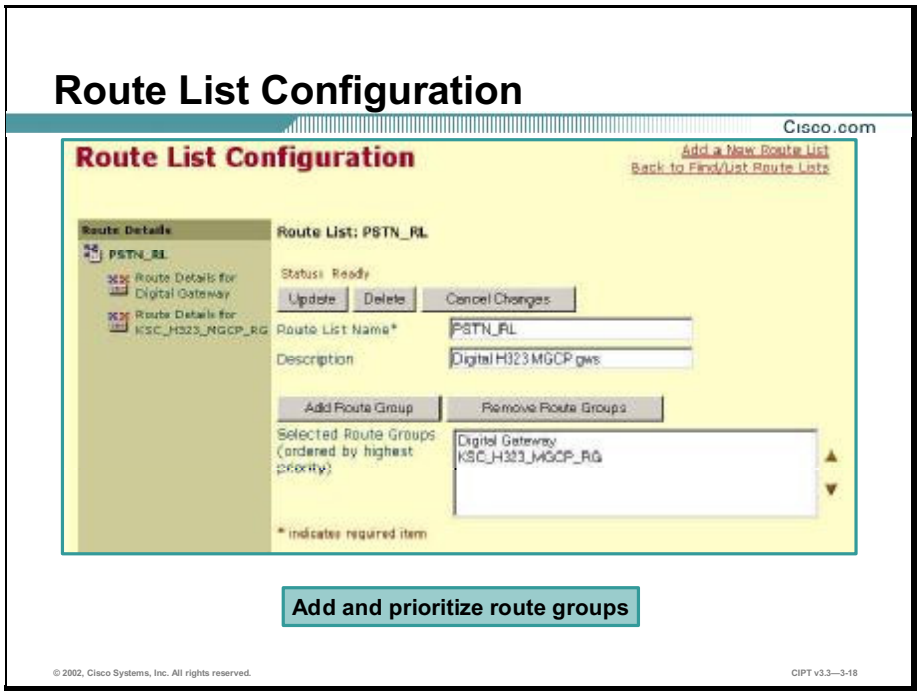
Route lists consist of an ordered list of route groups. Route lists expand on the route group concept and allow you to order and prioritize your route groups. Although a gateway or group of ports on a gateway can only belong to a single route group, route groups can belong to any number of route lists. Route groups give you granular control over external call routing.

With route lists, you can implement features, such as toll bypass and PSTN Fallback because within the route list you prioritize route groups that contain different types of gateways (IP WAN, PSTN, etc.).

Digit manipulation is the key to making toll bypass and PSTN Fallback features transparent to your users. Digit manipulation occurs in the form of calling and called party transformations.

Use calling party transformations to manipulate Caller ID information that is presented to the called party. Use called party transformations to actually manipulate the digits dialed. You can apply calling and called party transformations at five different levels of the call-routing process: at the originating device, as part of a translation pattern, as part of a route pattern, as part of a route list, or at the terminating device. Calling and called party transformations set at the route list level override transformations settings set at any other level.

Note	Calling and called party transformations are covered in detail in the Advanced Route Plan lesson later in this course.



Use these steps to configure a route list:

Step 1 Select **Route List** from the Route Plan menu on the Cisco CallManager Administration page.

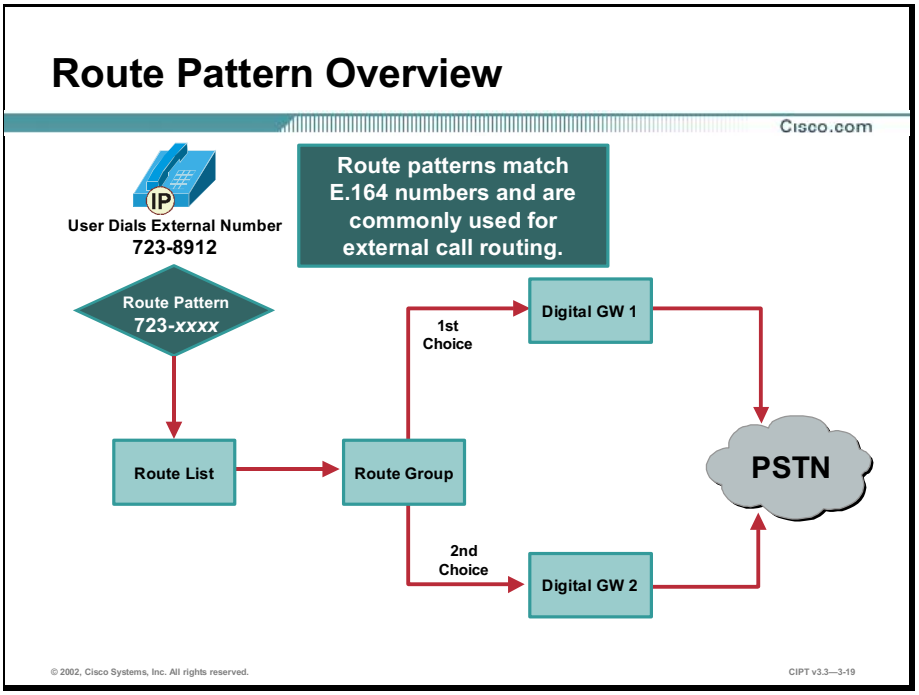
Step 2 Click the **Add a New Route List** hyperlink. Give the new route list a name and description, and click **Continue**.

Step 3 Click the **Add Route Group** button to add the appropriate route groups. This action brings up the Route Details page. You can set calling and called party transformations at this point. Setting these transformations is covered in the following topics.

Step 4 Click **Insert** to return to the Route List Configuration page. Use the arrows to prioritize the route groups.

Route Pattern

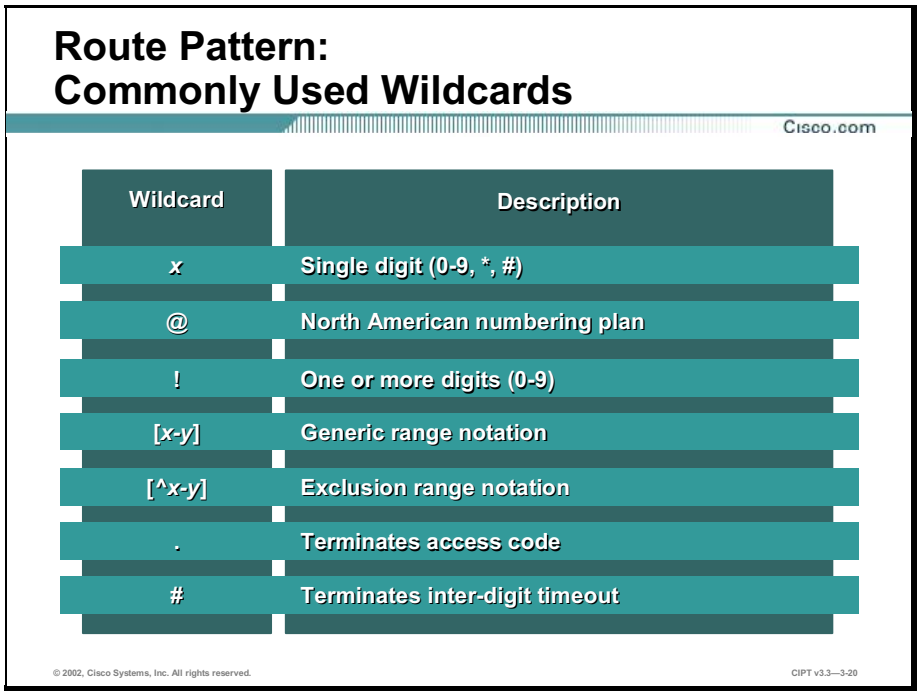
This topic describes route patterns for external call routing.



In the IP world, route patterns are the equivalent of static routes. The only difference is that route patterns point to E.164 numbers instead of IP addresses.

This topic covers external route patterns used for routing off-cluster calls. External route patterns can point to either an individual gateway or a route list. Here is the call process if the route pattern points to a route list:

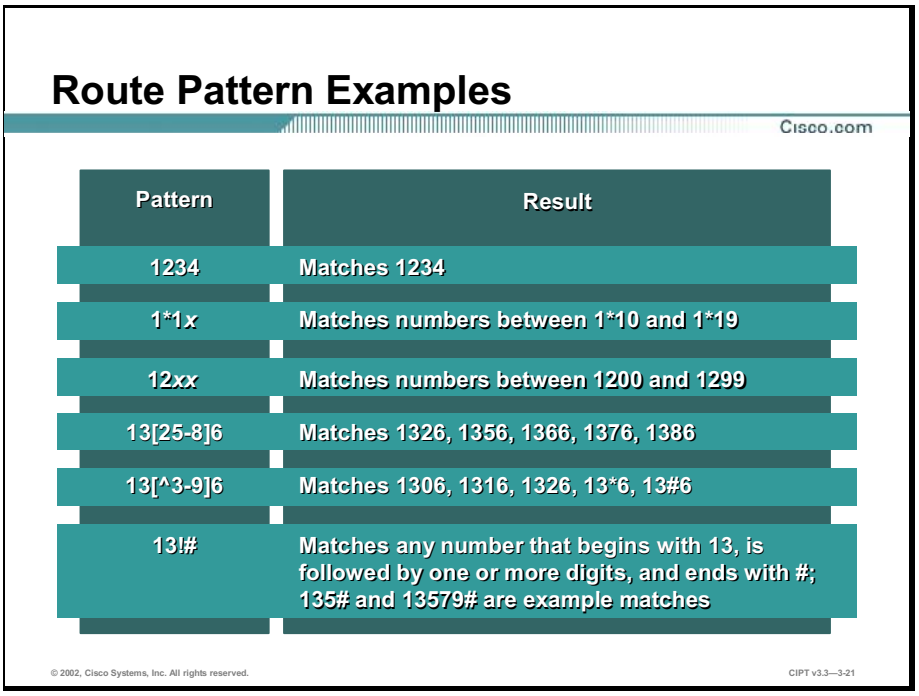
- When a user dials a number, CCM will analyze the dialed digits. If the set of digits matches a registered DN, CCM routes the call to the internal destination.
- If the set of digits matches an external route pattern, CCM then parses the route list associated with that route pattern. The route list contains a prioritized list of route groups and the route groups contain a prioritized list of voice gateways.
- If the preferred voice gateway is unavailable to handle the call, CCM passes the call to the next gateway, and so on until it either finds a gateway to route the call to or exhausts the list of gateways in the route group.
- If CCM exhausts the list of gateways in the route group, it passes the call to the preferred gateway in the next route group in the route list. This process repeats until CCM finds a gateway that can handle the call, or until it exhausts the list of route groups in the route list. If CCM is unable to find a gateway that can take the call, the call fails and the end user will receive a fast busy signal.



A route pattern is a sequence of digits and other alphanumeric characters. If a route pattern contains all numeric digits, it is an exact match route pattern and only matches one destination. By including nonnumeric wildcards in a route pattern, the route pattern can represent multiple destinations. The purpose of using wildcards is to reduce the number of route patterns that you need to configure. For example, a single route pattern of 1*xxx* would match all dialed numbers from 1000-1999.

Table: Wildcards

Wildcard	Description
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, #	Single digits that can be included in a route pattern
[*xyz*]	Set of matching digits. For example, [458] matches one occurrence of either 4, 5, or 8.
[*x-y*]	Range of digits. For example, [3-9] matches one occurrence of either 3, 4, 5, 6, 7, 8, or 9. You can use the range notation along with the set notation. For example, [3-69] matches one occurrence of either 3, 4, 5, 6, or 9.
[^*x-y*]	If the first character after the open angle bracket is a carat, the expression matches one occurrence of any digit (including * and #) except those specified. For example, [^1-8] matches one occurrence of 9, 0, *, or #.
<wildcard>?	A question mark following any wildcard or bracket expression matches zero or more occurrences of any digit that matches the previous wildcard. For example, 9[12]? matches the following dial strings: 9, 91, 92, 912, 9122, 92121, and many others.
<wildcard>+	A plus sign following any wildcard or bracket expression matches one or more occurrences of any digit that matches the previous wildcard. For example, 3[1-4]+ matches 31, 3141, 3333, and many others.



Although the examples in the figure show four-digit extensions, you do not usually use route patterns for internal numbers. Route patterns are normally in the form of seven-digit numbers, such as 723-*xxxx*, or longer.

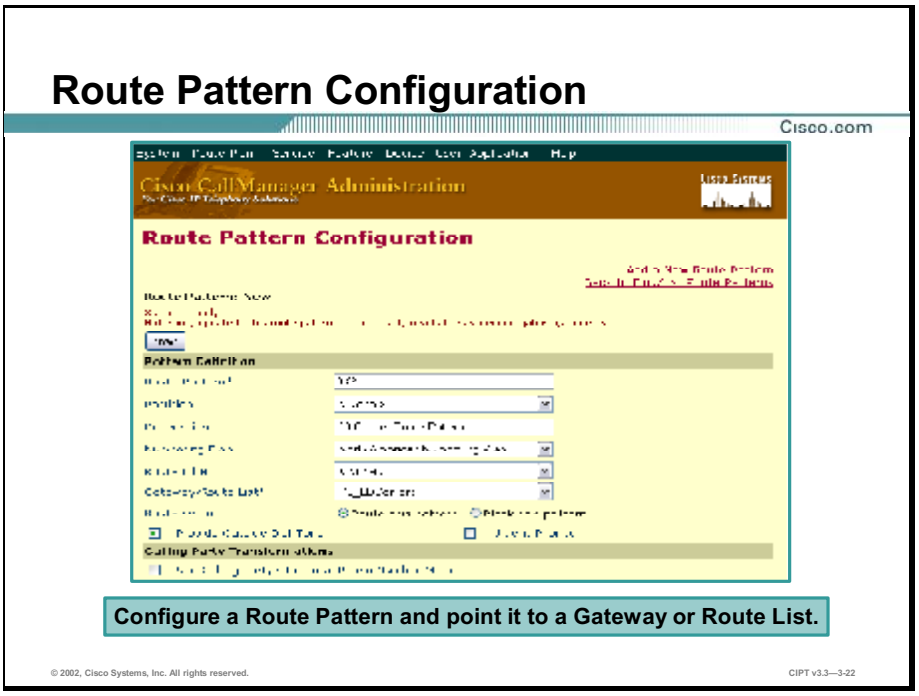
A great example of this is the 9.@ route pattern. The first digit of the route pattern matches a dialed digit of "9," which users commonly use as a code to gain outside access to the PSTN. The second digit "." is used to identify the first digit as an access code, and all numbers afterward as the dial string. The third digit "@" is the wildcard used to match the North American Dialing Plan.

The North American Dialing Plan encompasses these dial strings:

Table: Dial Strings

Dial String	Description
Service calls	Service calls are in the form of three to four-digit calls used to access telephony services such as 911, 411, 611, etc.
Local Calls	Local calls are in the form of a seven-digit number (*xxx-xxxx*) used to dial within your local calling area.
Expanded Local Calls	Expanded local calls are in the form of a 10-digit number (*xxx-xxx-xxxx*) used to dial expanded area local calls.
Long-Distance Calls	Long-distance calls are in the form of a 10-digit number (*xxx-xxx-xxxx*) used to place long-distance calls directly to a long-distance carrier.
Direct-Dial Long-Distance Calls	Direct-Dial Long-Distance calls are in the form of an 11-digit number (1-*xxx-xxx-xxxx*) used to place a long-distance call through a local carrier.
International Calls	International calls are in the form of 01 1 *xx xxxxxxxxx* where xx is the country code. The actual length of the dial string depends on which country you are calling.

Note This is a just a partial list of the different dial strings that the 9.@ route pattern will match. The North American Dialing Plan and the 9.@ route pattern are covered in more detail in the Advanced Route Plan lesson.



Use these steps to configure a route pattern:

Step 1 Select **Route Pattern** from the Route Plan menu on the Cisco CallManager Administration page.

Step 2 Click the **Add a New Route Pattern** hyperlink.

Step 3 To create a route pattern, type your route pattern (including wildcards if necessary) in the Route Pattern field and select a route list or gateway from the Gateway/Route List menu. The Partition and Route Filter fields will be covered later in the course.

Step 4 If you configure route a pattern to route off-network calls to the PSTN (which most route patterns are) make sure to check the **Provide Outside Dial Tone** check box. This plays a second dial tone for the user when they dial the outside access code.

If CCM receives a dial string for which multiple route patterns match, CCM must wait for the interdigit timeout before applying the longest match rule and deciding which route pattern to use. The interdigit timeout parameter is also used with route patterns that contain the "!" wildcard. The ! wildcard indicates a variable length dial string and forces the CCM to wait for the interdigit timeout to expire before it can determine the actual dial string that the user wants to dial.

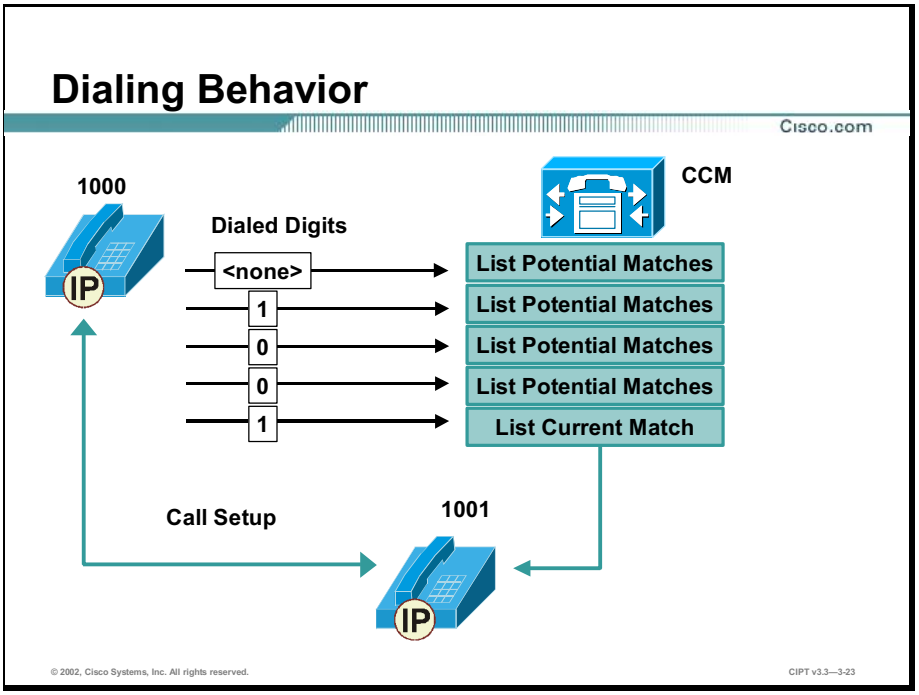
You can override the interdigit timeout behavior for a specific route pattern by checking the **Urgent Priority** check box. When a route pattern is marked as urgent, CCM immediately routes any outbound calls that match the pattern. This avoids the interdigit timeout issue. However, you should use this very carefully as it can prevent users from reaching certain destinations if it is configured incorrectly.

If your route patterns point to specific gateways and not route lists, you can set calling and called party transformations at the gateway level. If calling and called party transformations are set here and the route pattern points to a route list, CCM overrides the transformation settings by any transformation settings configured on the route list.

Near the bottom of the Route Pattern Configuration screen, you will find the ISDN Network-Specific Facilities Information Element configuration. This feature allows you to enter the appropriate carrier identification code (up to four digits) to route long-distance calls to specific interexchange carriers on a route pattern by route pattern basis.

Digit Analysis

This topic explains the digit analysis behavior of CCM.



The call-routing component behavior can be counterintuitive. Whenever a user places a call from a device registered with CCM, CCM must analyze each dialed digit to determine where to route the call. In collecting dialed digits, the call routing component goes through the following process:

1. CCM compares the current sequence of dialed digits against the list of all route patterns and determines which route patterns currently match. Then, CCM names the set of route patterns that currently match the dialed digits *currentMatches*.

   — If *currentMatches* is empty, the user dialed digit string does not currently correspond with a destination.

   — If *currentMatches* contains one or more members, the call routing component determines the closest match. The closest match is the route pattern in *currentMatches* that matches the fewest number of route patterns. For example, the dialed digit string 2000 matches both route pattern 2*xxx* and 20*xx*. Although there are 1000 different dialed digit strings that match 2*xxx*, only 100 dialed digit strings match 20*xx*. Therefore, 20*xx* is the closest match.

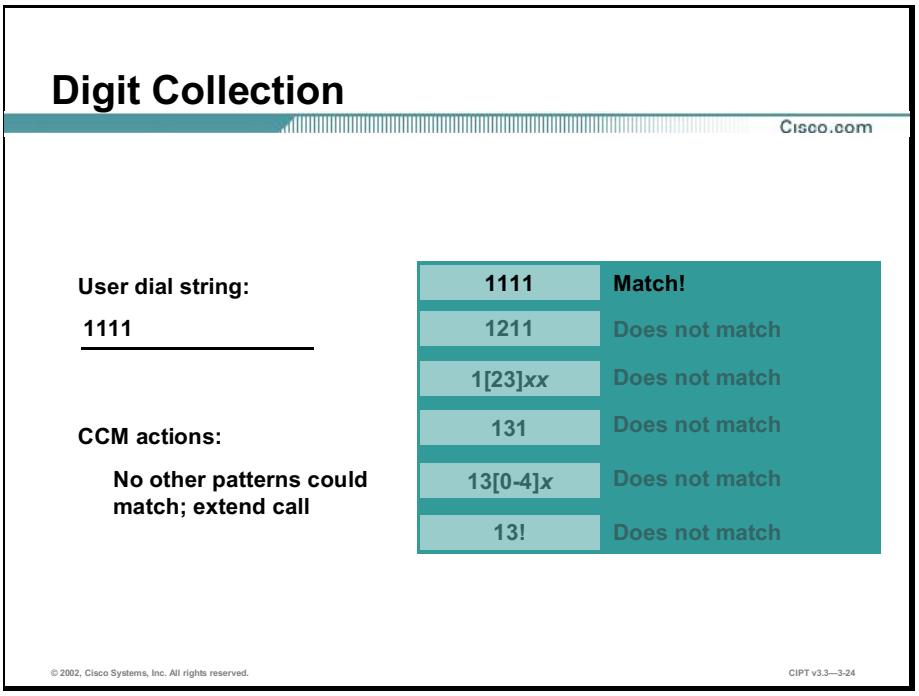
2. While performing Step 1, CCM determines whether different route patterns might match if the user were to dial more digits. CCM names the condition of having potential matches for a dialed digit string *potentialMatches*.

- If *potentialMatches* holds true, the call routing component waits for the user to dial another digit. If the user dials another digit, the sequence of events restarts at Step 1 using the new digit string.

- If *potentialMatches* no longer holds true or a dialing timeout has elapsed, then the call routing component selects a destination.

- To select a destination, the call routing component looks at the closest match. If there is no closest match, the dialed digit string does not correspond with a destination. Furthermore, no more digits are forthcoming. CCM rejects the call attempt.

- Otherwise, CCM extends the call to the device associated with the closest match.

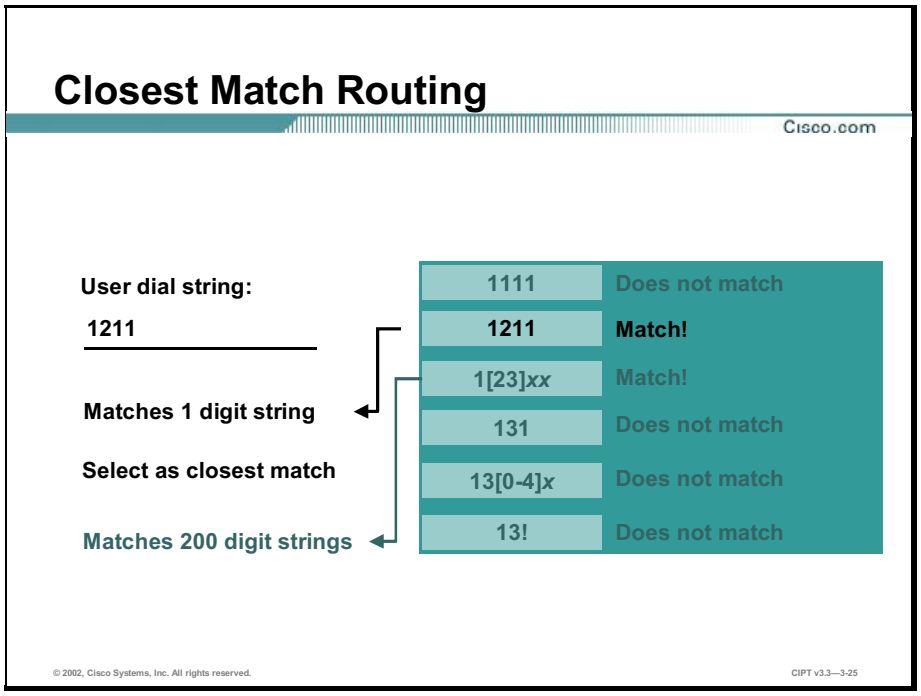


This figure details a call-routing example in which one route pattern matches the dialed digits exactly. The CCM used in this example includes the route patterns shown in the figure above.

When the user goes off-hook, CCM begins its routing process. The current set of collected digits is empty. Every route pattern that CCM has configured is a potential match at this point. As long as the *potentialMatches* condition holds true, CCM must wait for more digits.

The user now dials a 1. At this time, there are no current matches and every route pattern is still a potential match. The user dials another 1. At this point, CCM eliminates route patterns 1211, 1[23]*xx*, 131, 13[0-4]*x*, and 13! as potential matches. The only route pattern left is 1111. However, because there are no current matches and the *potentialMatches* condition is still true, CCM must continue to analyze digits. This requirement is in place because the user may continue dialing and dial a string that matches a route pattern exactly.

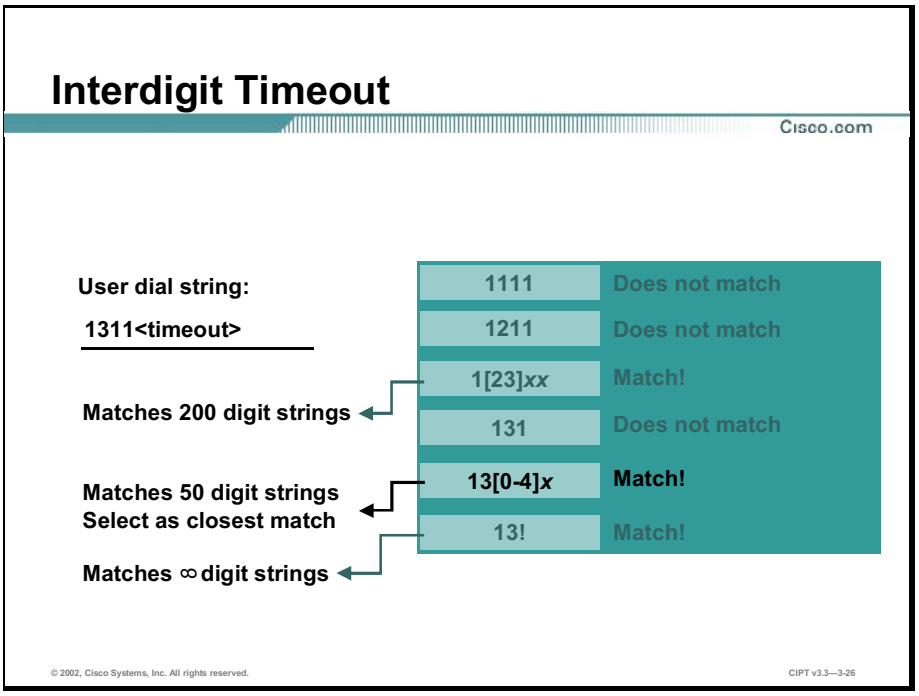
The user dials another 1, which does not change anything. The condition *currentMatches* is false and *potentialMatches* is still true. The user dials 1 again. At this point, the route pattern 1111 is a match and the *currentMatches* condition is true. CCM removes the route pattern 1111 from the potential matches table. Because there are no more route patterns in the potential matches table, any further dialed digits will not cause CCM to match a different route pattern. At this point CCM routes the call to the dialed destination.



This figure details a closest match call-routing example. The CCM used in this example includes the route patterns shown in the figure above.

The user dials the digits 12. At this point, CCM eliminates the route patterns 1111, 131, 13[0-4]X, and 13! from being potential matches. This leaves route patterns 121X and 1[23]*xx* as potential matches. Because there are no current matches and the *potentialMatches* condition is true, CCM continues to analyze digits.

The user dials another 1, which does not change anything. The condition *currentMatches* is false and *potentialMatches* is still true. The user dials 1 again. At this point, the route patterns 121X and 1[23]*xx* are current matches and CCM removes them from the potential matches table. Because the potential matches table does not contain additional route patterns, any further dialed digits will not cause CCM to match any different route patterns. Now, CCM must decide where to route the call based on the route patterns available in the current matches table. This is where the closest match rule is applied. The route pattern 121X matches 10 destinations (1210 – 1219). The route pattern 1[23]*xx* matches 200 destinations (1200 – 1299 and 1300 – 1399). CCM then routes the call to the gateway or route list associated with the 121X route pattern.



If you configure a CCM with route patterns that contain wildcards that match multiple digits, CCM must often wait for the interdigit timeout to expire before routing the call. The ! wildcard usually represents a variable length dial string and will never be an exact match for a group of dialed digits. The CCM used in this example includes the route patterns shown in the figure.

In this example, the user has dialed a string of 1311. This causes CCM to eliminate the route patterns 1111, 121X, and 131. CCM places the route patterns 1[23]*xx*, 13[0-4]*x*, and 13! in the current matches table. The 13! route pattern remains in the potential matches table. The 13! route pattern ensures that the *potentialMatches* condition is always true, as CCM has no way of knowing if the user intends to keeping dialing. For example, the user may intend to dial the number 1311555. As long as the *potentialMatches* condition is true, CCM must continue to wait for dialed digits.

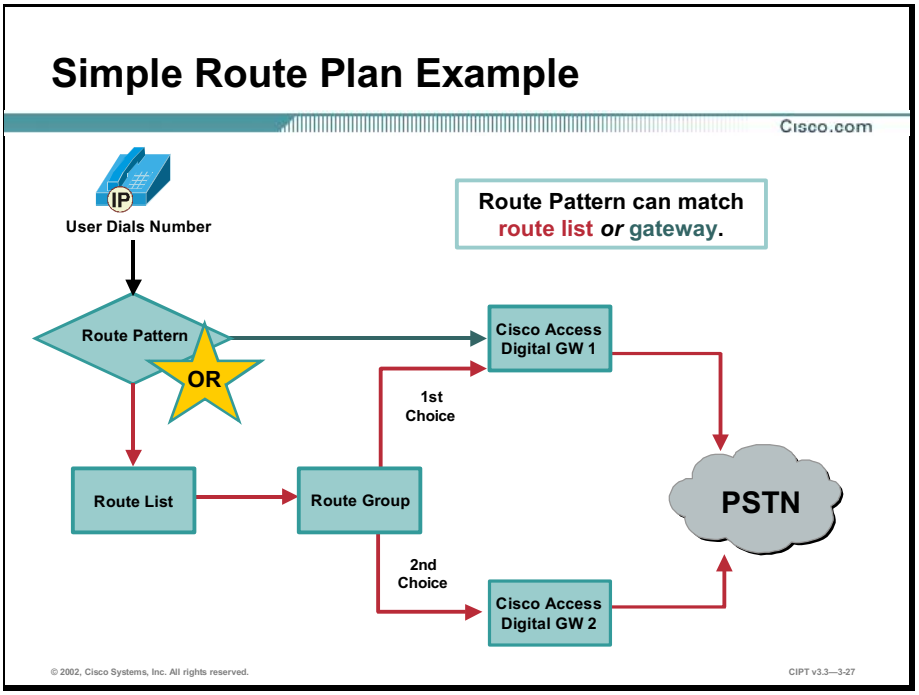
In this case, the only event that allows CCM to select a destination is an interdigit timeout. When the interdigit timeout timer expires, CCM knows that no more digits are forthcoming and can now make a final routing decision. In this example, the user dialed 1311 and then stopped dialing digits. This triggered an interdigit timeout and caused the CCM to make a final decision based on the following route patterns in the current matches table: 1[23]*xx*, 13[0-4]*x*, and 13!. Because the dial string of 1311 matches multiple route patterns, the closest match rule is applied.

The route pattern 1[23]*xx* matches 200 destinations (1200 – 1299 and 1300 – 1399). The route pattern 13[0-4]X matches 50 destinations (1300 – 1349). The route pattern 13! matches an infinite number of destinations. CCM uses this pattern only if it is the only route pattern in the current matches table. The call is routed to the gateway or route list associated with the 13[0-4]X route pattern.

Note The system interdigit timeout defaults to 15 seconds. To change it, change the value associated with the CCM service parameter TimerT302_msec. This parameter defines the duration of the interdigit timer in milliseconds (ms). The default is 15,000 ms.

Call Routing Summary

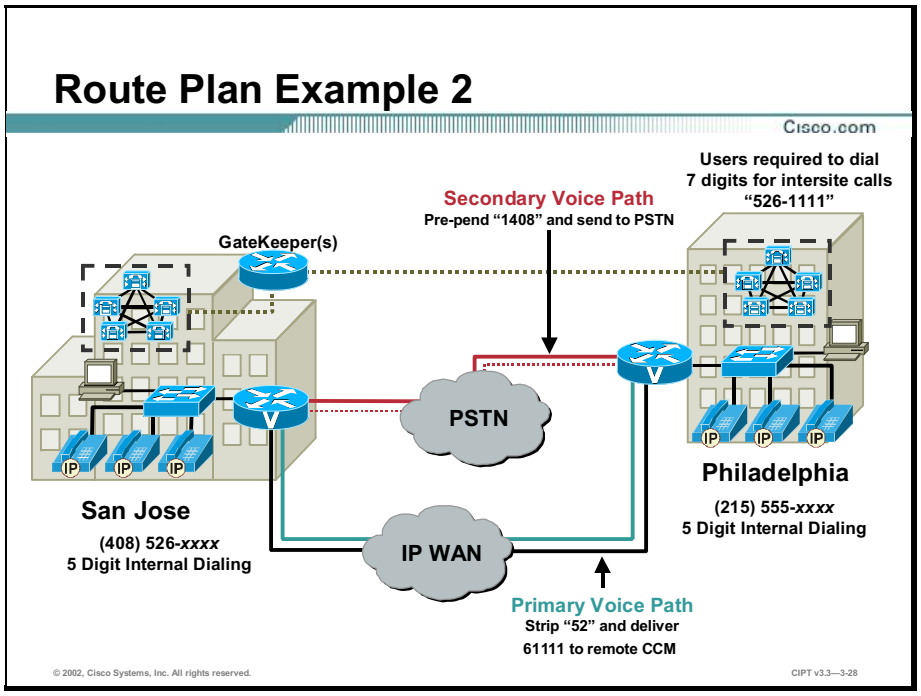
This topic summarizes the call-routing process.



The figure details a simple route plan. In this scenario, the network administrator configured two gateways (Digital_GW1 and Digital_GW2). These two gateways provide long-distance access to the PSTN. Digital_GW1 connects to a carrier that offers a long-distance rate of 7 cents per minute. Digital_GW2 connects to a carrier that offers a long-distance rate of 10 cents per minute.

The network administrator created a route group RG_PSTN to group these gateways and give first priority to Digital_GW1. The route list RL_PSTN utilizes the route group RG_PSTN. Currently, users only need to call long distance to one destination, which is a remote office in San Jose, California. Therefore, the administrator created the San Jose route pattern 408-555-*xxxx*. This route pattern then associates directly with the RL_PSTN route list.

Users also need to dial off-cluster to the PSTN to reach destinations within the local calling area. A separate gateway (Local_GW) connects to the local exchange carrier (LEC) for local PSTN calls. The administrator defined the route patterns 723-*xxxx*, 836-*xxxx*, and 868-*xxxx* for local calls. These route patterns point directly to the Local_GW gateway for local PSTN access through the LEC.

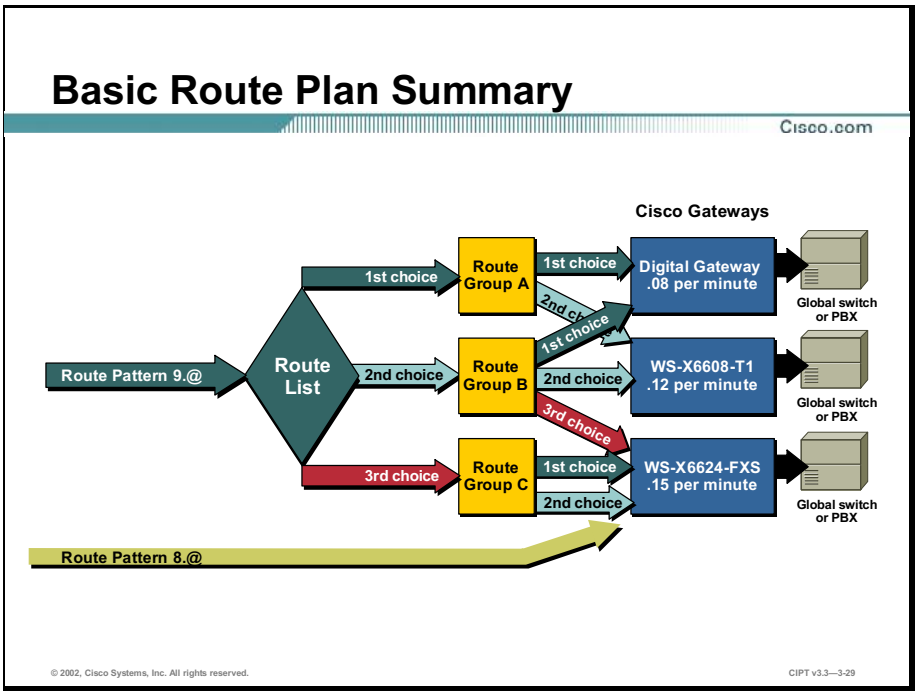


This figure details a more complex route plan, including features such as toll bypass and PSTN Fallback. In this example, the ABC Company has two main offices in San Jose and Philadelphia, Pennsylvania. The users at ABC Company dial five-digit extensions to reach users within the same site (5*xxxx* in Philadelphia and 6*xxxx* in San Jose). As you can see in the figure, each site has its own CCM cluster. You can classify these types of calls as on-cluster or internal calls.

The users also dial seven-digit numbers to reach users in other sites (526-*xxxx* to reach San Jose and 555-*xxxx* to reach Philadelphia). The calls between sites are off-cluster or external calls and require the configuration of a route plan. In this example, when a user in Philadelphia dials 526-1111, the local CCM cluster analyzes the dialed digits and looks for a match. In this case, 526-1111 matches the route pattern of 9.@ (which symbolizes the North America Dialing Plan).

At this point, the CCM knows that it must route this external call to a gateway. CCM now looks at the route list associated with the 9.@ route pattern to determine the correct gateway. In this example, CCM uses the gateway connected to the IP WAN first, for cost reasons (toll bypass). Before CCM can route the call across the IP WAN, it must perform digit manipulation (in the form of a called party transformation) so that the remote CCM can receive the call in a format that it understands (5 digit numbers).

If the IP WAN is down or the IP WAN does not have sufficient resources, CCM can route the call across the gateway connected to the PSTN. Since a call from Philadelphia to San Jose across the PSTN is a long-distance call, CCM must perform digit manipulation (in the form of a called party transformation) to change the dial string of 526-1111 to 1-408-526-1111, allowing the PSTN to understand the dialed digits. The call routing process is transparent to the end users, and they are not able to discern whether CCM has routed the call over the IP WAN or the PSTN.



A basic route plan consists of the following items: voice gateways, route groups, route lists, and route patterns.

Route patterns (required) should represent all valid digit streams. Route patterns can be assigned directly to a gateway, or to a route list for more flexibility, such as setting digital access gateway as first choice for the least expensive route.

Route patterns on gateway devices can be assigned to a specific port or to all ports (depending on the gateway).

Optional route list sets route group usage order. If a route list is used, you must also configure route groups.

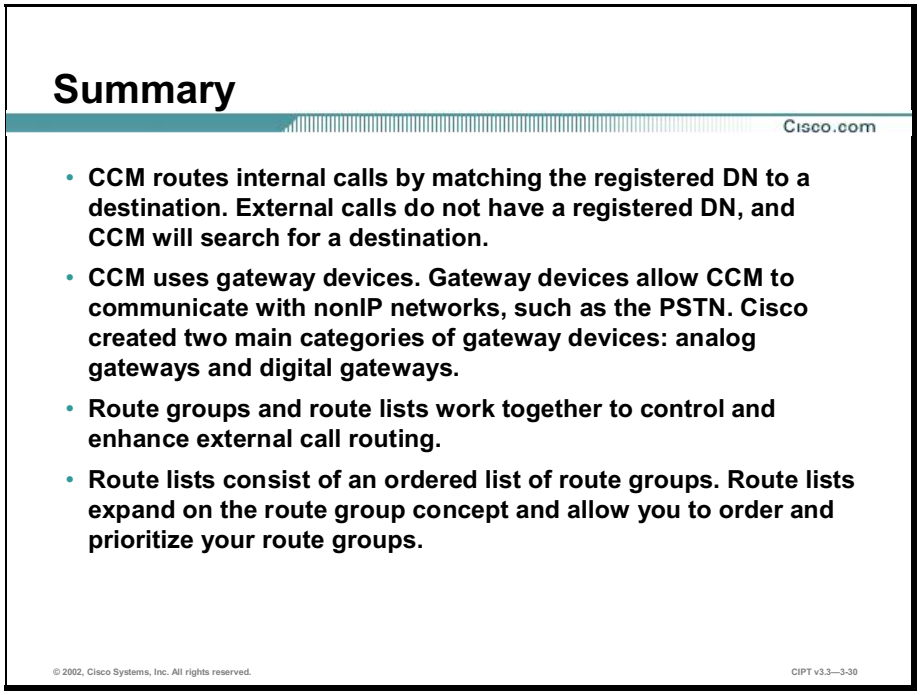
Optional route group(s) sets access gateway device usage order. This can be used to select the least expensive route and allows overflow from a busy or failed device to an alternate device.

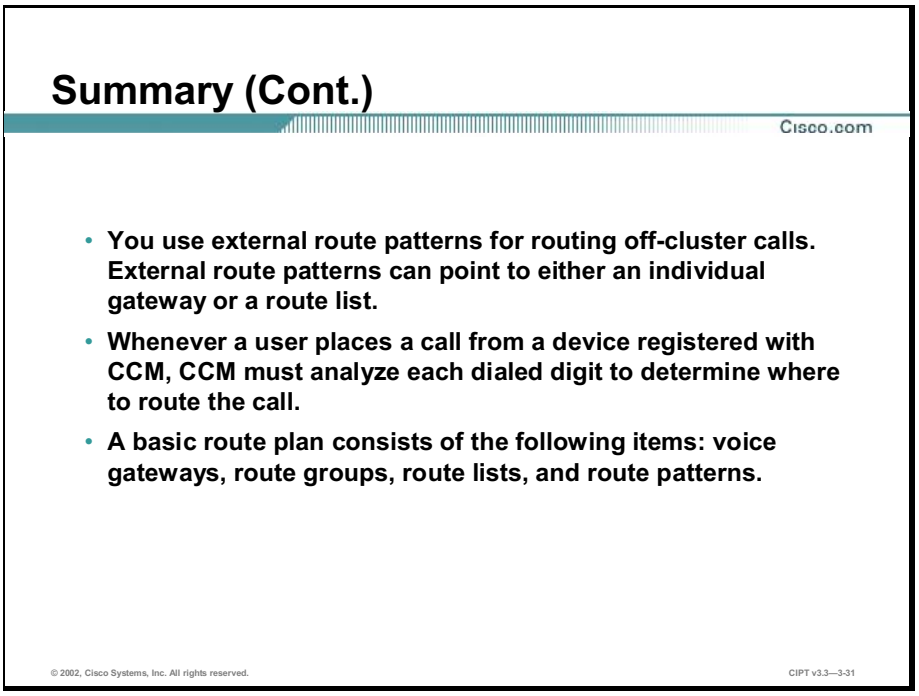
This is the recommended route configuration order: add the gateway, add a route group for the gateway, add a route list for the route group, and add route patterns to the route list

A route plan is required to route external or off-cluster calls in a Cisco IP telephony network. By understanding the call-routing process of CCM you can design your route plan to take advantage of cost considerations and redundancy.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Advanced Route Plan lesson

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of the following work together to control and enhance external call routing?

A) route groups and route lists

B) route lists and route patterns

C) translation patterns

D) none of the above

Q2) What is the key to making toll bypass and PSTN Fallback features transparent to your users?

A) digit manipulation

B) dialing 9 for second dial tone

C) route groups

D) route lists

Q3) Which of the following are valid wildcards? (Choose three.)

A) *

B) !

C) .

D) $

Q4) Which of the following sets the interdigit timeout to 15 seconds?

A) 15

B) 150

C) 1500

D) 15000

Q5) Which of the following constitutes a basic route plan? (Choose four.)

A) route groups

B) voice gateways

C) route lists

D) route patterns

E) CCM clusters

Q6) Which type of ports can be configured for an analog gateway? (Choose two.)

A) FXO

B) FXS

C) PRI

D) T1

Q7) What can be placed into a route list?

A) route groups

B) route patterns

C) route lists

D) devices

Advanced Route Plan

Overview

This lesson defines advanced route plans. Multiple digit manipulation is a feature offered by Cisco CallManager (CCM). Building simple route plans, advanced route plans, route filters, and digit transformation and translation patterns will customize route plans. You can use route plan reports to view all route patterns in a Cisco IP telephony clustered solution.

Importance

This lesson benefits those individuals who wish to increase employee productivity by providing abbreviated dialing and truncating the dialed digits to extend calls. This lesson also provides information on how to protect a Cisco IP telephony solution from toll fraud by applying route filters.

Objectives

Upon completing this lesson, you will be able to:

- Identify and define the tags and operatives used for route filters
- Define and configure digit discard instructions
- Use transformation masks
- Define and configure translation patterns
- View route plan reports for overlapping patterns

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Basic route plan construction

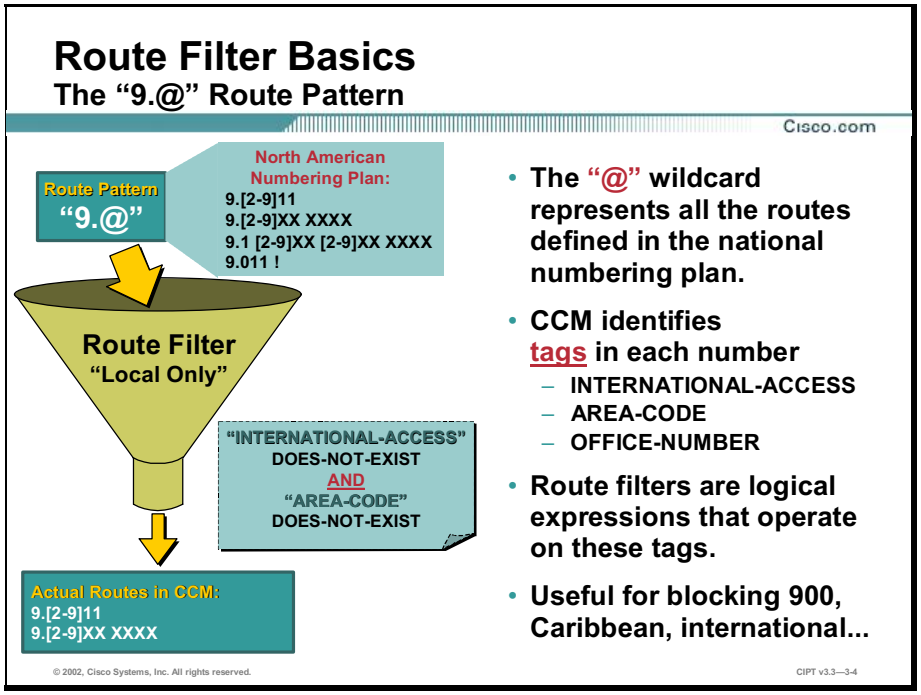
Outline

This lesson includes these topics:

- Overview
- Route Filters
- Digit Discard Instructions
- Transformation Masks
- Translation Patterns
- Route Plan Report
- Summary
- Lesson Review

Route Filters

This topic discusses the configuration and application of route filters in a route plan.



You can assign route filters to route patterns with the @ route pattern (9.@) to help reduce the number of route patterns required. You can accomplish this reduction by filtering what is included in the 9.@ route pattern.

Note	Route filters can be very complex. The most common use of route filters is local 7-digit dialing in North America. Most areas in North America are moving to a full 1+10 or 10-digit E.164 dialing.

When using the 9.@ route pattern, Cisco CallManager (CCM) recognizes that dialing is complete when the user dials 1+10 or just ten digits (local area codes without the 1). If the number dialed does *not* begin with a 1, CCM considers it a local area code and assumes dialing is complete after ten digits.

In an area where seven digits are dialed for local numbers, CCM cannot recognize which office exchange codes (N*xx*s) to use for routing unless you specifically code them as route patterns. Generally, telco service providers arrange many N*xx*s in a given area code—contiguously—where you could use route pattern wildcards to assist in your configuration. Coding these individual route patterns for N*xx*s could be extremely difficult. You can use a route filter to simplify this procedure.

A route filter called seven-digit dialing is always preconfigured in CCM. You should assign this route filter to any 9.@ route pattern in an area that uses seven-digit dialing. This route filter removes all local area codes. If a dialed number does not begin with a 1, then it is a seven-digit

number, and CCM considers dialing complete after seven digits. This would require you to configure local area codes specifically as separate route patterns. This is generally not an issue because the number of area codes in a geographical region is usually small.

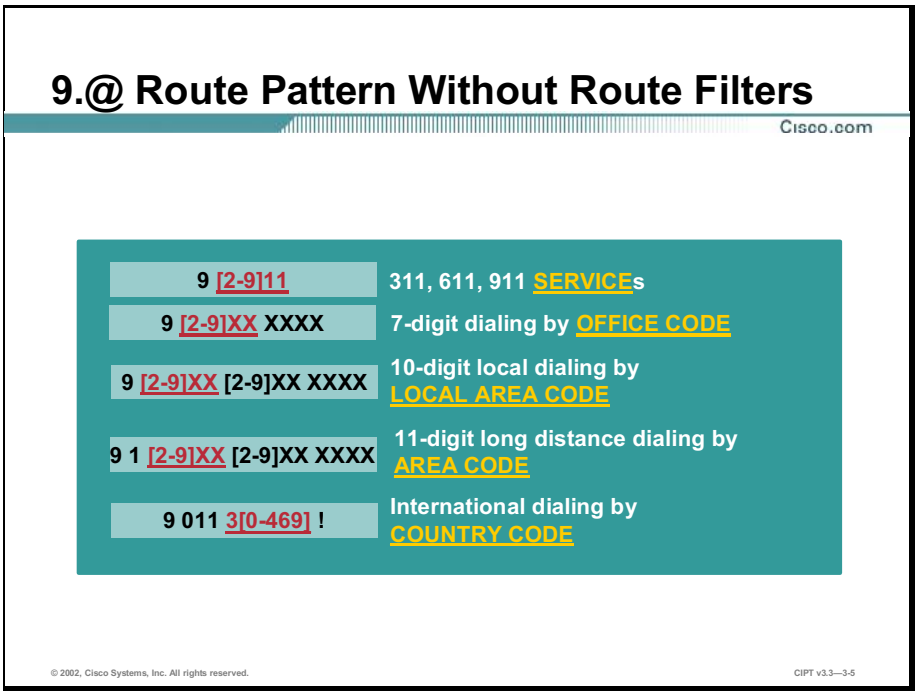
Table: Route Filter Tags

Tag Name	Example Pattern	Description
AREA-CODE	1 **214** 555 1212	The area code in an 11-digit long distance call.
COUNTRY-CODE	011 **33** 123456#	The country code in an international call.
END-OF-DIALING	011 33 123456**#**	The #, which terminates inter-digit timeout for an international call.
INTERNATIONAL-ACCESS	**01** 1 33 123456#	The initial 01 of an international call.
INTERNATIONAL-DIRECT-DIAL	01 **1** 33 123456#	The digit that denotes the direct-dial component of an international call.
INTERNATIONAL OPERATOR	01 **0**	The digit that denotes the operator component of an international call.
LOCAL-AREA-CODE	**214** 555 1212	The area code in a 10-digit local call.
LOCAL-DIRECT-DIAL	**1** 555 1212	The initial 1 required by some 7-digit calls.
LOCAL-OPERATOR	**0** 555 1212	The initial 0 required for operator-assisted local calls.
LONG-DISTANCE-DIRECT-DIAL	**1** 214 555 1212	The initial 1 required for long distance direct dialed calls.
LONG-DISTANCE-OPERATOR	**0** 214 555 1212	The initial 0 required for operator-assisted long distance calls.
NATIONAL-NUMBER	011 33 **123456**#	The national number component of an international call.
OFFICE-CODE	1 214 **555** 1212	The office exchange code of a North American call.
SATELLITE-SERVICE	011 881**4**1234#	A specific value associated with calls to the satellite country code.
SERVICE	1 **411**	Access to local telephony provider services.
SUBSCRIBER	1 214 555 **1212**	A particular extension served by a given exchange.
TRANSIT-NETWORK	101 **0321** 1 214 555 1212	Long distance carrier code.
TRANSIT-NETWORK-ESCAPE	**101** 0321 1 214 555 1212	The escape sequence used for entering a long distance carrier code.

The types of patterns included when a 9.@ route pattern is added are:

- No filter
- Service Exist
- Country-code does-not-exist

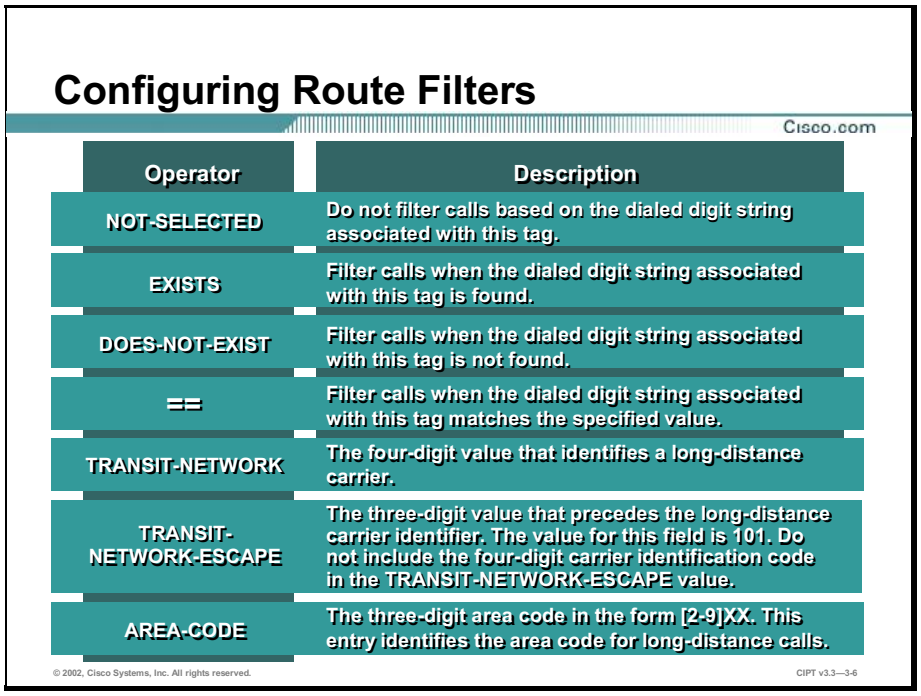
- Area Code = 900



The figure here shows the individual patterns that CCM adds to the 9.@ route pattern without filters.

The @ symbol wildcard matches all North American Numbering Plan (NANP) numbers. The following route patterns are examples of NANP numbers that are included in the @ wildcard:

- 0
- 1411
- 19725551234
- 101028819725551234
- 01133123456789



You can configure a route filter by using the Cisco CallManager Administration window.

Step 1 Select the **Route Plan** menu.

Step 2 Choose **Route Filter** from the menu bar.

Step 3 Select **NANP** from the Dial Plan menu.

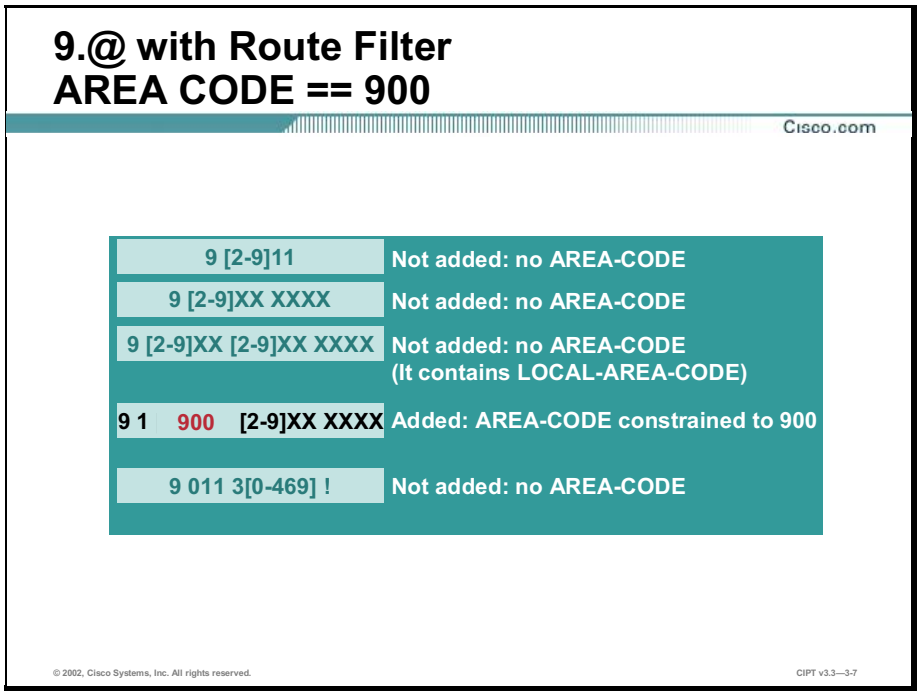
Step 4 Enter a name in the Route Filter Name field. The name can consist of up to 50 alphanumeric characters, and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Each route filter name must be unique to the route plan.

The tag operators in the route filter determine if CCM filters a call based on the existence or the contents of the dialed digit string associated with that tag. The route filter operators—EXISTS and DOES-NOT-EXIST—check for the existence of that part of the dialed digit string. The operator = = matches the actual dialed digits with the specified value or pattern.

The following are route filter examples:

- A route filter that uses the variable AREA-CODE and the operator DOES-NOT-EXIST, selects all dialed digit strings that do not include an area code.
- A route filter that uses the variable AREA-CODE, the operator = =, and the entry 515, selects all dialed digit strings that include the 515 area code.
- A route filter that uses the variable AREA-CODE, the operator = =, and the entry 5[2-9]*x*, selects all dialed digit strings that include area codes in the range of 520 through 599.

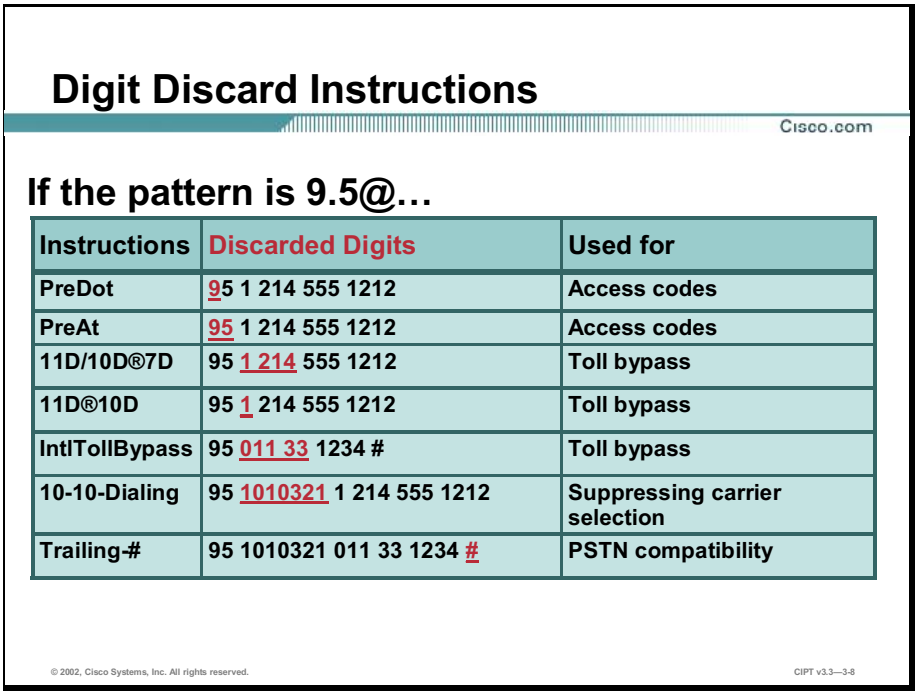
- A route filter that uses the variable TRANSIT-NETWORK, the operator = =, and the entry 0288, along with the variable TRANSIT-NETWORK-ESCAPE, the operator = =, and the entry 101, selects all dialed digit strings with the carrier access code 1010288.



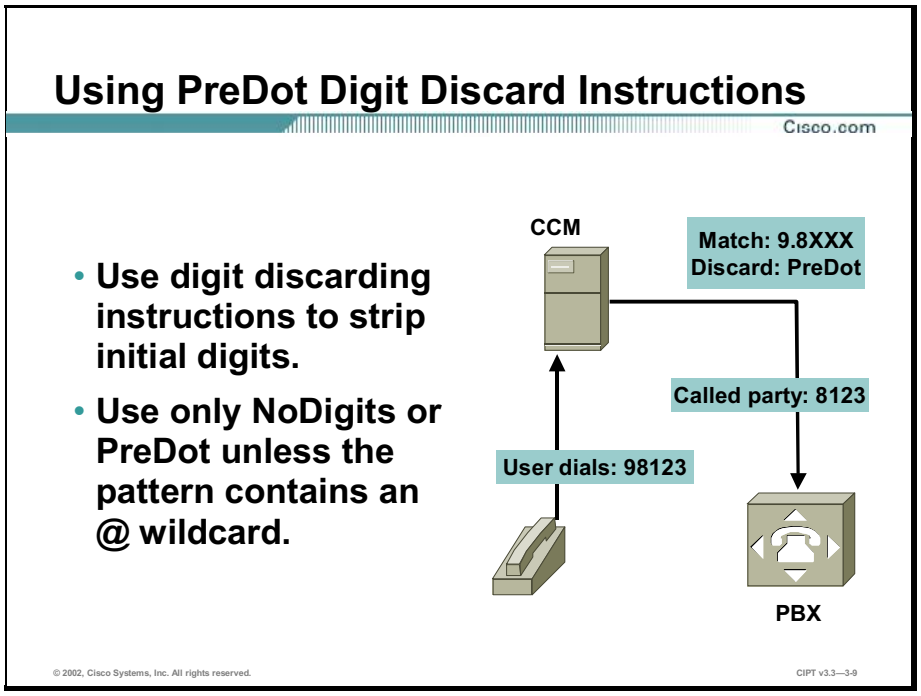
The figure here shows the patterns that CCM adds when you apply the AREA-CODE = = 900 filter to the 9.@ route pattern. A route filter that uses the variable AREA-CODE, the operator = =, and the entry 900, selects all dialed digit strings that include the 900 area code. After you apply the route filter to the route pattern, you are given the configuration option to Route this pattern or Block this pattern. By selecting the Route this pattern radio button on the Route Pattern Configuration window, you allow all calls where AREA-CODE = 900, while denying all other route patterns. Generally, this is not your desired result. Instead, select the **Block this pattern** radio button to prevent all calls where AREA-CODE = 900, but allow all other route patterns.

Digit Discard Instructions

This topic discusses the digit discard instructions available in CCM.



Digit discard instructions allow conversions of a dialed number specific to a national numbering plan. In general, digit discard instructions apply only to route patterns that contain the @ wildcard. You can use the digit discarding instruction PreDot with route patterns that use the "." wildcard *even if the route patterns do not contain the @ wildcard*. CCM applies digit discard instructions to the called party transformation masks at the route pattern, the route details of a route list, or a translation pattern. Digit discard instruction identifiers, shown in the figure here, are additive. The digit discard instruction PreDot 10-10-Dialing combines the effects of each individual identifier. If you do *not* want to discard digits, select **NoDigits**.

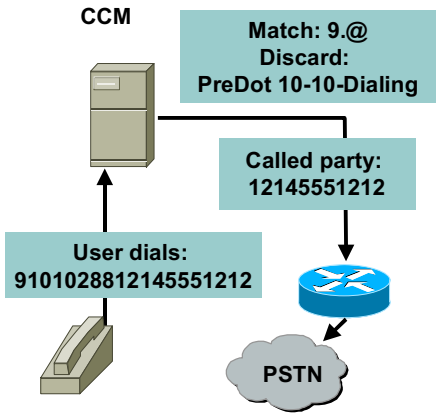


CCM applies the PreDot discard digits instruction to the 9.8*xxx* route pattern, strips the 9 from the dialed digits, and sends only the 8123 to the PBX.

Using Compound Digit Discard Instructions

Cisco.com

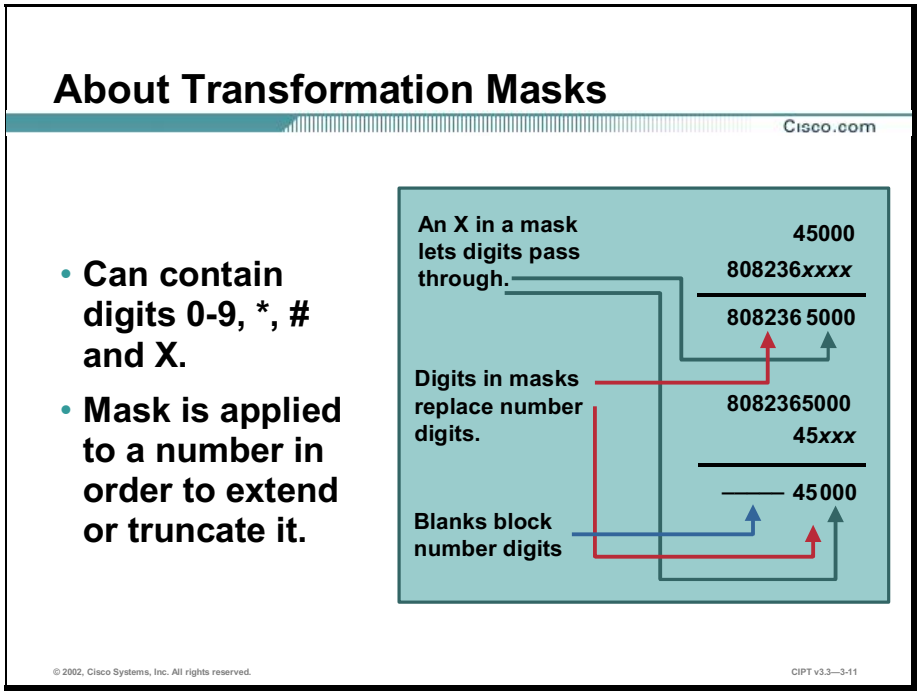
- Use digit discarding instructions to discard whole sections of the dialed number.
- All digit discarding instructions are available.



CCM applies the PreDot 10-10-Dialing digit discard instruction to the 9.@ route pattern, strips the 91010288 from the dialed digits, and sends only 12145551212 to the gateway device.

Transformation Masks

This topic discusses transformation masks in a route plan.



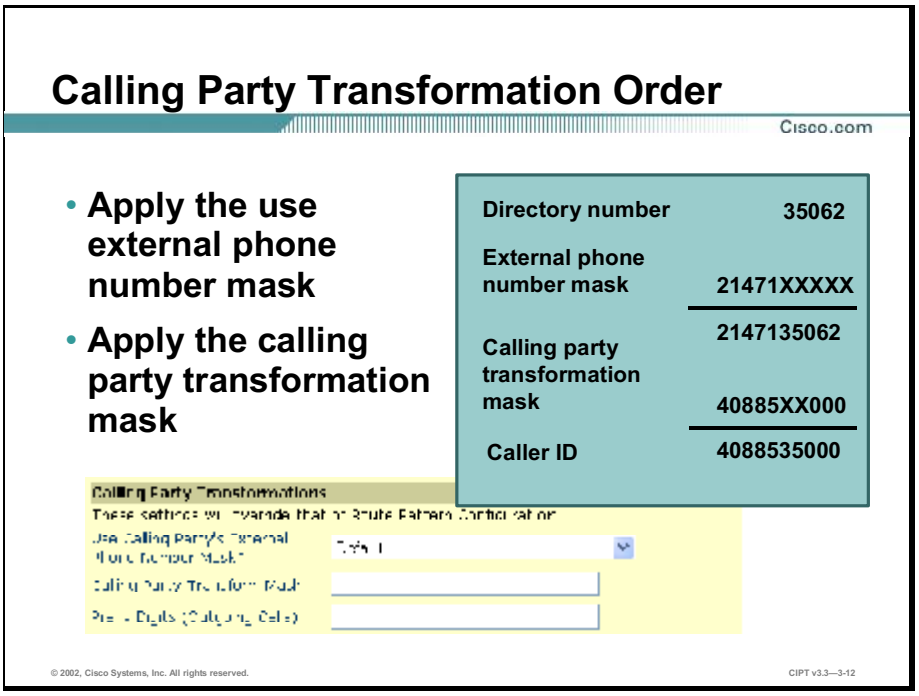
Dialing transformations allow the call routing component to modify either the calling number or the dialed digits of a call. Transformations that modify the calling number are *calling-party* transformations; transformations that modify the dialed digits are *called party* transformations.

A mask operation allows the suppression of leading digits, the change of some digits while leaving others unmodified, and the insertion of leading digits.

A mask operation requires two pieces of information: the number you wish to mask and the mask itself.

In the mask operator, CCM overlays and aligns the number with the mask so that the last character of the mask aligns with the last digit of the number. CCM uses the corresponding digit of the number wherever the mask contains an *x*. If the number is longer than the mask, the mask obscures the extra digits.

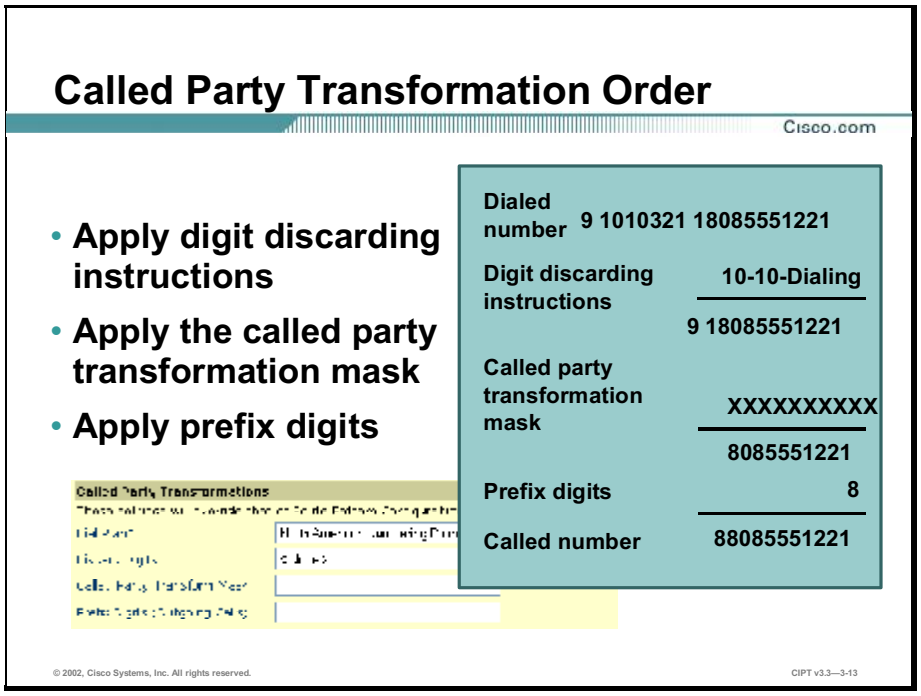
Note CCM also uses a concept called *translation patterns*, which rely heavily on dialing transformations to operate. Translation patterns and dialing transformations are separate concepts. Dialing transformations is a generic concept that refers to any setting in CCM that can change the calling number or dialed digits. Dialing transformations appear not only in the Transformation Pattern Configuration window but also in the Route Pattern Configuration window, numerous gateway configuration windows, and in service parameters.



The examples shown are the applicable settings for *calling party* and *called party* transformation and the order in which CCM processes those instructions. You can configure three types of calling party transformations in the call-routing component and on route lists:

- Use the external phone number mask, which instructs the call-routing component to use the external phone number of a calling station rather than its directory number (DN) or the Caller ID information. You can apply the external phone number mask on a line-by-line basis through the DN configuration screen on the device.
- The calling-party transformation mask allows the suppression of leading digits, leaves other digits unmodified, and inserts leading digits.
- Prefix digits allow the pre-pending of specified digits to the calling number.

CCM applies the transformations in the order listed in the example.



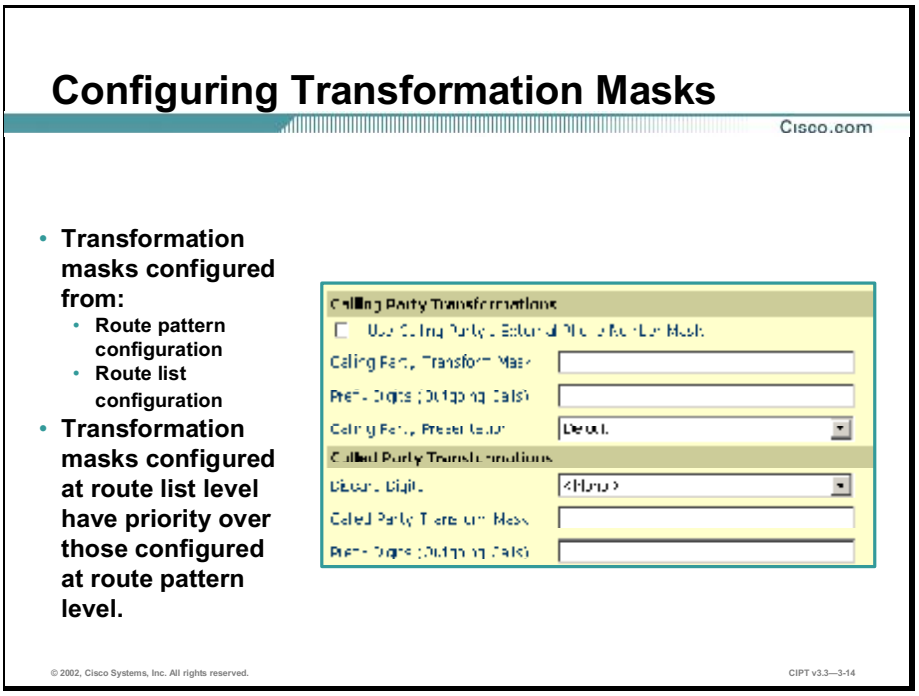
You can configure the following three types of called party transformations in the call-routing component and on route lists:

- Digit discarding instructions allow the discarding of subsections of numbers in the NANP. They are critical for implementing toll-bypass solutions. This occurs when CCM must convert the long-distance number that the calling user has dialed into a local number. This number allows CCM to pass the digits to the PSTN. You can also use digit discard instructions to discard PSTN access codes, such as 9.

- Called party transformation allows the suppression of leading digits, changes the existing digits while leaving others unmodified, and inserts leading digits.

- Prefix digits allow pre-pending of one or more digits to the called number.

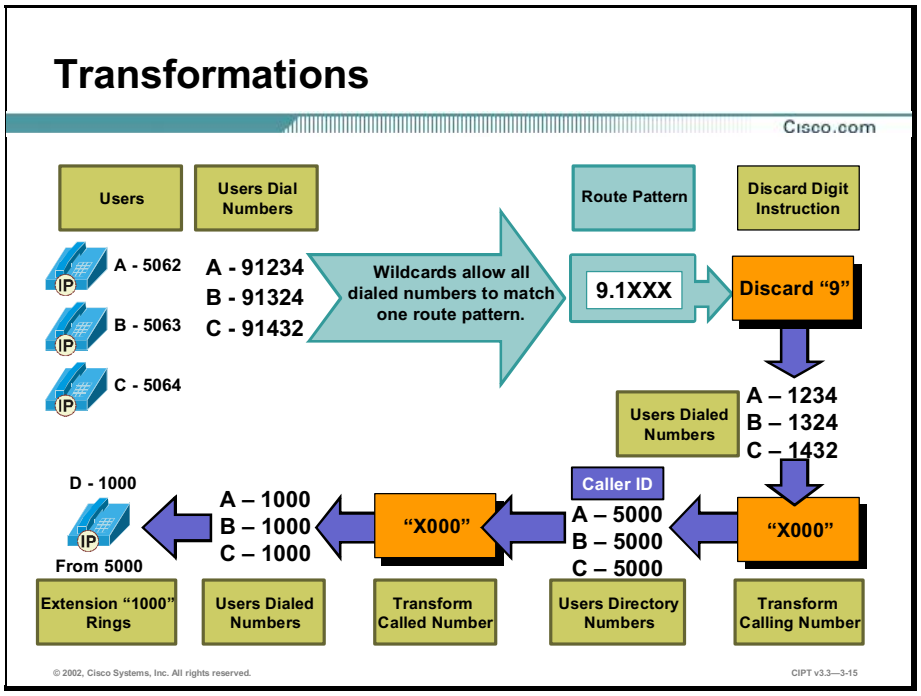
CCM applies the transformation in the order listed in the example.



The calling party transformation setting used in route lists applies to the individual route groups that make up the list, rather than the entire route list. The calling party transformations settings assigned to the route groups in a route list override any calling party transformations settings assigned to a route pattern associated with that route list.

Because you can be more specific, network administrators usually apply transformation masks at the route list level. This way, you can assign a different transformation mask for each route group in the route list.

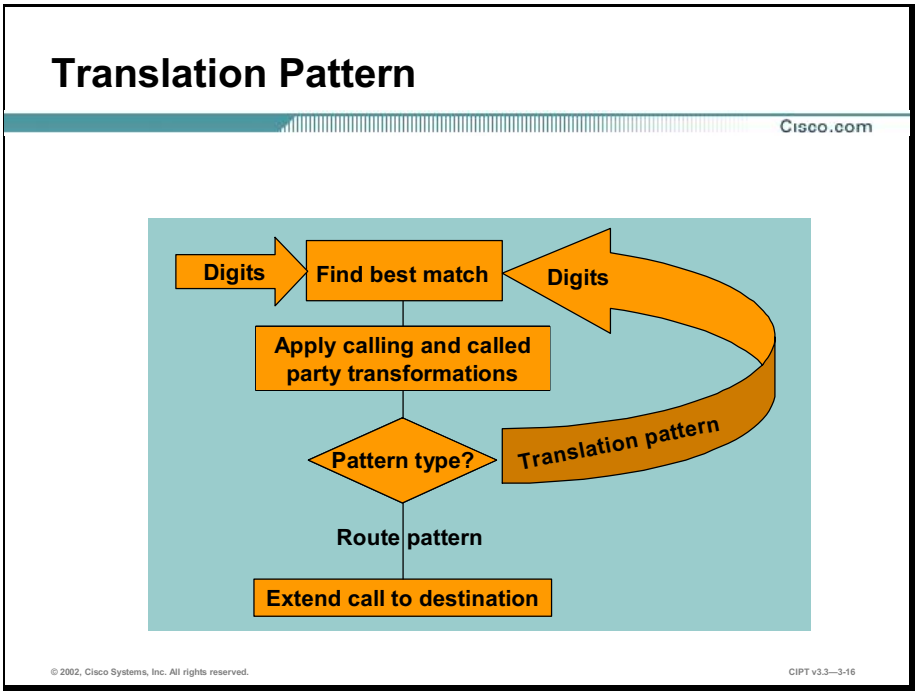
For example, a network administrator has two route groups created: the PSTN route group and the IP WAN route group. Each of these route groups contain multiple gateways that connect to their respective network. When CCM forwards a call to a gateway in the PSTN route group, the network administrator applies a mask that transforms the number into an E.164-compliant phone number. However, when CCM uses a gateway from the IP WAN route group, CCM leaves the number as a four-digit extension.



The figure summarizes the transformations that are available within CCM. User A has a DN of 5062. This user dials DN 91234. The dialed number matches the route pattern 9.1*xxx*. The discard digit instructions contain the instructions to discard the 9. The dialed number is now 1234. The calling number 5062 now passes through the calling number transformation mask, which contains instructions to change the last three digits of the calling party number to 000. The new calling number is 5000. CCM then passes the called number 1234 through the called number transformation *x*000 that changes this number to 1000. The result is a calling party number of 5000 and a called number of 1000.

Translation Patterns

This topic discusses the functionality and configuration of translation patterns.

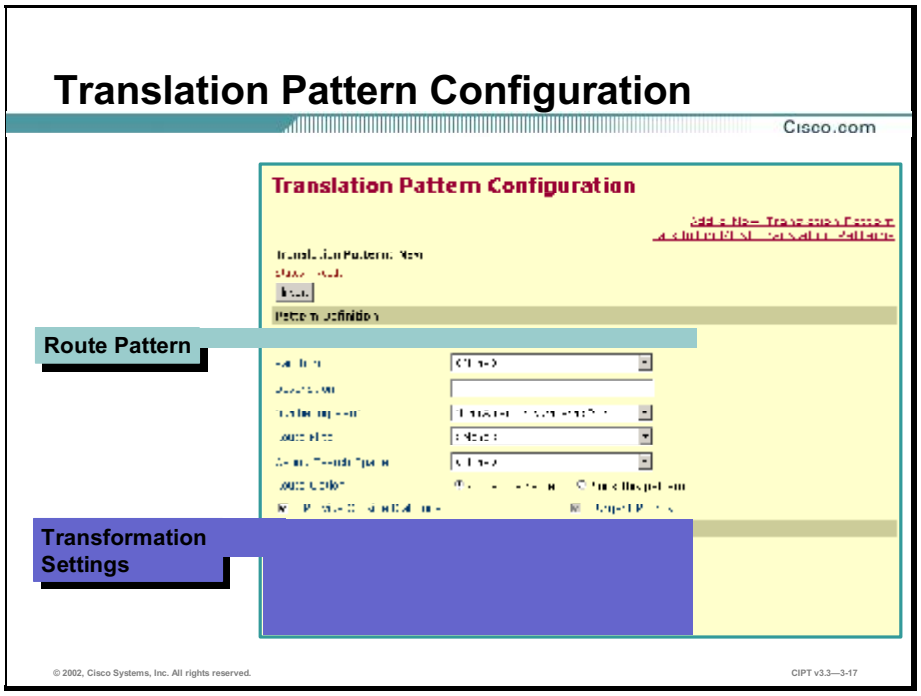


Translation patterns allow routing indirection into the call-routing process. The patterns create defining aliases for the endpoints in the network. The following are examples of these aliases:

- Security desk and operator functionality
- Hotline private line, automatic ringdown (PLAR) functionality
- Extension mapping from the public to a private network
- Insertion of access codes in the Received Calls and Missed Calls menus of Cisco IP Phones
- Multiple tenant applications

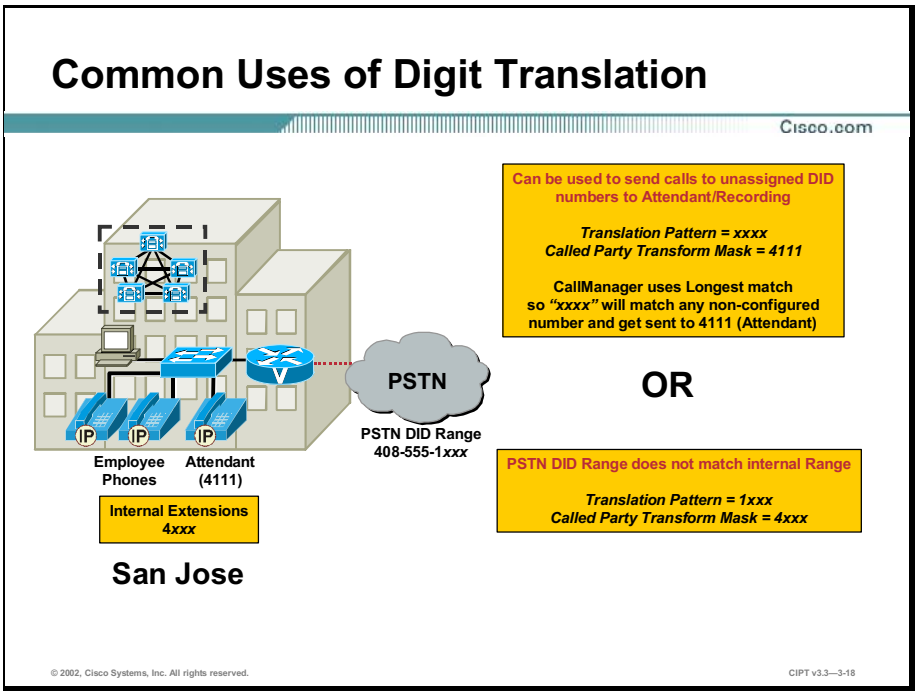
Translation patterns use the results of called party transformations as a set of digits for a new analysis attempt. CCM uses the results of the second analysis attempt to determine which destination to ring.

The second analysis attempt might match a translation pattern. In this case, CCM applies the calling and called party transformations of the matching translation pattern and uses the results as the input for another analysis attempt. To prevent routing loops, CCM breaks chains of translation patterns after ten iterations.



Configuration of a translation pattern is similar to configuration of a route pattern. Each pattern has calling and called party transformations and wildcard notation. The difference is that when CCM applies the translation pattern, it starts the digit analysis process over and routes the call through a new path if necessary.

To configure a translation pattern, click the **Route Plan** menu and choose **Translation Pattern**. You can define the route pattern to match and the calling or called party transformation settings that you would like to apply.

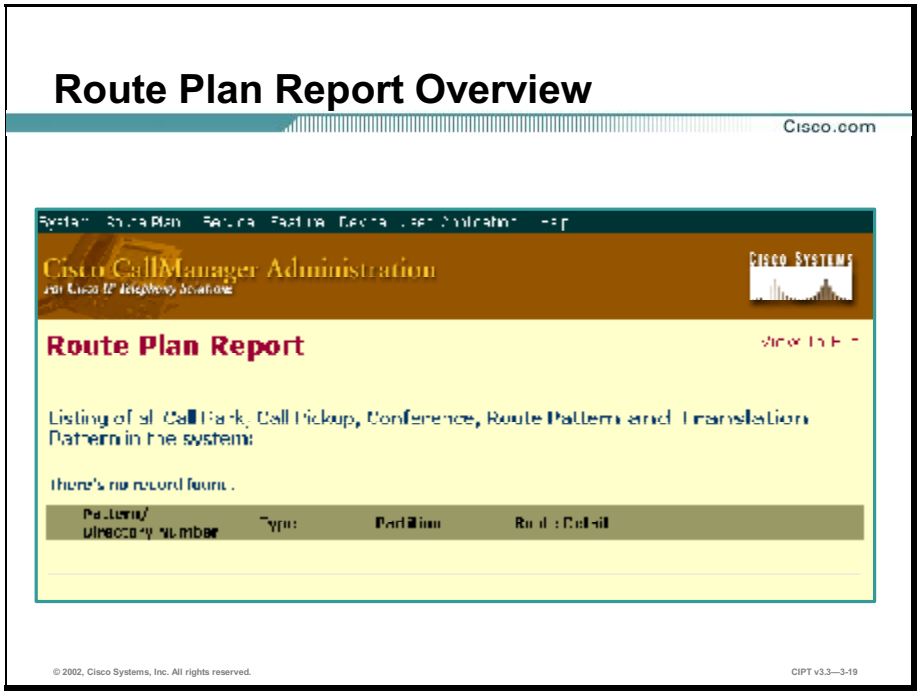


The figure here shows an application for translation patterns. When the Direct Inward Dialing (DID) range from the central office (CO) does not match the internal DN range, you can use a translation pattern to make the connection.

In the figure, a San Jose, California company has a PSTN DID range of 408-555-1*xxx*. However, all of the internal four-digit extensions begin with 4*xxx*. When the company receives an incoming call, the company could use digit discard instructions to remove the 555 from the beginning of the number. However, the 1*xxx* extension still remains. Instead, the translation pattern could apply a 4*xxx* called party transformation mask. This would convert the 1*xxx* external DID range to a 4*xxx* internal range. After CCM applies the transformation mask, it reanalyzes the dialed number and directs it to the correct internal extension.

Route Plan Report

This topic provides an overview of the route plan report.

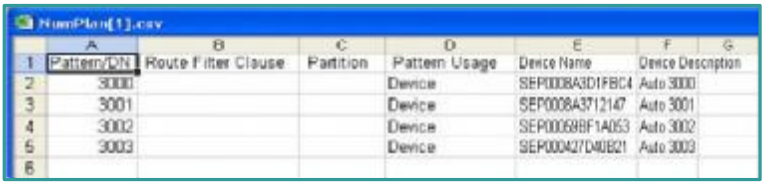


The route plan report is a listing of all the call park numbers, call pickup numbers, conference numbers (such as Meet-Me numbers), route patterns, and translation patterns in the system. The route plan report allows you to view either a partial or full list, and go directly to the associated configuration windows. You can accomplish this by selecting a route pattern, partition, route group, route list, call park number, call pickup number, conference number, or gateway.

The route plan report allows you to save report data into a CSV file that you can import into other applications. The CSV file contains more detailed information than the web pages, including DNs for phones, route patterns, and translation patterns.

Generating a Route Plan Report

Cisco.com



- **Select Route Plan Report from the Route Plan menu.**
- **Click the View In File hyperlink to save the file to a .csv template.**

To view a route plan report in a CSV file follow the steps below.

Step 1 Select **Route Plan**>**Route Plan Report**.

The route plan report shows 50 items per window.

Step 2 Select **View In File**. A NumPlan.csv download dialog box appears.

From this dialog box, you can either save or open the file.

Step 3 Select **Save File** in the dialog box.

Another window appears allowing you to save this file to a location of your choice.

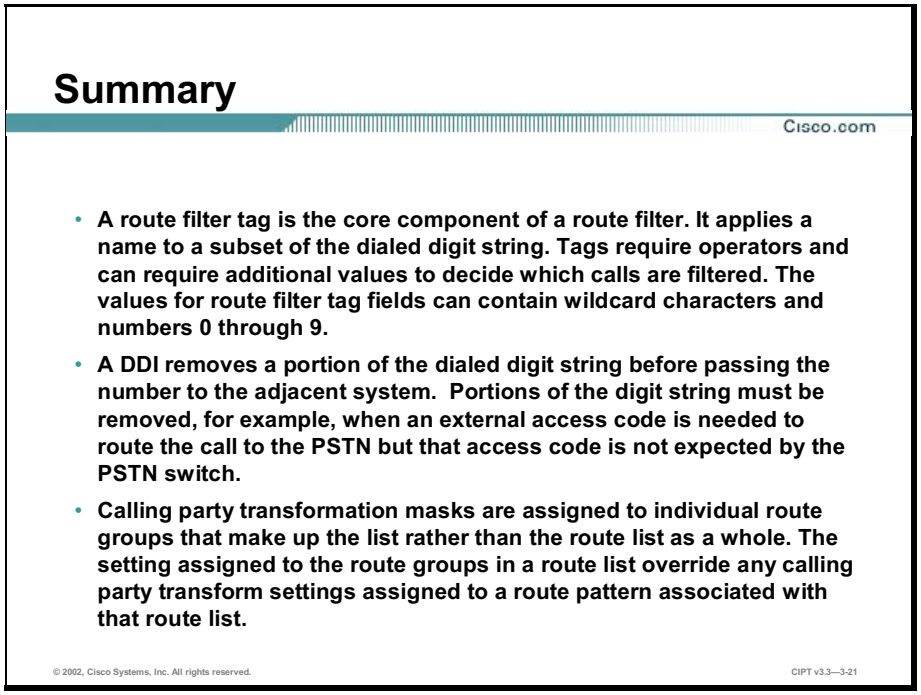
Note You may change the name of the file, but the file name must have a .csv extension.

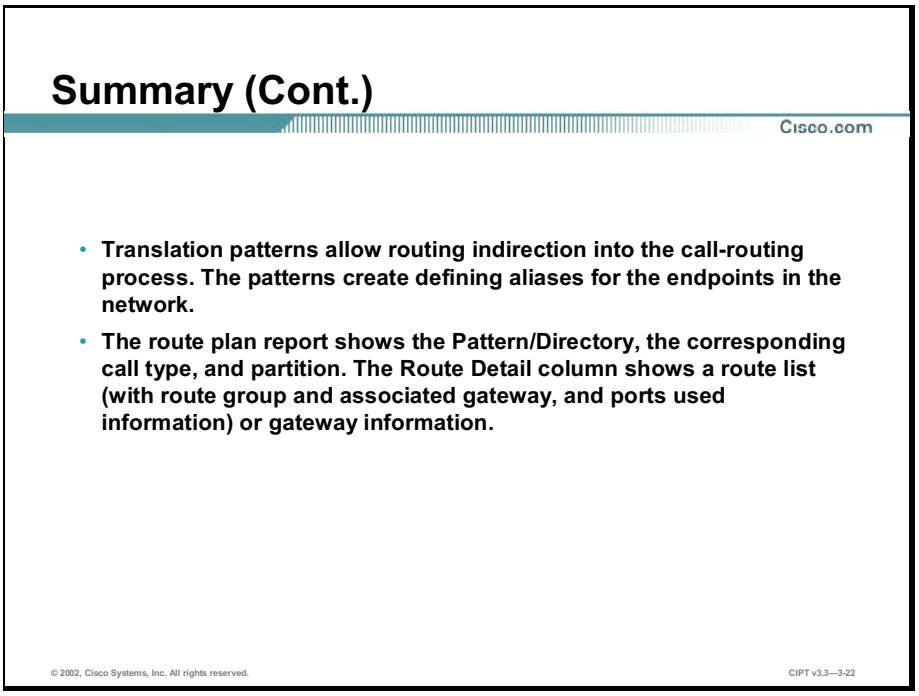
Step 4 Select the location in which to save the file and click **Save**. The file should now be saved to the location you designated.

Step 5 Locate the CSV file you just saved and double-click on its icon to view it.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Telephony Class of Service lesson

References

For additional information, refer to these resources:

- Smith, A., Chris Peace, Delon Whetton, and John Alexander. *Cisco CallManager Fundamentals: A Cisco AVVID Solution.* San Jose, California: Cisco Press; 2001.

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of these file extensions does CCM use by default to generate a route plan report?

A) **.**csv

B) .doc

C) .pdf

D) .txt

Q2) What does CCM do when dialed digits match a translation pattern?

A) extends the call to the destination

B) forwards the call to a route pattern

C) selects the closest match to that pattern

D) sends the transformed digits through digit analysis one more time

Q3) When DN 8500 calls and a calling transformation mask of 972555*xxxx* is applied, what CLID is sent?

A) 8500

B) 5558500

C) 9725558500

D) 19725558500

Q4) What are the final digits CCM sends when the discard digits instruction PreDot is applied to the 9.8085551212 pattern?

A) 98085551212

B) 5551212

C) 95551212

D) 8085551212

Q5) Network administrators use route filters with which route pattern wildcard?

A) *x*

B) ?

C) !

D) @

Telephony Class of Service

Overview

In a Cisco IP telephony solution, it is important to provide levels of access for the different users in your organization. This lesson discusses how to implement partitions and calling search spaces to provide a telephony class of service (CoS) based on users and locations. You will also learn the importance of partitions and calling search spaces as they apply to emergency call routing.

Importance

This lesson benefits network administrators who want to provide CoS in a Cisco IP telephony solution, which provides increased security and defines limits on where users can call or forward their calls. This lesson provides information on how to configure partitions and calling search spaces in order to help the overall design for security and safety on the network.

Objectives

Upon completing this lesson, you will be able to:

- Identify and describe partitions and calling search spaces using examples and analogies
- Configure partitions and apply them within a Cisco IP telephony solution
- Configure calling search spaces and apply them within a Cisco IP telephony solution
- Identify the considerations when using partitions and calling search spaces to address problems with geographic locations, multiple tenants, and user classes
- Identify the purpose of the Cisco Emergency Responder

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- A basic understanding of Cisco CallManager Administration and basic route plan

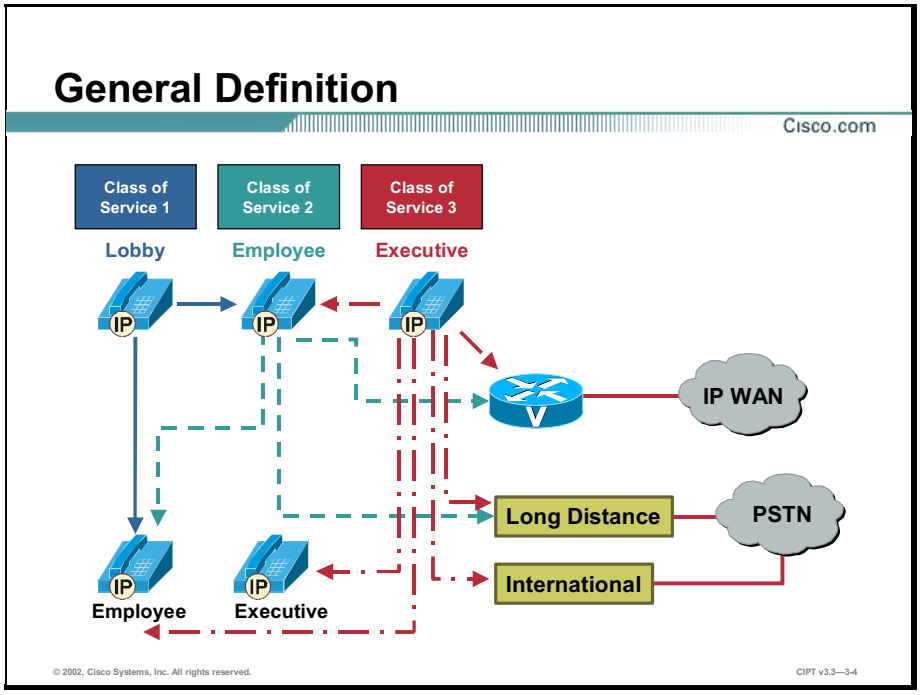
Outline

This lesson includes these topics:

- Overview
- Class of Service
- Partitions
- Calling Search Spaces
- Using Partitions and Calling Search Spaces for Emergency Calls
- Cisco Emergency Responder
- Summary
- Lesson Review

Class of Service

This topic provides a general definition and analogies for class of service (CoS), partitions, and calling search spaces.

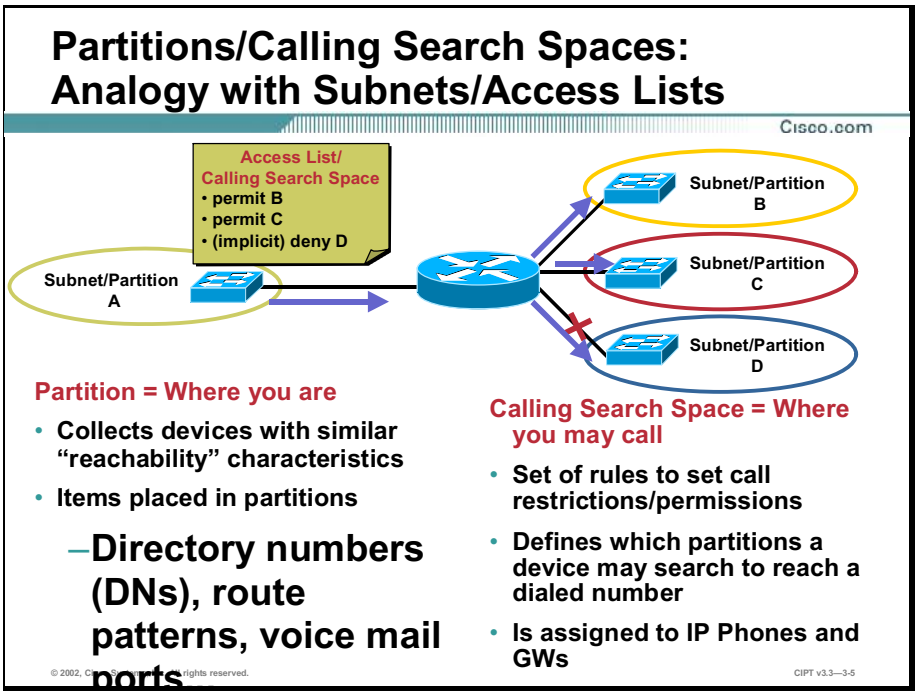


CoS is best defined in Newton's Telecom Dictionary, 18th Updated and Expanded Edition. The dictionary has three definitions for CoS: 1) Internal to a PBX, 2) On the public switched network, and 3) On a packet switched network, courtesy of Cisco Systems, Inc.

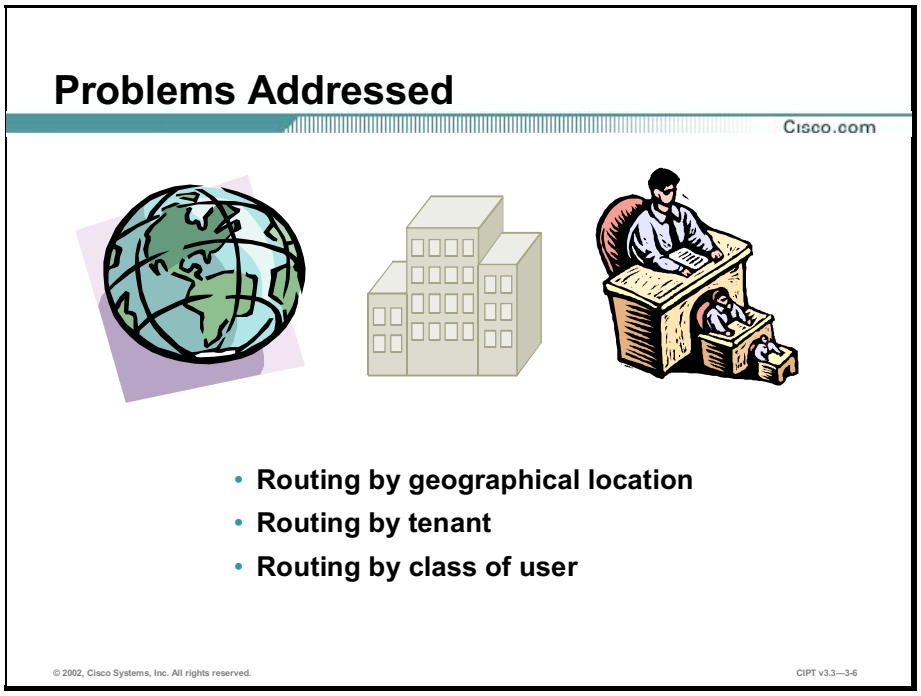
CoS is defined by the first Newton definition, Internal to a PBX, and states:

1. *"Each telephone in a corporation telephone system may have a different collection of privileges and features assigned to it, such as access to long distance, international calls, 900 area code calls, 976 local calls, etc. Let us say that you are concerned that your people will waste the company's money by frivolously calling expensive numbers, so you might wish to define "Class of Service" assignments in your PBX. You could have one that's called "ability to dial everywhere except 900 area code, international calls and all 976 numbers." That could be Class of Service Assignment B. When you give a telephone to an employee, you could give that person COS B. Big bosses, on the other hand, might need to call internationally, but not 900 area code or 976 calls. That could be called Class of Service Assignment A. Class of Service assignments, if properly organized, can become an important tool in controlling telephone abuse."*

Cisco CallManager (CCM) has the ability to apply the above CoS to devices by configuring partitions and calling search spaces.



Partitions and calling search spaces draw an analogy to routers with access lists. You can think of a partition as an IP subnet where you place users. In addition, you can compare a calling search space to an inbound access list that dictates the subnet that you can reach.



Partitions and calling search spaces are designed to address three specific problems:

- **Routing by geographical location:** Partitions and calling search spaces ensure that CCM does not redirect callers to the incorrect geographical location. This is critical in the case of emergency calling.

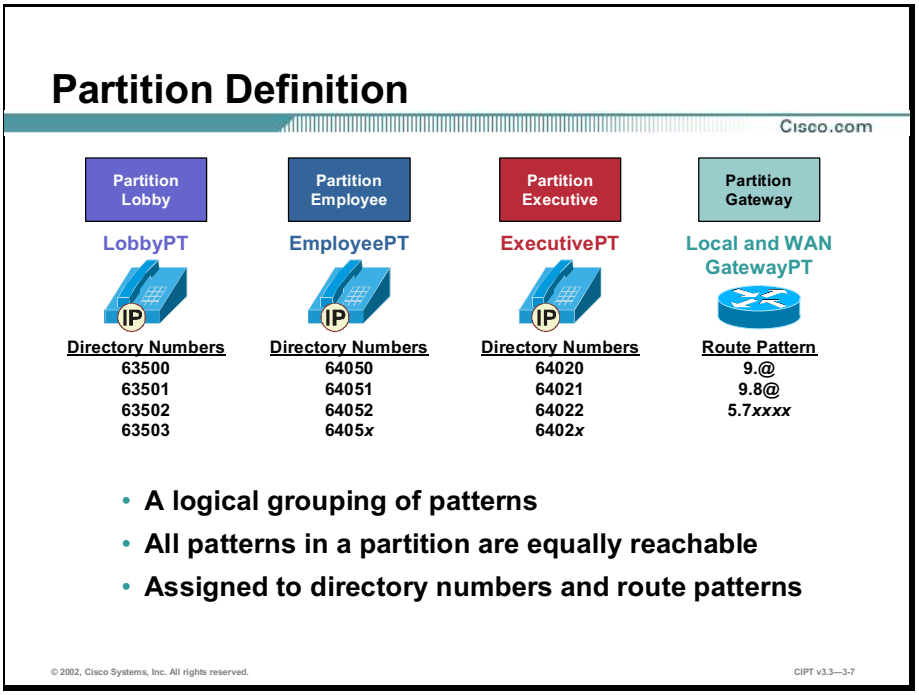
- **Routing by tenant:** Partitions and calling search spaces dictate the numbers that tenants can reach. This is useful in a multitenant building with a centrally managed telephone system.

- **Routing by class of user:** Partitions and calling search spaces dictate the numbers individuals are able to dial. This is useful for restricting employees or lobby telephones from dialing long-distance numbers.

Partitions and calling search spaces provide a way to segregate the global dialable address space. The global dialable address space is the complete set of dialing patterns to which CCM can respond.

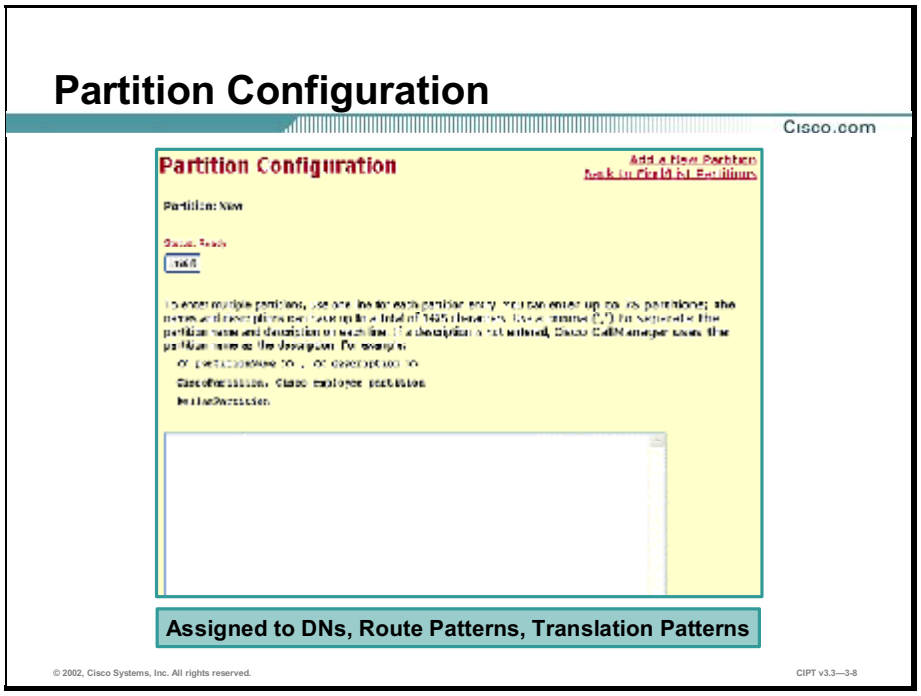
Partitions

This topic discusses partitions and the configuration of partitions.



A partition is a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Items typically placed in partitions are IP Phones, DNs, and route patterns. These are entities associated with the DNs that users dial. For simplicity, partitions are usually named for their characteristics, such as AZ911PT and so on. When a DN or route pattern is placed into a certain partition, a rule is created that specifies the devices that are able to call that directory number or route pattern.

Partitions do not significantly impact the performance of digit analysis, but every partition specified in the calling search space of a device does require an additional pass through the analysis data structures. Digit analysis looks through every partition in a calling search space for the best match. CCM uses the order of the partitions listed in the calling search space to break ties only when there are equally good matches in two different partitions. If you do not specify a partition for a route pattern or a DN, CCM lists the route pattern or DN in the null partition to resolve dialed digits. Digit analysis always looks through the null partition last.



To configure partitions, click the **Route Plan** menu and choose **Partition**. When the **Find and List Partition** window appears, click the **Add a New Partition** hyperlink. The **Partition Configuration** window shown in the figure appears. From here, you can add any number of partitions using the following syntax:

Partition_Name, Description

Cisco CallManager Administration requires that you enter the partition name only. However, adding a description for the partition can be useful for documentation purposes.

Example

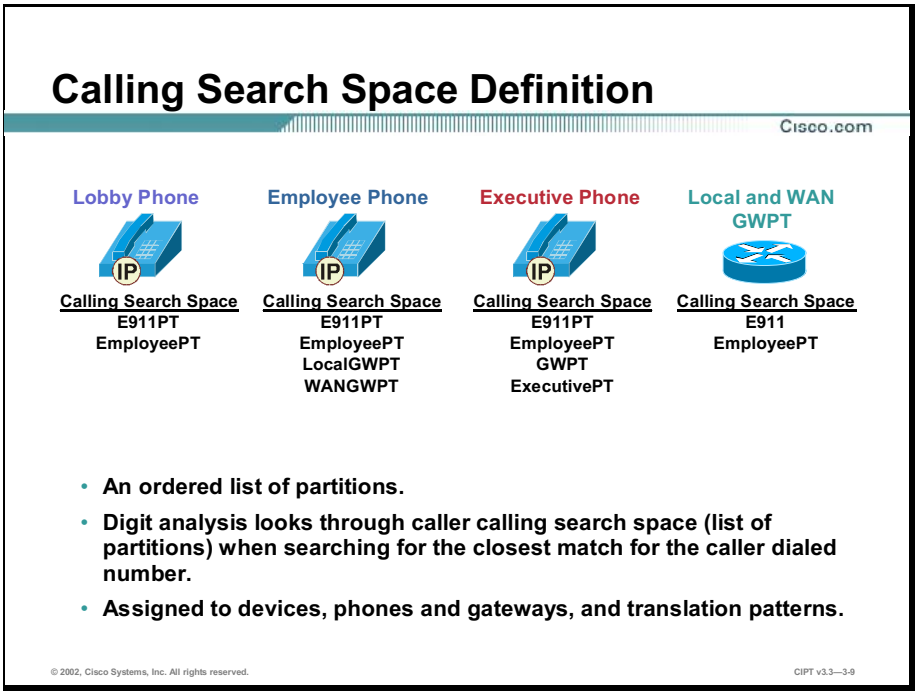
The network administrator at the ABC Company must allow certain individuals to call the DNs in the 1*xxx* and 2*xxx* ranges. Before assigning the DNs to a partition, the administrator must first configure the partitions using the Partition Configuration page in Cisco CallManager Administration. The administrator could add the necessary partitions using the following format:

- DN_1*xxx*, Directory Numbers 1000-1999
- DN_2*xxx*, Directory Numbers 2000-2999

After the administrator adds the partitions, he must assign DNs. To do this, the administrator must enter the configuration mode of the telephones that have the DNs, proceed to the Directory Number Configuration page, and select the partition from the menu.

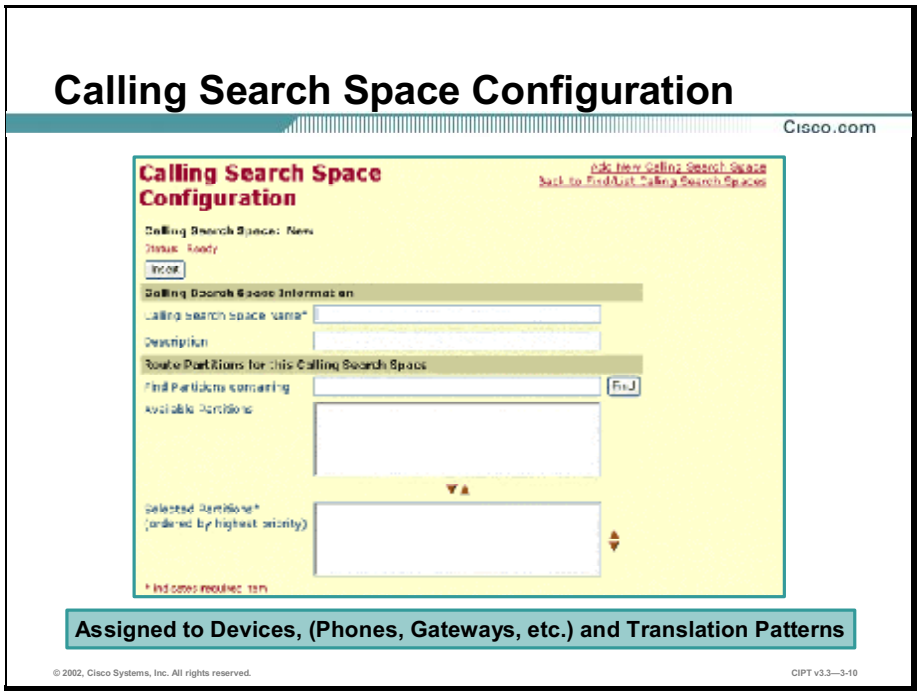
Calling Search Spaces

This topic discusses the function and configuration of calling search spaces.



A calling search space is an ordered list of partitions that the CCM digit analysis looks at before a telephone call is placed. Calling search spaces determine the partitions that calling devices (such as IP Phones, Cisco IP SoftPhones, and gateways) can reach when attempting to complete a call.

When you assign a calling search space to a device, the list of partitions in the calling search space defines the route patterns and DNs that the CCM allows the device to reach. If a device attempts to reach a route pattern or DN that is not in its calling search space, it recieves a fast busy signal.



After configuring the partitions and assigning DNs or route patterns to those partitions, you must configure calling search spaces that contain a prioritized list of the available partitions. The figure here shows the Calling Search Space Configuration page in Cisco CallManager Administration.

You can use the arrows between the Available Partitions and Selected Partitions dialog boxes to choose the partitions that you want to add to the calling search space. You can reorder partitions by using the arrows to the right of the Selected Partitions dialog boxes. To reduce call-processing time, place the partitions with the most frequently used numbers at the top of the Selected Partitions list.

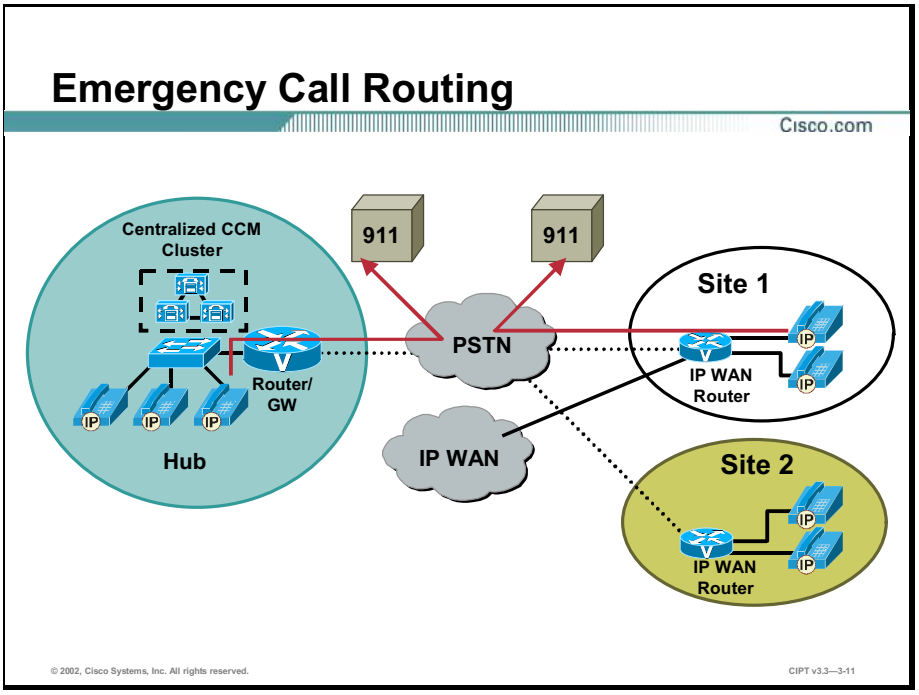
Example

In order to restrict access to the 1*xxx* and 2*xxx* partitions, the network administrator from the ABC Company must create a calling search space named "1*xxx*_Only" and add the DN_1*xxx* partition to this calling search space. The administrator then creates another calling search space named "2*xxx*_Only" and adds the DN_2*xxx* partition to this calling search space. Finally, the administrator creates a calling search space named "All_DNs" and adds both the DN_1*xxx* and DN_2*xxx* partitions to this calling search space.

After configuring the calling search spaces, the administrator assigns them to the various network devices. For example, Telephone A is assigned the "1*xxx*_Only" calling search space, which means that Telephone A can call only the DNs assigned to the partition DN_1*xxx*. By assigning Telephone B to the 2*xxx*_Only calling search space, the administrator restricts Telephone B from calling any numbers outside of the DN_2*xxx* partition. If the administrator assigns Telephone C to the All_DNs calling search space, Telephone C can call the DNs assigned to partitions DN_1*xxx* and DN_2*xxx*.

Using Partitions and Calling Search Spaces for Emergency Calls

This topic explains how you can use partitions and calling search spaces to force CCM to route users dialing the 911 (or 9.911) string through a gateway connecting to the PSTN in the local area. (Although the 911 implementation is specific to the North American market, you can use the same configuration for emergency call numbers anywhere in the world.)



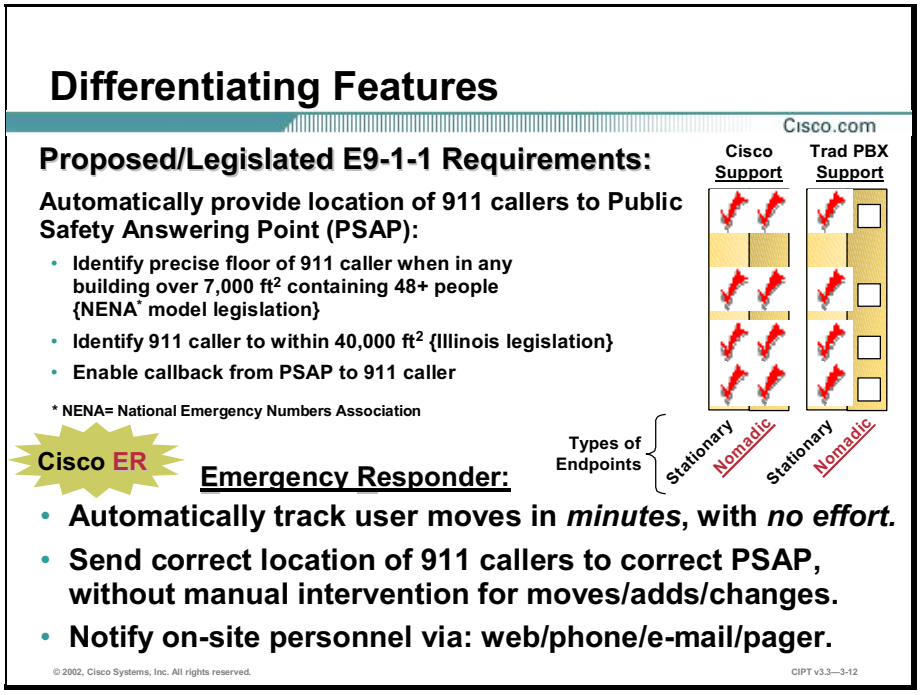
Correct configuration of emergency call routing is critically important in any voice network. One of the benefits of IP telephony is the ability to forward voice calls over the IP WAN. In the case of emergency calls, this can be detrimental.

The figure above shows three sites connected through the PSTN and the IP WAN. These sites could exist at disparate locations around the world. A serious problem can arise if a user located in Site 2 dials an emergency number (such as 911) and, through poor configuration, it is forwarded across the WAN and out the PSTN connection at Site 1.

You can prevent this situation from occurring through the proper implementation of partitions and calling search spaces. You must place the emergency numbers for each geographic location in their *own* partition. Then, you should give the devices at each location the ability to reach *only* the partition containing the emergency numbers for *their* location.

Cisco Emergency Responder

This topic discusses the Cisco Emergency Responder (ER) application used to provide E-911 service in a Cisco IP telephony solution.



Cisco ER is appropriate for:

- Single or multicluster CCM installations with 48+ IP Phones per site
- E911 extension support to include extension mobility and/or IP Phones that move between cubicles, offices, floors, buildings, or campuses
- Shared line appearances on telephones in multiple physical locations
- Cisco SoftPhone running on desktops and/or laptops directly attached to Cisco Catalyst switches
- Cisco IP Phones connected to Cisco Catalyst switches

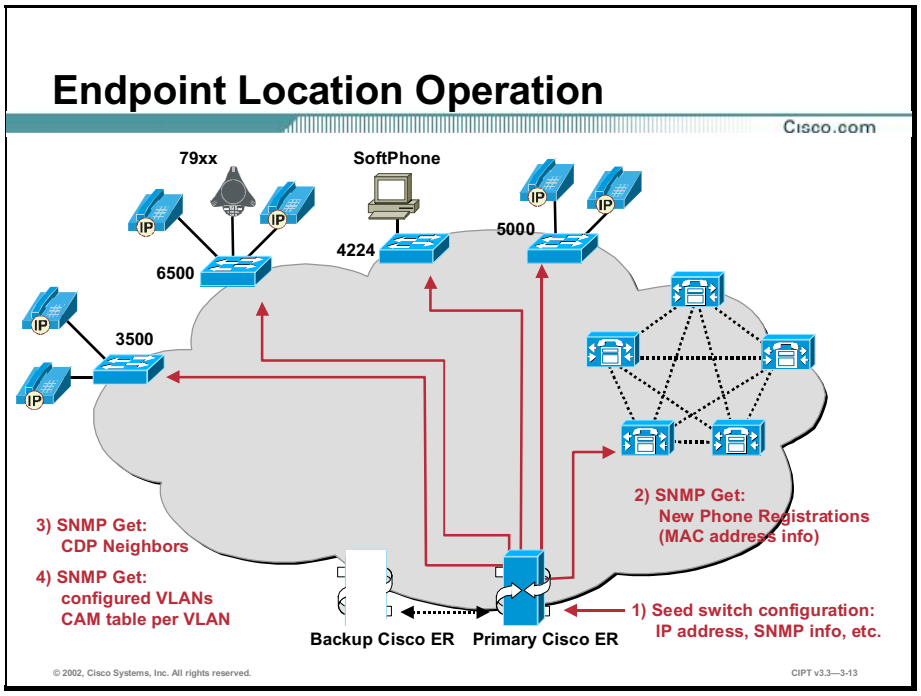
Cisco ER is not necessary for:

- Stationary IP Phones that do not use extension mobility or shared-line appearances
- Small offices with fewer than 48 telephones

Deployment scenarios

The following are deployment scenarios addressed by Cisco ER:

- Large networks
- Ability to run Cisco ER on redundant dedicated Cisco Media Convergence Server (MCS) platforms
- Ability to communicate with multiple CCM clusters with storage of the ER configuration information in the directory of a single CCM cluster
- Each campus with one or more CCM clusters should have a pair of ER servers
- Use centralized ER servers and distributed Centralized Automatic Message Accounting (CAMA)/PRI gateways for the centralized deployment model



The preferred method is using the telephone's MAC address discovery via Cisco Discovery Protocol (CDP). Discovery via content-addressable memory (CAM) table (mapping of MAC address to switch ports) is an alternative (but may be less efficient).

When using the switch CDP neighbors (preferred) to find the telephone devices, the following guidelines need to be followed:

- Requires a list of switch IP addresses (or Domain Name System [DNS] names) with Simple Network Management Protocol (SNMP) "read" strings in Cisco ER
- Requires CDP support in telephone device
- Minimal impact to switching infrastructure

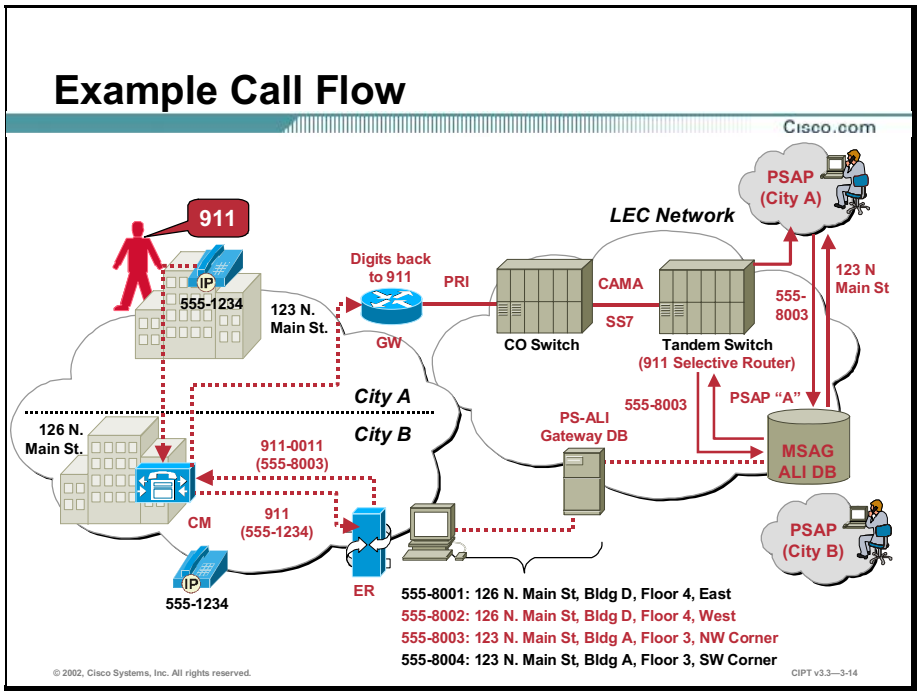
When using the switch CAM table (alternate) to find telephone devices, the following guidelines need to be followed:

- Requires a list of switch IP addresses, telnet and enable passwords, and SNMP read strings
- Used following failure to discover telephones as CDP neighbors
- Greater impact on switching infrastructure; per-switch option to disableThe following are the supported endpoints used with Cisco ER:
- CDP Neighbor search
  - Cisco 7905, 7910, 7912, 7940, 7960, 7935 (w/firmware upgrade)

- CAM Table search
  - Cisco IP SoftPhone v1.2 (supports CDP search in later release)
  - Older Cisco telephones: SP12+, VIP30
  - Skinny-enabled, non-CDP devices/clients
- Manual endpoint entry
  - FXS ports (callback support varies w/config)
  - Telephones behind PBXs awaiting migration
  - Static H.323 and SIP endpoints (e.g. desktop PC)
  - Local telecommuters (same area code)

These are the supported Catalyst Switches (non-cluster):

- Cat 6500, 5000, 4000 series
- Cat 3500XL, 4200 series (w/software upgrade)

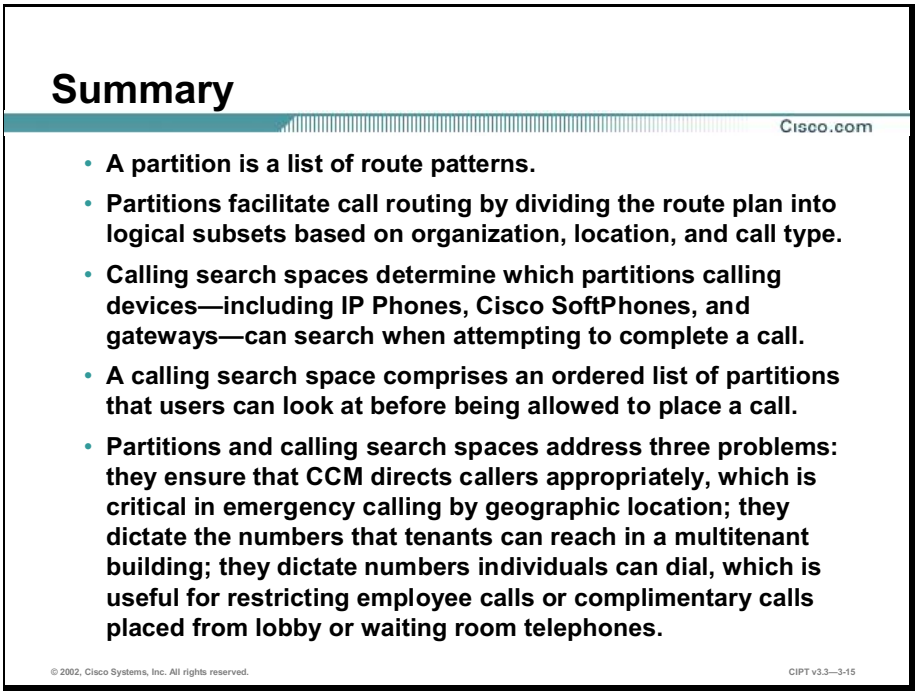


The first scenario in this figure occurs when the telephone (555-1234) dials 911. This is a simple resolution for Cisco ER.

A more complicated scenario occurs when the telephone extension with the same DN is in another city and Cisco ER must route the call with the correct information to the correct Public Safety Answering Point (PSAP).

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Call Admission Control and Survivable Remote Site Telephony lesson

References

For additional information, refer to these resources:

- Newton, H. *Newton's Telecom Dictionary, 18th Updated and Expanded Edition.* New York, New York: CMP Books; 2002.
- Smith, A., Chris Peace, D. Whetton, and J. Alexander. *Cisco CallManager Fundamentals: A Cisco AVVID Solution.* San Jose, California: Cisco Press; 2001.
- Cisco ER:
  http://www.cisco.com/univercd/cc/td/doc/pcat/erv.htm
  http://www.cisco.com/warp/public/cc/serv/mkt/sup/svsptl/iptlsv/e911q_qp.htm

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which three of these problems are addressed with calling search spaces and partitions? (Choose three)

A) routing by geographical location

B) routing by tenant

C) routing by class of user

D) routing by devices

Q2) Which of these statements best describes a partition?

A) a logical grouping of route patterns

B) a logical grouping of telephone devices

C) a logical grouping of gateway devices

D) a logical grouping of route lists

Q3) Which of these statements best describes a calling search space?

A) ordered list of partitions

B) ordered list of route patterns

C) route patterns with similar calling capabilities

D) route Groups with similar calling capabilities

Q4) Which of these should occur during an emergency call?

A) The call should be routed across the WAN to the local PSTN.

B) The call should be routed to the local PSTN.

C) The call should not be routed.

D) The call should be routed using route lists.

Q5) Which of these is not a deployment scenario recommended to use with Cisco ER?

A) single or multi-cluster call-manager installations with 48+ IP Phones per site

B) extends E9-1-1 support to include extension mobility and/or IP Phones that move between cubicles, offices, floors, buildings, or campuses

C) shared line appearances on telephones in multiple physical locations

D) small offices with fewer than 48 telephones

Call Admission Control and Survivable Remote Site Telephony

Overview

This lesson describes Call Admission Control (CAC) and survivable remote site telephony (SRST). CAC controls the number of calls between two endpoints, which is important to maintain quality of service (QoS) for both new and existing calls. The SRST feature provides call-handling support if Cisco CallManager (CCM) or WAN link fail.

Importance

When an IP WAN connects two clusters, CAC is vital to protect calls from other voice calls that can oversubscribe the IP WAN bandwidth and affect voice quality. The gatekeeper device, which you can configure two ways, is a CAC device that controls how voice calls use the IP WAN bandwidth.

Objectives

Upon completing this lesson, you will be able to:

- Describe the importance of CAC for maintaining QoS
- Identify the gatekeeper procedures with H.323 endpoints
- Configure a gatekeeper device as an anonymous device that performs CAC and E.164 address resolution
- Describe the importance of CAC in a centralized call-processing deployment Configure SRST on a supported gateway

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Gateway configuration in Cisco CallManager Administration
- Cisco IOS Configuration

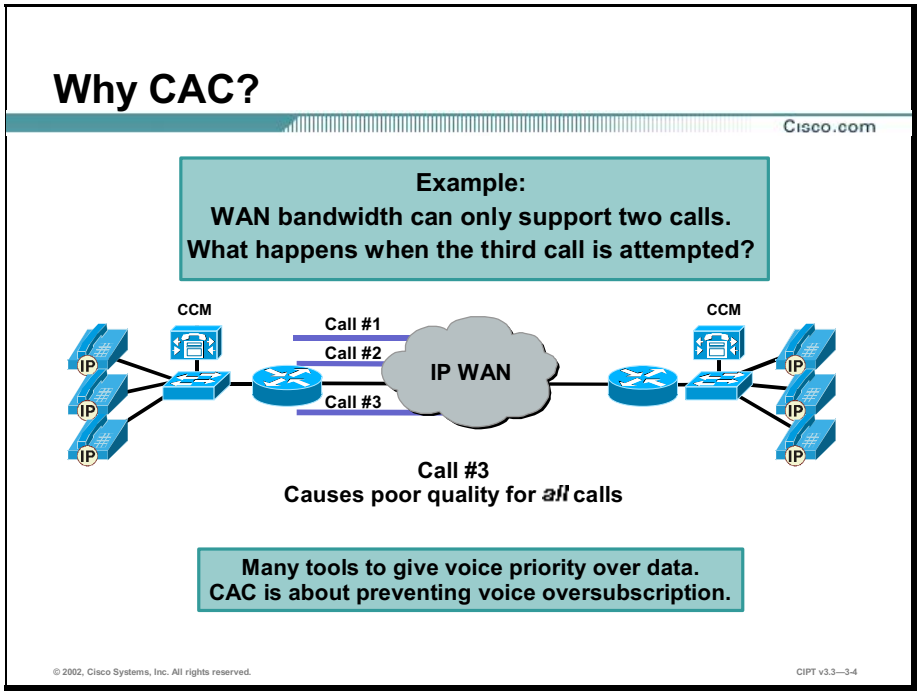
Outline

This lesson includes these topics:

- Overview
- CAC
- Procedures
- CCM Gatekeeper Configuration
- Centralized Deployment CAC
- SRST
- Summary
- Lesson Review

CAC

This topic discusses the importance of Call Admission Control (CAC).

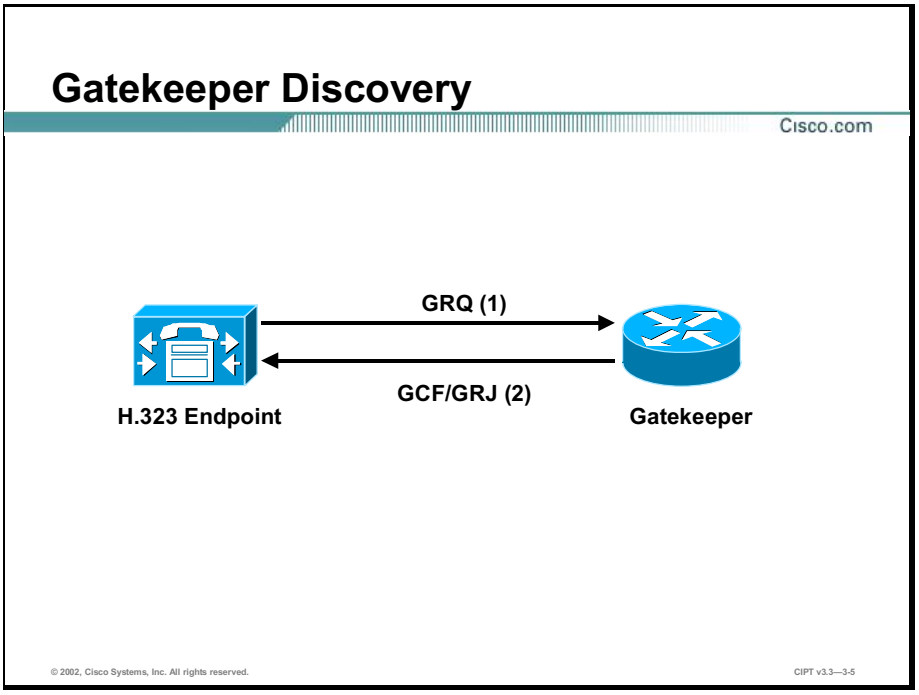


CAC provides you with mechanisms to control the quantity of calls between two endpoints. Controlling the number of calls, or the amount of bandwidth that is required between two endpoints, is key to maintaining quality of service (QoS) for all existing and new calls. You can provision the network to carry a specific amount of real-time traffic. Any traffic that exceeds the provisioned bandwidth will be subject to delay, jitter, and possibly packet loss.

The coder-decoder (codec) used for the call determines the bandwidth calculations used with CAC.

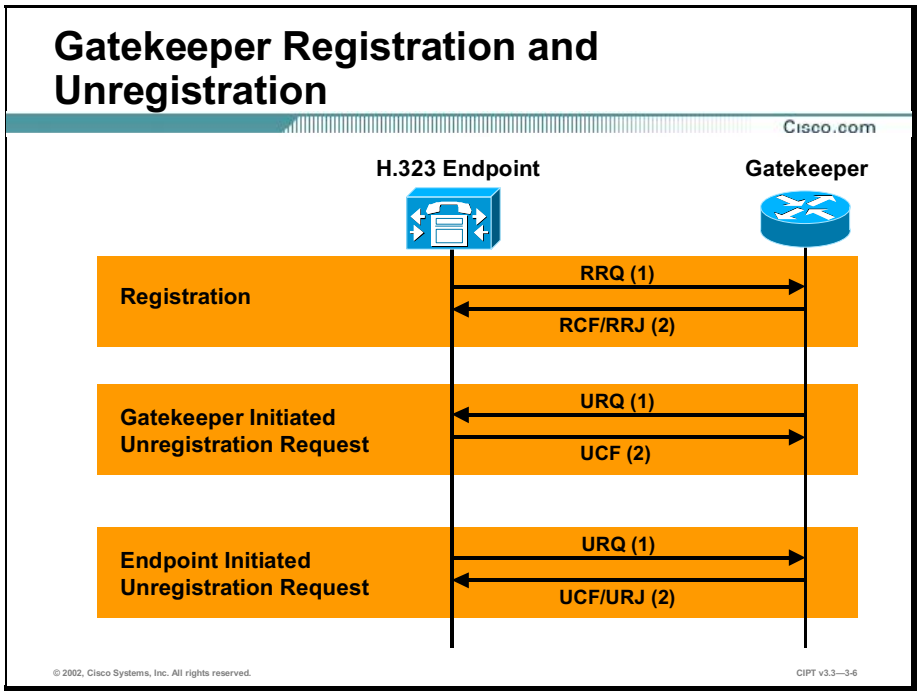
Procedures

This topic describes the language of the gatekeeper. The gatekeeper requires a variety of messages before and during calls.



The first process an endpoint must go through is gatekeeper discovery. An endpoint achieves gatekeeper discovery either manually or through autodiscovery.

Autodiscovery uses multicast to discover the gatekeeper. A Gatekeeper Request (GRQ) is multicast and any gatekeepers that can accept a registration will return a Gatekeeper Confirmation (GCF). If a gatekeeper cannot accept a registration, it will return a Gatekeeper Reject (GRJ).



A Cisco IOS gatekeeper supports two types of registration:

- Full Registration
- Lightweight Registration

An endpoint must always use a full registration during the initial registration process. An endpoint may use lightweight registration to maintain registration. Should an endpoint become unregistered with the gatekeeper, a full registration is required.

Full registration requires the endpoint to register any E.164 address, H.323 ID, device type, and other possible parameters each time it registers. This procedure involves additional processing load on a gatekeeper every time an endpoint registers or renews its registration. The Registration Request (RRQ) includes the time between renewal of registrations or Time to Live (TTL), and the gatekeeper may replace or return this value unchanged.

Note You can make the returned TTL value configurable with Cisco IOS 12.1.5T and later.

The lower the TTL value, the higher the load on the gatekeeper processing the registration. The impact of a higher value results in the gatekeeper being unaware of an endpoint that has lost connectivity. Use 30 to 300 seconds, depending on design requirements.

When the endpoint sends a full RRQ to the gatekeeper, the gatekeeper responds with a Registration Confirmation (RCF) to accept, or a Registration Reject (RRJ) to refuse. The gatekeeper may refuse the registration for many reasons, such as duplicate E.164 or H323 IDs or ambiguous information.

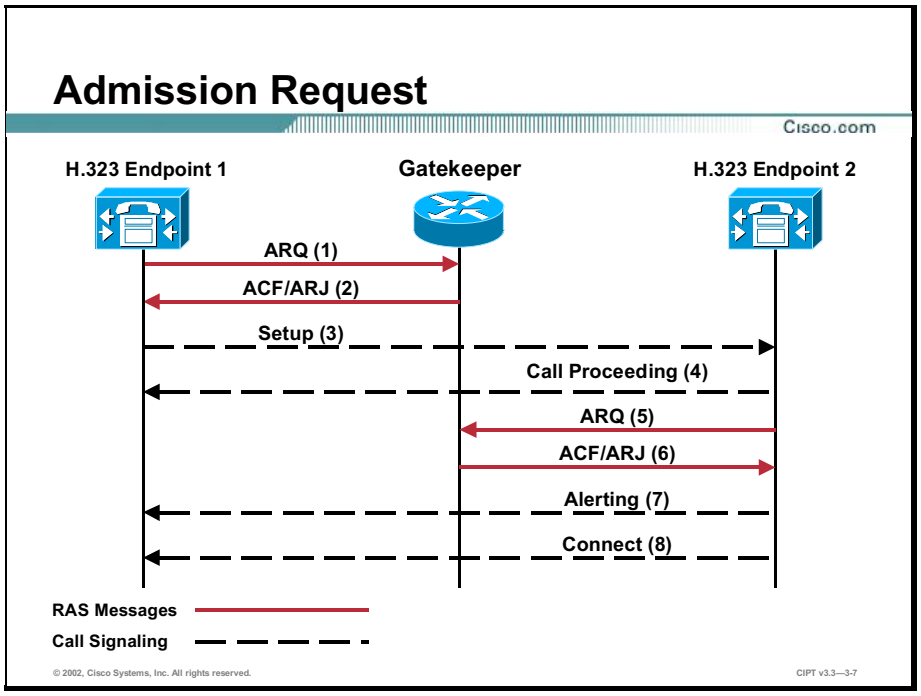
An endpoint registration has a finite life. Before the TTL expires, the endpoint is required to renew its registration by sending an RRQ. If the TTL expires and the gatekeeper has not received an RRQ from the endpoint, the endpoint will become unregistered.

Lightweight registration reduces the processing load on the gatekeeper during registration renewal. The gatekeeper receives an RRQ with the keepalive bit set and the minimum required information from the endpoint. If the gatekeeper accepts the renewal, the gatekeeper will return an RCF to the endpoint and reset the TTL timer. If the gatekeeper rejects the renewal with an RRJ, the endpoint becomes unregistered.

If the endpoint is unregistered, the endpoint must start the gatekeeper discovery and registration process again.

At any time, an endpoint or a gatekeeper may cancel a registration with an Unregister Request (URQ), normally used during configuration changes.

An endpoint or gatekeeper sends an Unregister Confirmation (UCF) in response to a URQ. If an unregistered endpoint sends a URQ to a gatekeeper, the gatekeeper will respond with an Unregister Reject (URJ) to indicate the error. Cisco IOS gatekeepers, Cisco IOS Gateways, and Cisco CallManager (CCM) support lightweight registration.



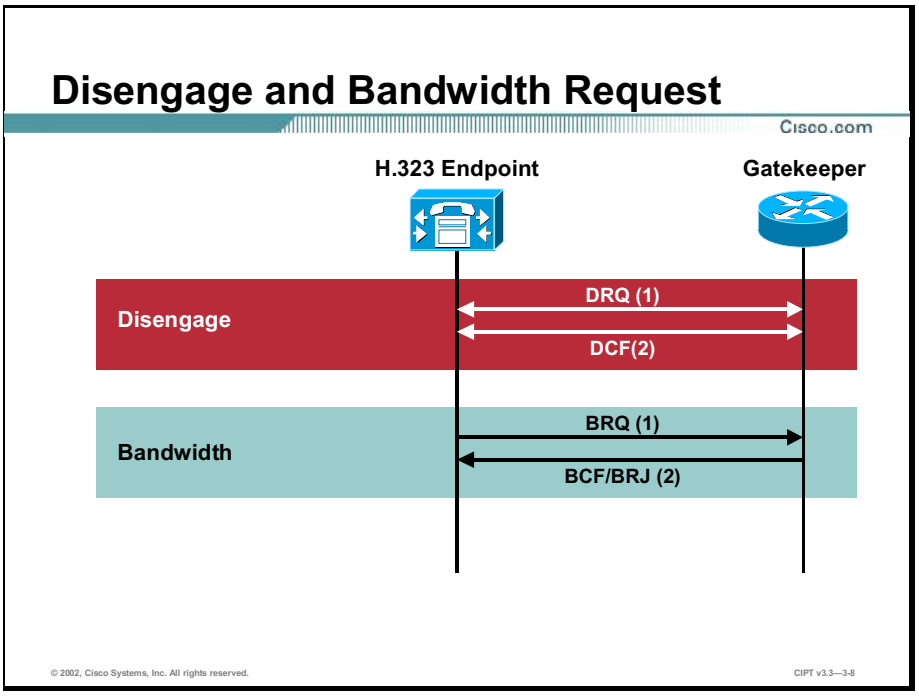
Telephony endpoints (IP Phones or Cisco IP SoftPhones) send an Admission Request (ARQ) to the gatekeeper to initiate a call. The ARQ contains an H.323 ID or the E.164 address of a destination or called party it wishes to reach. Also contained within the ARQ message are the call bandwidth (not including the header overhead), the source E.164 address, and/or H.323 ID of the calling party.

Note The call bandwidth requested will be the upper limit of both the transmitted and received bit rate for all video and audio channels.

Note There will always be an E.164 address with CCM.

The gatekeeper will respond to the ARQ with either an Admission Confirmation (ACF) or an Admission Reject (ARJ). The gatekeeper sends the ACF if the requested bandwidth is available and the called endpoint is found. The ACF contains the IP address of the endpoint. On receipt of an ACF from the gatekeeper, the endpoint sends a setup message directly to the other endpoint, using the IP address returned in the ACF.

If either bandwidth is unavailable or the called endpoint is not registered, the gatekeeper sends an ARJ.



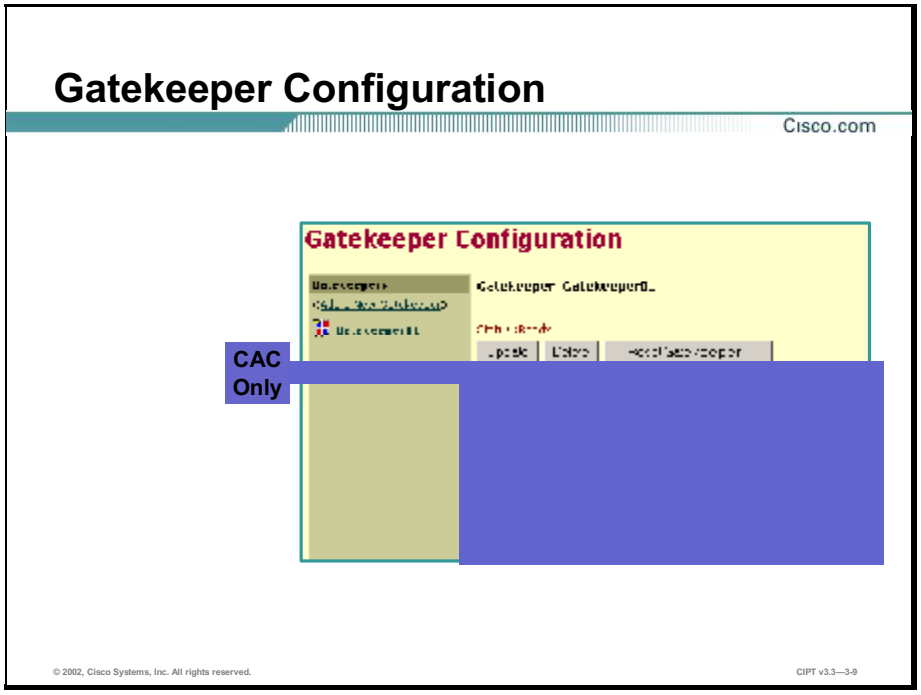
When an endpoint terminates a call, the endpoint is required to indicate the termination to the gatekeeper and return the used bandwidth. The endpoint sends a Disengage Request (DRQ) to the gatekeeper to indicate that the call is complete. The gatekeeper responds with a Disengage Confirmation (DCF) and returns the previously used bandwidth to the pool.

The gatekeeper can also clear the call by sending a DRQ to the endpoint, forcing the endpoint to clear the call with the other endpoint and return a DCF.

If during the duration of the call the bandwidth requirement changes, due to a changing codec or additional media channels opening or closing, the endpoint may request or release the bandwidth by sending a Bandwidth Request (BRQ). The gatekeeper will respond with a Bandwidth Confirmation (BCF) if the bandwidth is available or refuse the request with a Bandwidth Reject (BRJ) if the bandwidth is not available.

CCM Gatekeeper Configuration

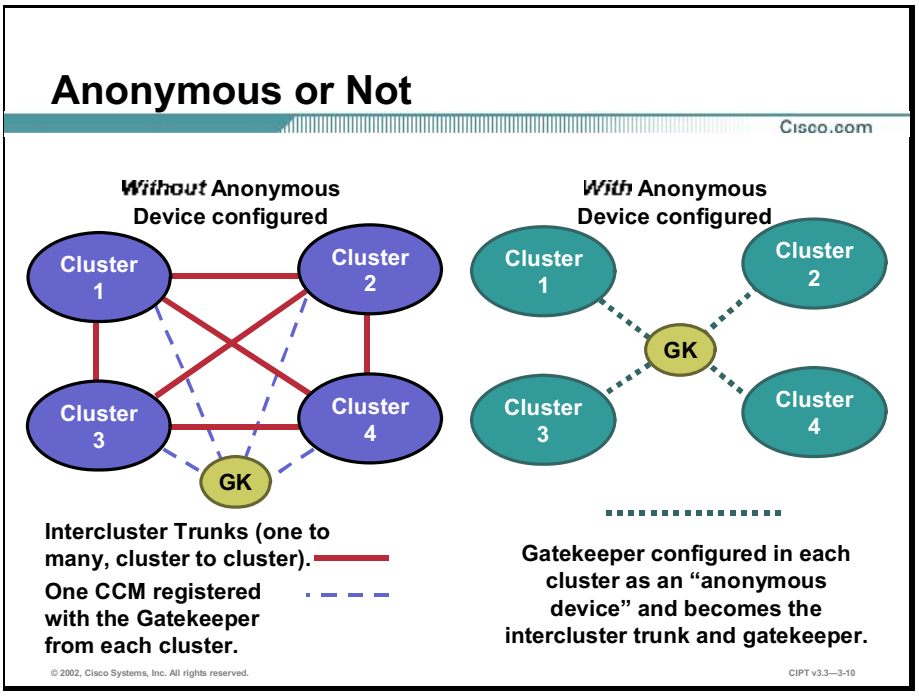
This topic describes the configuration details needed when adding a gatekeeper in a Cisco IP telephony solution.



CCM uses gatekeepers for a variety of purposes. CAC is a basic feature of gatekeepers for calls from one CCM to another CCM or H.323 gateway. CCM also uses the gatekeeper for E.164 address resolution on intercluster calls between CCMs. Using gatekeepers for E.164 address resolution centralizes dial plan administration.

CCM supports two user-definable versions of the H.323 gateway. The first is the H.225 version, which allows connectivity to H.323 Cisco IOS gateways. The second version is the intercluster trunk. The intercluster trunk provides specific, Cisco functionality for calls between CCM clusters.

A third system gateway, called the “anonymous device,” provides gatekeeper E.164 address resolution.



Intercluster trunk gateways require additional consideration. The Device Name entered for the gateway destination is a CCM server in another cluster.

If you have more than one CCM server in the cluster, but only one defined gateway, a failure of that single server in the remote cluster stops all intercluster calls. Therefore, you must connect each server-processing call by an intercluster trunk gateway to all remote call-processing servers.

The remote cluster also requires a corresponding number of intercluster gateways defined back to the local call-processing servers. This symmetrical configuration eliminates one-way calling paths and introduces fault tolerance in the design. This configuration also greatly increases complexity.

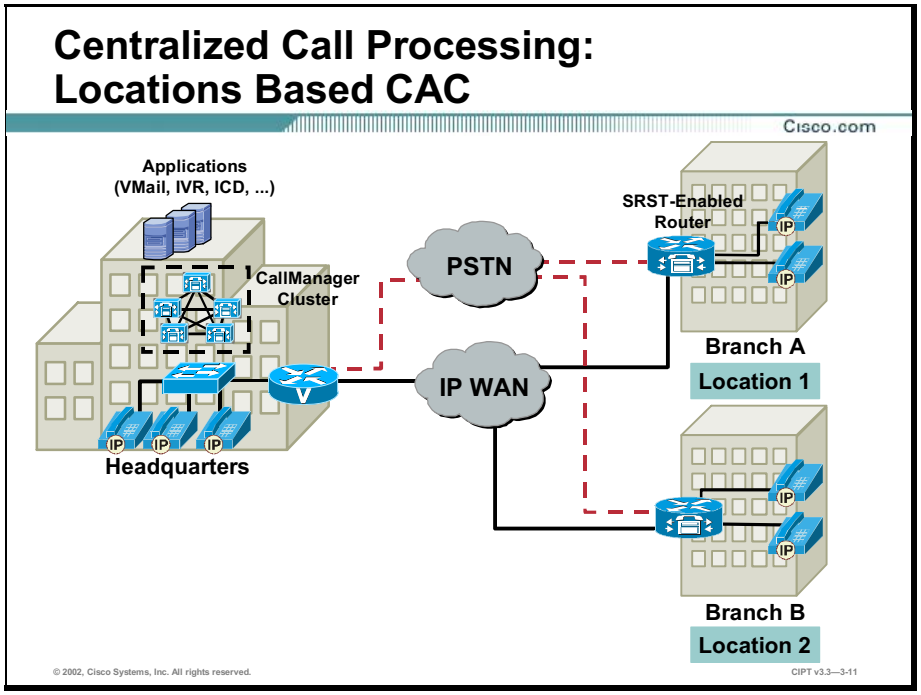
There is an alternative to the multiple, point-to-point intercluster trunk gateways. The Gatekeeper Configuration page provides an Allow Anonymous Calls check box.

This option enables a special gateway that is a point-to-multipoint intercluster trunk. It creates an anonymous device, which is a special intercluster trunk gateway. AnonymousDevice appears in the gateways list in the Route Pattern and Route Group configuration pages.

The advantage of AnonymousDevice is that each CCM cluster only needs a single intercluster trunk gateway for connectivity to all other CCM clusters.

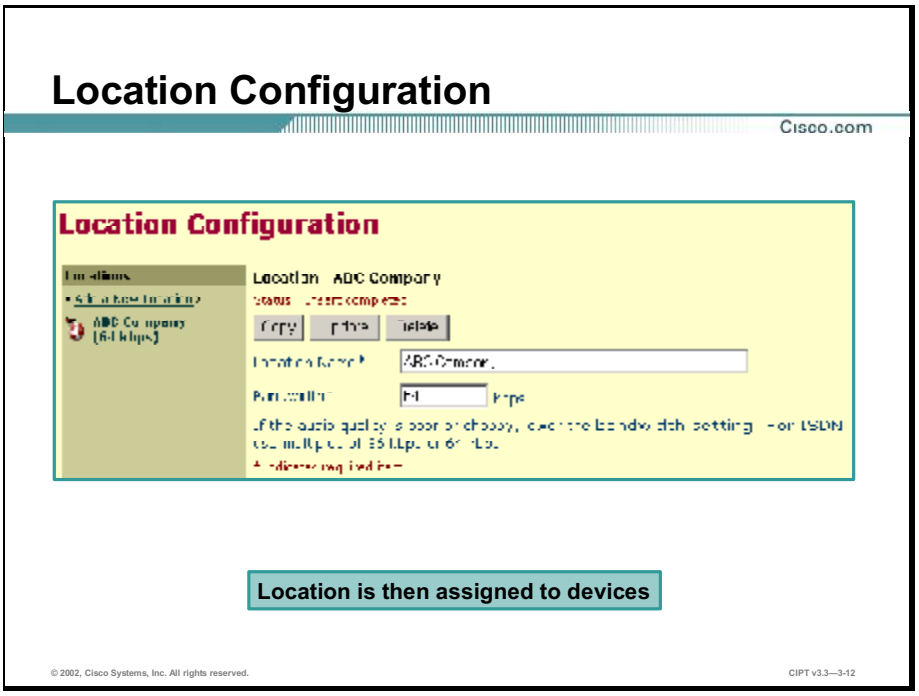
Centralized Deployment CAC

This topic describes CAC in a centralized call-processing deployment.



CCM provides a simple locations-based CAC mechanism for hub and spoke topologies, used primarily for centralized call processing. During the configuration of a device on CCM, you can place the device in any location. The CCM has no knowledge of where the device is physically located.

If the device moves from one physical location to another, without changing the location configuration, CCM will incorrectly calculate bandwidth for that device, which renders the locations-based CAC unusable.



To place a device in a location, first define the available locations and bandwidth from the Cisco CallManager Administration pages. Access the Cisco CallManager Administration pages by choosing **System>Location**.

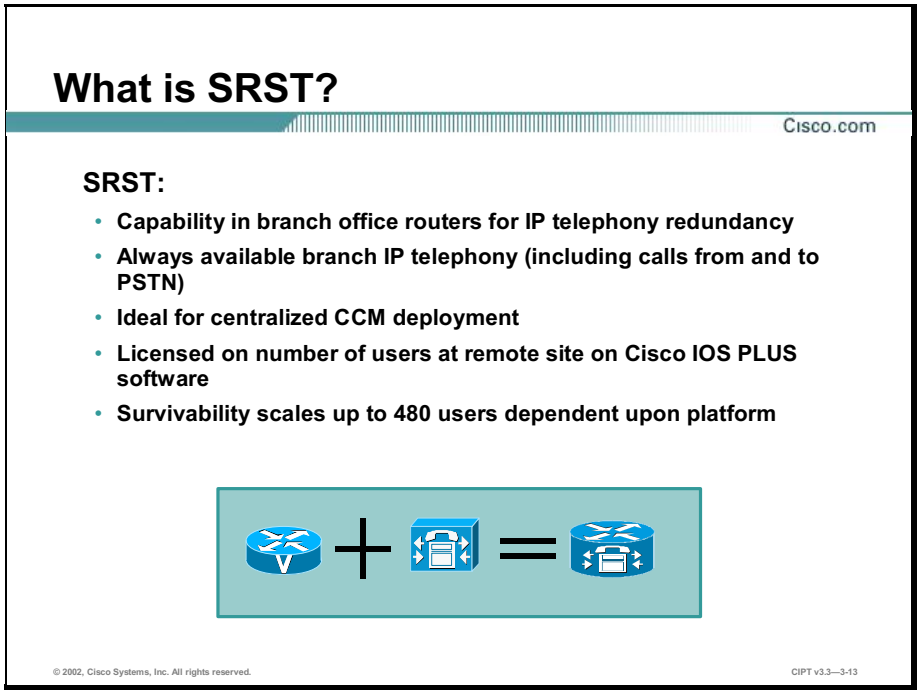
After defining the locations with the available bandwidth, you can configure the devices in that location. The example shows a defined location Branch A, which has 256 kbps of available bandwidth that will support up to three G.711 calls, ten G.729 calls, or a mixture of both.

The device configuration pages allow you to specify the location of the device from a menu. Devices that allow location definition include telephones, gateways, and computer telephony integration (CTI) route points. Telephone devices include IP Phones, CTI Ports, and H.323 clients.

The figure shows a gateway defined as ABC Company and configured to be in the Branch A location. Each call placed to or from this device is admitted by CCM, based on the available bandwidth in the Branch A bandwidth pool. When attempting a call with insufficient bandwidth available, the call will fail due to insufficient bandwidth resources, and the endpoint will receive a busy tone. Additionally, IP Phones with a display will receive a Not Enough BW message.

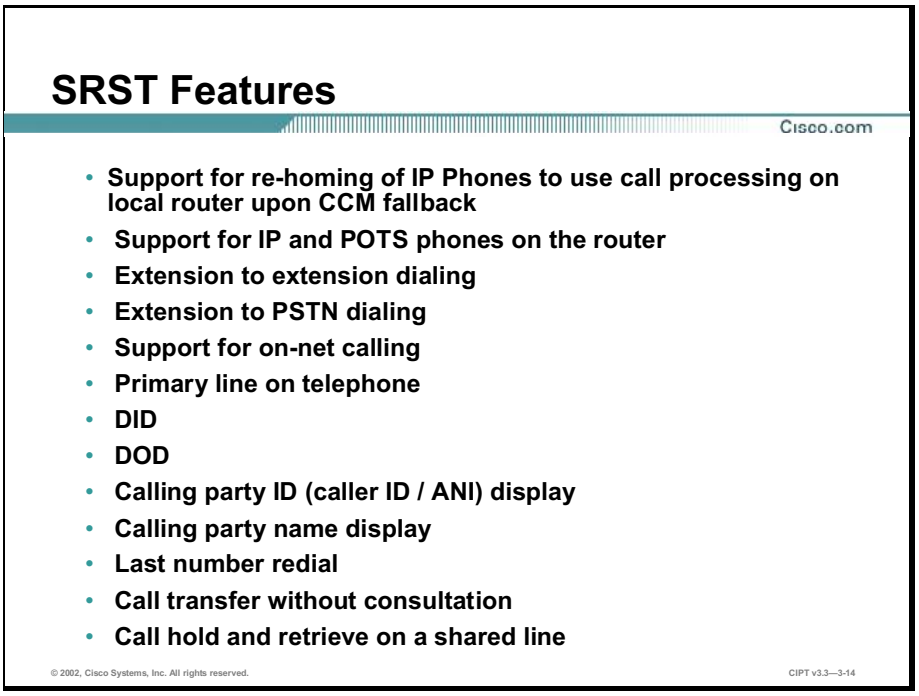
SRST

This topic discusses the survivable remote site telephony (SRST) feature used in a centralized call-processing deployment.



The SRST feature provides call-handling support on the gateway router for attached IP Phones when a CCM or WAN link fails. On restoration of the CCM or WAN link, the CCM resumes the call-handling capabilities for the IP Phones. The implementation of this feature is transparent to the end user. The SRST-enabled router supports:

- IP Phone to IP Phone on router calls
- IP Phone to Public Switched Telephone Network (PSTN) calls
- Multiple lines per IP Phone
- Multiple line appearance across IP Phones
- Call hold and pickup on a shared line
- Call transfer of local calls
- Caller ID information
- Up to 24 telephones on 2600 and 3620 platforms
- Up to 48 telephones on 3640 and 3660 platforms



With the current Cisco Architecture for Voice, Video and Integrated Data (AVVID), CCMs provide call-processing functions for IP Phones. Placing CCMs in central locations allows this architecture to be cost effective. In addition, the central locations can often provide call-processing functions for IP Phones located in remote locations.

There is weakness in this architecture when a WAN connection fails and remote IP Phones cannot make calls. This weakness can be a serious problem when it comes to emergency calls such as E911.

A simple way of solving this problem is to provide limited call-processing capabilities in the remote office router. IP Phone enhancements grant the ability to rehome to the call-processing functions in the local router when on WAN failure detection. This solution is the CCM Fallback feature.

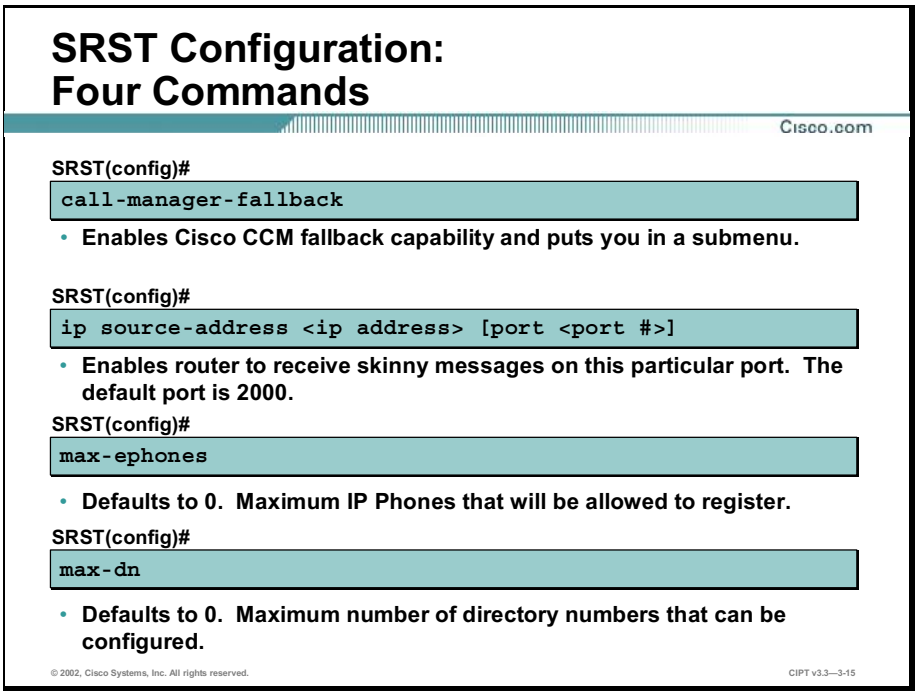
The CCM Fallback feature is referred to as SRST. SRST telephone features include:

- Support for IP Phones and plain old telephone service (POTS) telephones on the router
- Extension to extension dialing
- Extension to PSTN dialing
- Primary line on IP Phone
- Direct Inward Dial (DID)
- Direct Outward Dial (DOD)

- Calling party ID (Caller ID/ANI) display
- Calling party name display
- Speed Dialing
- Last number redial
- Call transfer without consultation (local to router only)
- Call hold/resume
- Multiple extensions (up to six extensions per IP Phone on 7960 IP Phones)
- Multiple line appearances with up to 24 appearances per system
- Distinctive ringing
- Extension class of service (CoS)
- Full interworking with Cisco gatekeeper functionality
- Voice-mail support (only to local answering machine)
- Billing support using Call Detail Records (CDRs)

Router WAN interface support includes:

- WAN link types: Frame Relay, ATM, multilink point-to-point protocol (MLPPP), serial, ATM adaptation layer 2 (AAL2), digital subscriber line (DSL)
- Voice over Frame Relay (VoFR), Voice over ATM (VoATM), ATM adaptation layer 5 (AAL5), Voice over IP (VoIP)
- Codec types G.711, G.728, G.726, G.729, G.729a, G.723
- Support of T1 & E1 channel-associated signaling (CAS) trunks to PSTN
- Support of ISDN BRI
- CDR and billing support



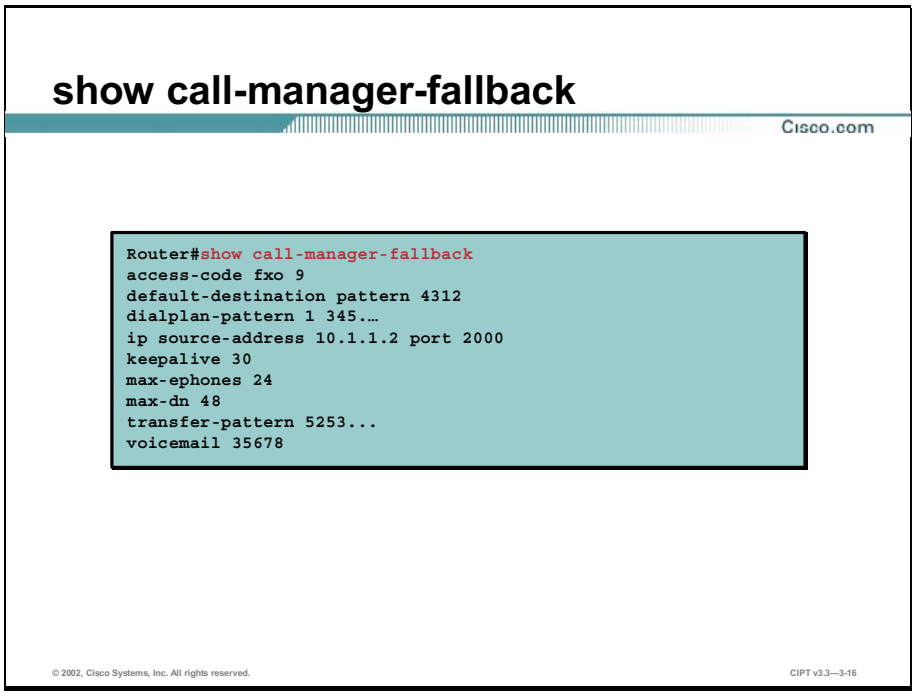
The most common application of SRST is to maintain basic IP telephony functionality for the IP Phones at the remote branch offices, in the event the WAN link fails or the CCM at headquarters is no longer available.

The remote branch router will activate SRST functions and take over communication with the IP Phones. IP Phones are able to call each other and make off-net calls to the PSTN. In addition, the most basic telephone functions, such as hold and transfer, are still available.

There is one global command to configure for SRST: **`call-manager-fallback`**, which is a global command with a series of subcommands.

call-manager-fallback Subcommands

Command	Description
`access-code`	Define access-codes for outgoing calls
`default`	Set a command to its defaults
`default-destination`	Define/disable default destination dn for ringing on unknown called number
`dialplan-pattern`	Define E.164 telephone number prefix
`huntstop`	Stop hunting on Dial-Peers
`ip`	Define IP address and port for the IP Keyswitch
`keepalive`	Define keepalive timeout period to unregister IP Phones
`max-dn`	Specify maximum directory numbers supported on IP Keyswitch
`max-ephones`	Specify max number of IP Phones
`reset`	Reset IP Phones
`transfer-pattern`	Define valid call transfer destinations
`Voicemail`	Set voice-mail access number called when messages button is pressed



Below are examples of how to use some of the subcommands.

access-code fxo 9

This command associates the outgoing digit 9 with all Foreign Exchange Office (FXO) ports on the router. When the user dials the digit 9, one of the available FXO ports to PSTN is seized. The user can then dial the regular E.164 number to access a number in the PSTN. The advantage of this command is to select the type of ports rather than a single port. A request to a busy port will roll over to the next available port of the same type.

default-destination 2001

This command defines a default extension for all incoming calls that do not have an appropriate called number assigned. In this example, when an incoming call from an FXO port is not able to match to an appropriate called number, the call will route to extension 2001.

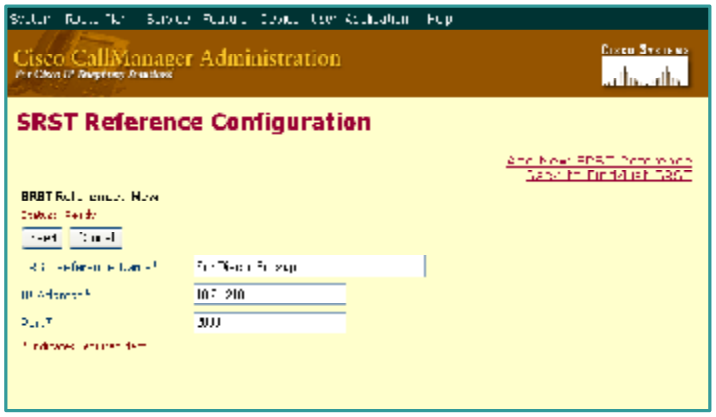
transfer-pattern 525.…

This command allows the transfer of calls to non-IP Phone numbers. By default, all IP Phones can be a transfer target. In this example, calls can transfer to all non-IP Phone numbers with prefix 525. Transfer of calls to an undefined number or prefix is blocked. You can enter a maximum of 32 transfer patterns.

voicemail 4001

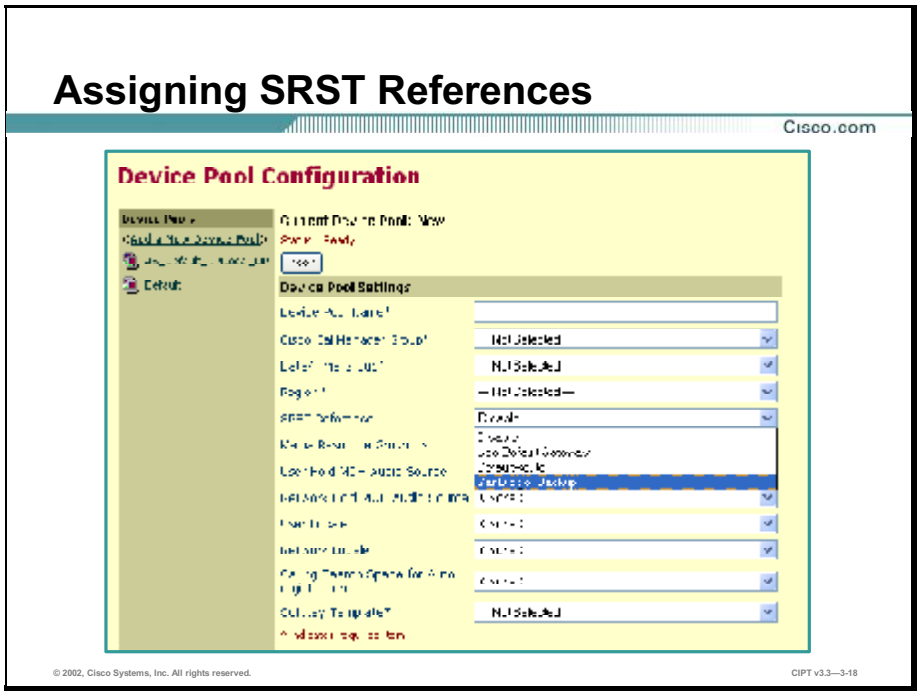
This command defines a dial-peer of a Foreign Exchange Station (FXS) port to route the call when the Message button on the IP Phone is pressed. In Phase 1, this process uses an answering machine on an FXS port. In this example, when the user presses the Message button on the IP Phone, the call proceeds to extension 4001, which is an answering machine. The user can then listen to the messages.

Creating an SRST Reference in Cisco CallManager Administration

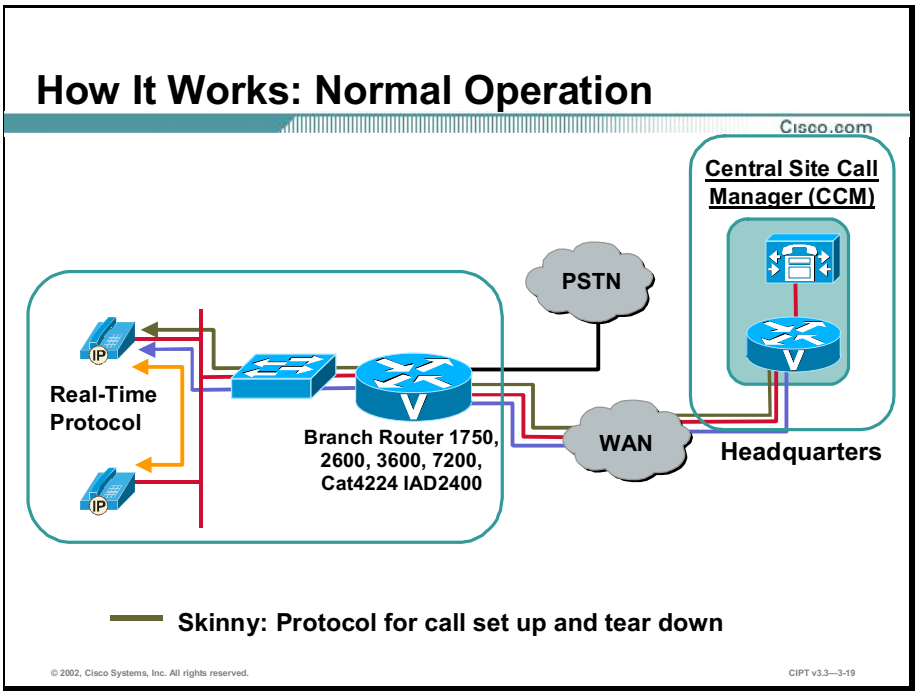


After you input the necessary Cisco IOS SRST gateway configuration, you must then configure the CCM to recognize the gateway as an SRST Reference. To configure SRST References, select the **System** menu in the Cisco CallManager Administration utility and select **SRST**. When the Find and List SRST References window appears, click the **Add a New SRST Reference** link in the upper-right area of the window. A window similar to the one shown in the figure should appear. In order to create a valid SRST Reference, you must enter the following fields:

- **SRST Reference Name:** This is a logical name you can use when referencing the SRST gateway. It does not need to match the name assigned to the gateway.
- **IP Address:** This is the IP address that the Cisco IP Phone should use when contacting the SRST gateway. The IP Phone itself must be able to reach this IP address.
- **Port:** This is the port number that the phone should use when contacting the SRST Reference. By default, this uses TCP port 2000.

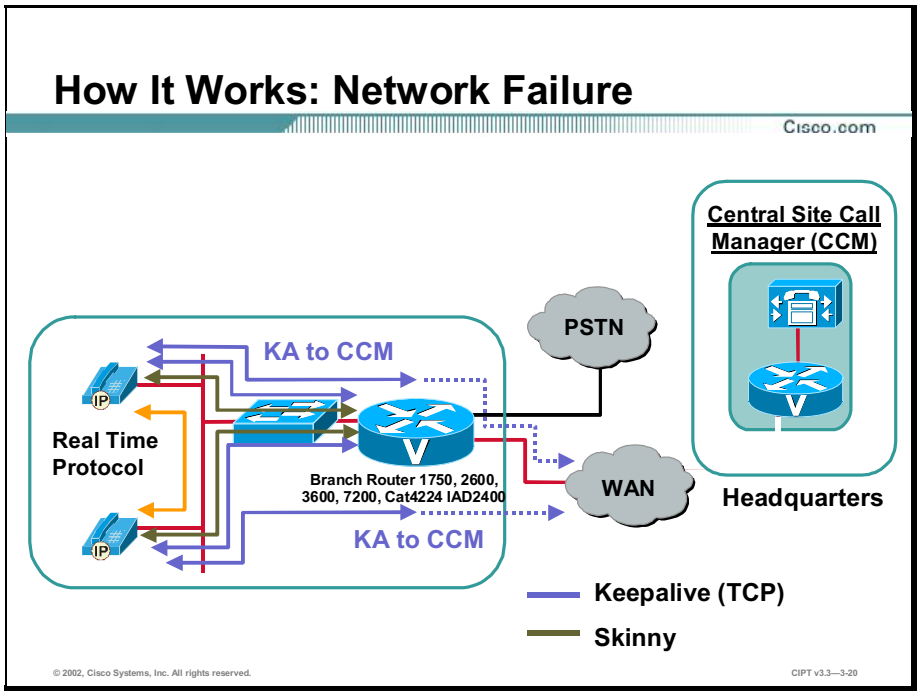


After you create the SRST Reference in CCM, you must assign the SRST Reference to the Cisco IP Phone. CCM creates this assignment through the Device Pool. In the Device Pool configuration, use the **SRST Reference** menu to select the SRST Reference that the IP Phone should use. If you would like the Cisco IP Phone to use its default gateway as the SRST Reference, you can choose the **Use Default Gateway** option from the menu. Using this option can simplify your SRST configuration.

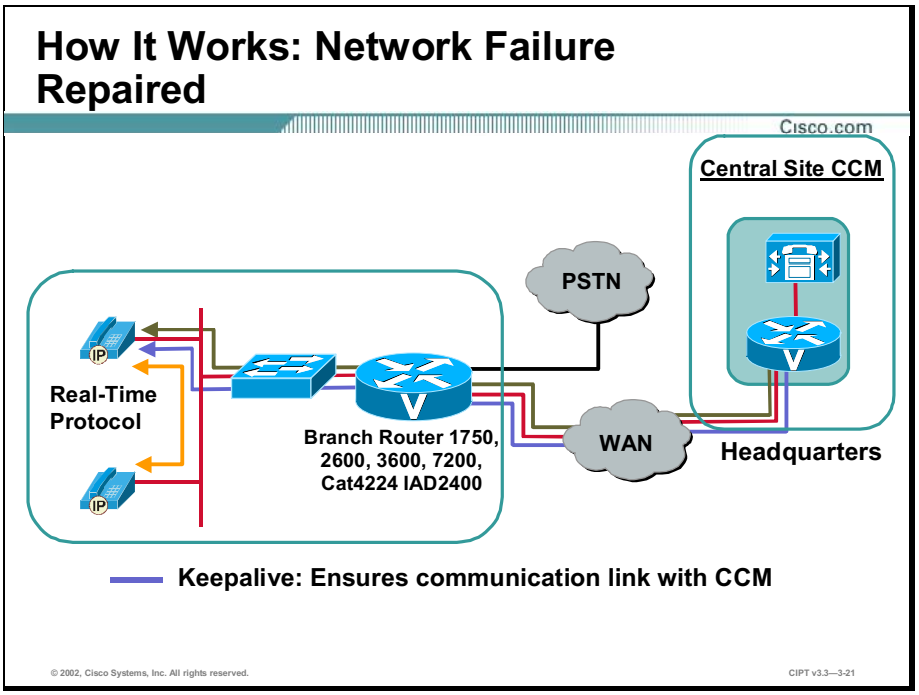


Shown here is an example of how the SRST feature works.

The SRST software operates by taking advantage of the keepalive packets emanating from both the centralized CCM cluster and local IP Phones. During normal operations, the CCM receives keepalive packets from the IP Phones. CCM performs call setup and processing, call maintenance, and call termination.



When the WAN link fails, Cisco IP Phones detect that they are no longer receiving keepalive packets from the CCM. Cisco IP Phones then register with the router. In this instance, the SRST software automatically activates and builds a local database of all Cisco IP Phones attached to it, up to the stated maximum. You can configure the IP Phones to query the router as a backup call-processing source when the central CCM does not acknowledge keepalive packets. The SRST router now performs call setup and processing, call maintenance, and call termination.

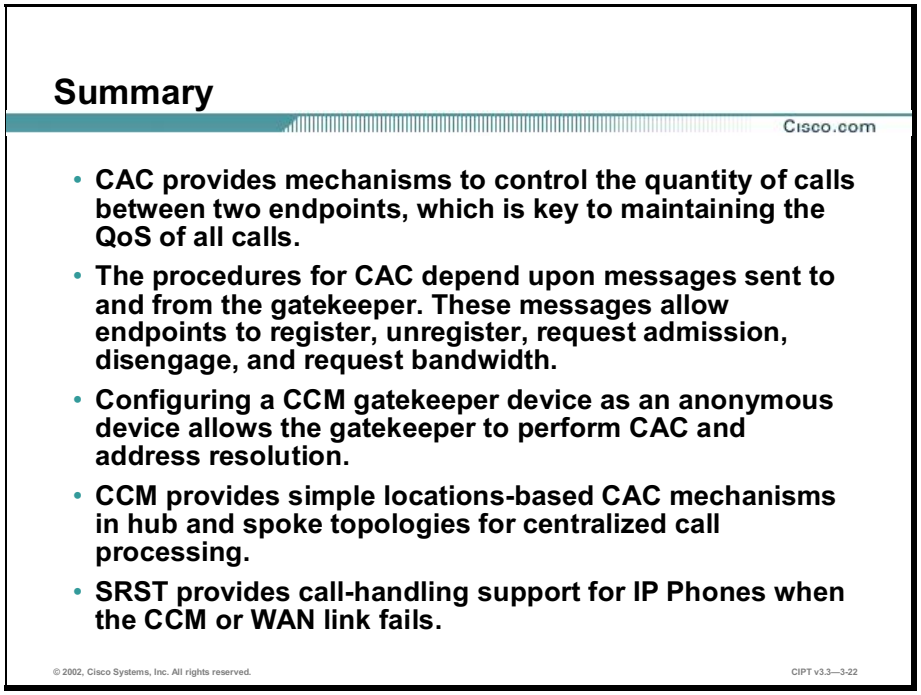


When the WAN link resumes, the IP Phones detect keepalive packets from the central CCM and revert to the central CCM for primary call setup and processing. As IP Phones rehome to the CCM, the SRST router purges its call-processing database and reverts to standby mode.

SRST only affects services and call establishment. Typical voice functions continue to be under the standard router gateway function. Calls in progress continue without interruption. IP Phones in use during WAN link recovery rehome to the CCM after the calls terminate.

Summary

This topic summarizes the key points you learned in this lesson.



Next Steps

After completing this lesson, go to:

- Features Plus module

References

For additional information, refer to this resource:

- http://www.cisco.com

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Without CAC, what happens to existing calls when the next call oversubscribes the WAN?

A) all calls are dropped

B) voice quality on all calls degrades

C) voice calls on the last call degrades

D) nothing

Q2) If a gatekeeper is configured as an anonymous device, what other function does the gatekeeper provide besides CAC?

A) intercluster trunk

B) digit analysis extension

C) voice quality debugger

D) firewall

Q3) How do the IP Phones in a branch site know to register to the gateway running SRST?

A) The telephone is part of the CCM list.

B) The IP address is configured on the gateway.

C) It is the default gateway IP address as part of the DHCP scope.

D) None of the above.

Q4) Which two of these options describe how endpoints achieve gatekeeper discovery? (Choose two.)

A) Autodiscovery

B) Manual discovery

C) assigned by the voice router

D) assigned by the CAC server

Q5) Which of these options would you configure for available bandwidth within the Cisco CallManager Administration window for CAC?

A) location

B) region

C) device pool

D) device defaults

4

Features Plus

Overview

This module describes the media resources for a Cisco IP telephony solution and provides an overview of Cisco CallManager (CCM) features and user options. This module also describes Call Admission Control (CAC) and survivable remote site telephony (SRST).

Upon completing this module, you will be able to:

- Define media resources
- Configure the softkey template
- Investigate and configure many of the features available on CCM
- Add and configure IP telephony users

Outline

The module contains these lessons:

- Media Resources
- Softkey Template
- Features
- Cisco IP Telephony Users

Media Resources

Overview

This lesson will teach you about available media resources in a Cisco IP telephony solution. You will learn how to configure and allocate conferencing, Media Termination Points (MTPs), transcoders, and Music On Hold (MOH) within a Cisco CallManager (CCM) cluster.

Importance

This lesson benefits those students who want to increase their understanding of configuring and allocating the media resources for a Cisco IP telephony deployment.

Objectives

Upon completing this lesson, you will be able to:

- Install and configure the MOH server, unicast Conference Bridge, media streaming application server, and transcoder
- Define and configure Conference Bridge resources
- Define and configure MTP resources
- Define and configure transcoder resources
- Define and configure MOH resources
- Allocate media resources using the media resource management configurations of media resource groups and media resource group lists

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Navigation in Cisco CallManager Administration
- Cisco IOS and Cisco Catalyst operation system command-line basics

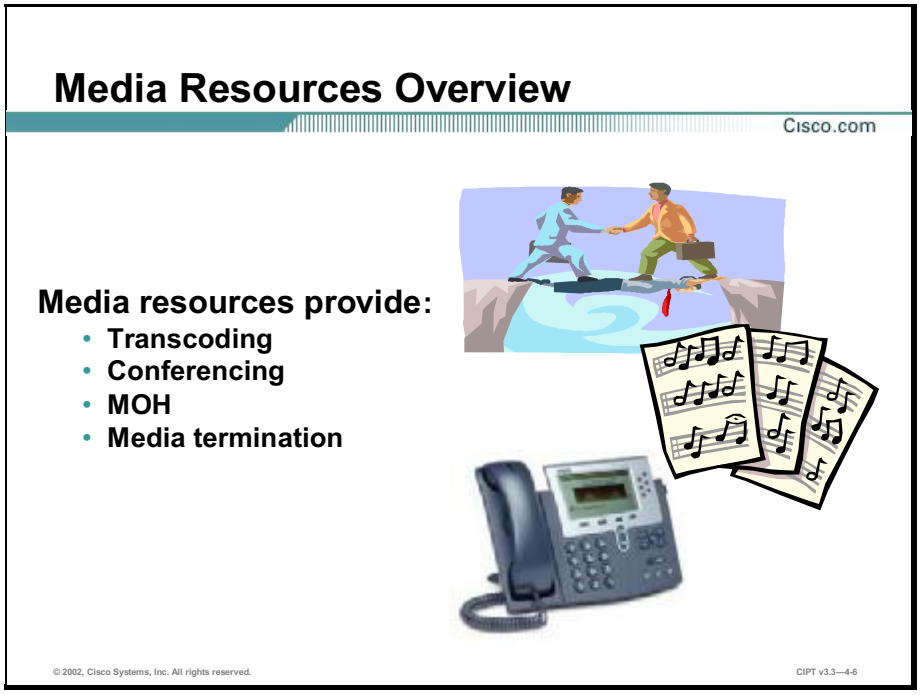
Outline

This lesson includes these topics:

- Overview
- Introduction to Media Resources
- Conference Bridge Resources
- Media Termination Point Resources
- Transcoder Resources
- Music On Hold Resources
- Media Resource Management
- Summary
- Lesson Review

Introduction to Media Resources

This topic examines how to install and configure the Music On Hold (MOH) server, the unicast Conference Bridge (CFB), the media streaming application server, and the transcoder.



Media resources provide services, such as transcoding, conferencing, MOH, and media termination. Media resource management provides access to media resources for all Cisco CallManagers (CCMs) in a cluster. Every CCM contains a software component called a media resource manager. The media resource manager locates a media resource to connect the media streams and to complete the feature.

Media resources are available in both hardware and software. Hardware resources on the Cisco Catalyst 4000 and 6000 series gateway module provide hardware support for the IP telephony features offered by CCM. These features include, hardware-enabled voice conferencing, hardware-based Media Termination Point (MTP) support for supplementary services, and transcoding services. CCM servers provide the software resources.

The available media resources include:

- MOH server
- Unicast CFB
- Media streaming application server (software MTP)
- Transcoder (XCODE)

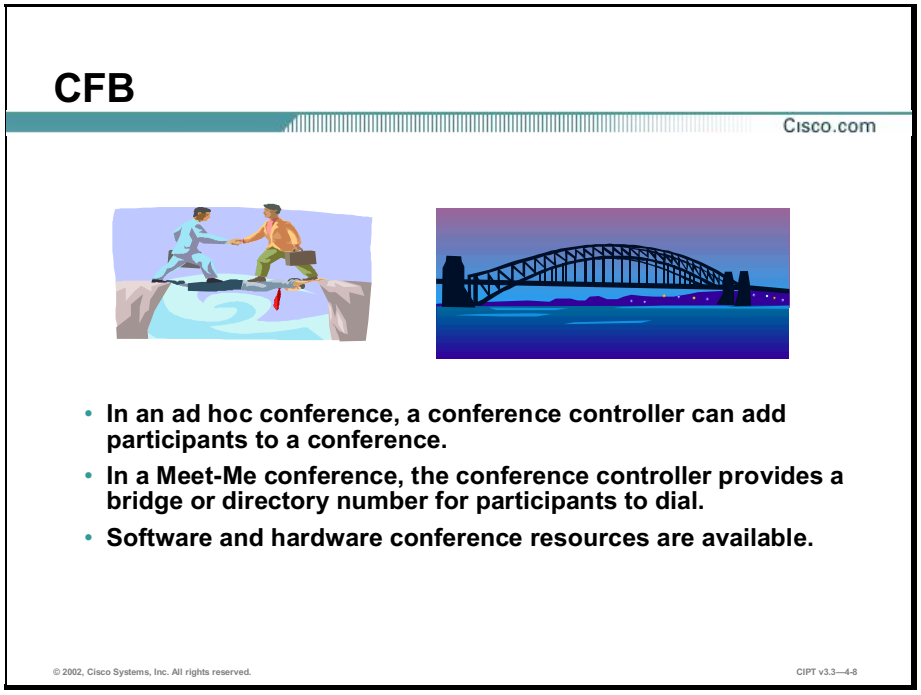
Installing Software Media Resources

After CCM is installed, you must activate the media resources. To activate the services in CCM, access the administration console and choose **Application**>**Cisco CallManager Serviceability**. From the Serviceability window, choose **Tools**>**Service Activation**. You can activate the services on any server you choose.

You must activate the Cisco MOH Audio Translator, Cisco IP Voice Media Streaming App, and the Cisco Messaging Interface services to activate the hardware and software resources. These components support the services that require media resources from the system.

CFB Resources

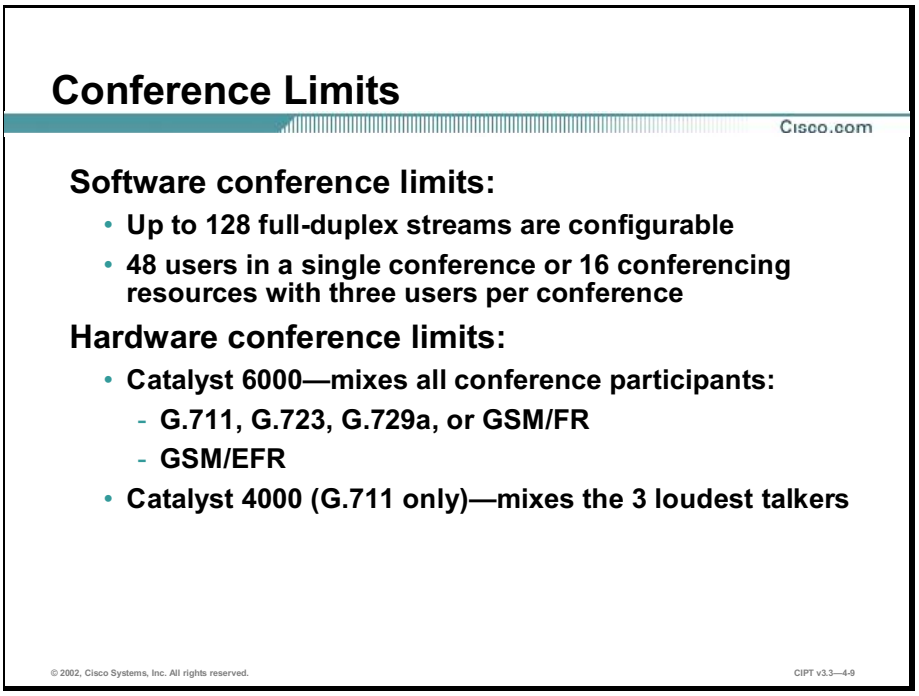
This topic examines how to install and configure software and hardware Conference Bridge (CFB) resources.



CFBs are available as both a software application and as a hardware solution. Each CFB is capable of hosting several simultaneous, multiple-party conferences. CFBs are designed to enable both ad hoc and Meet-Me voice conferencing:

- **Ad hoc conference:** A user, known as the conference controller, adds participants to a conference by calling the new participant and pressing the **Conference** button or **Confrn** softkey. Only the conference controller can add participants to an ad hoc conference. An ad hoc conference can continue if the conference controller hangs up, but new participants cannot be added.

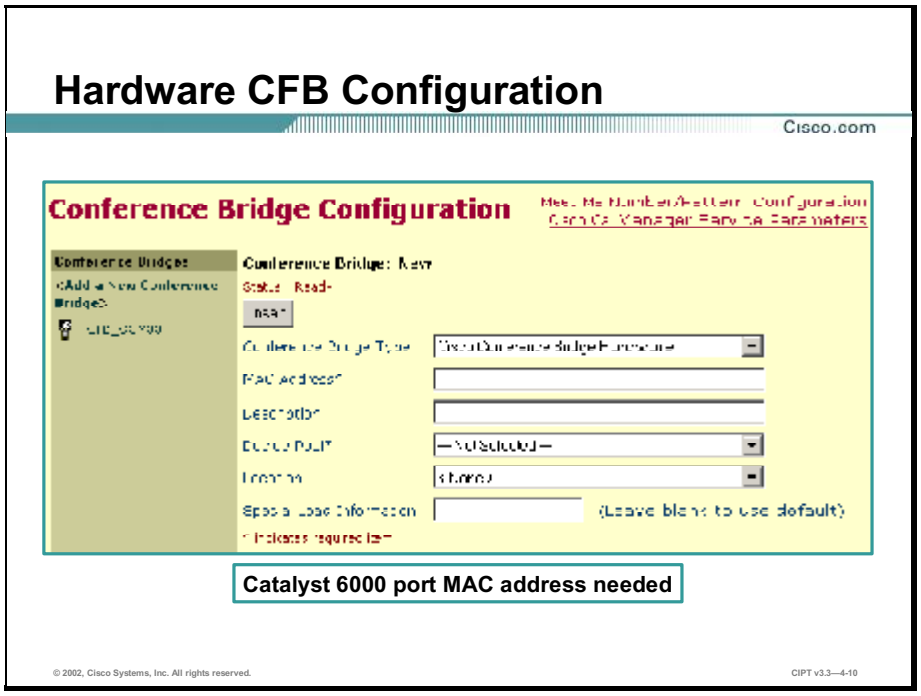
- **Meet-Me conference:** A user, known as the conference controller, presses the **MeetMe** button or softkey and establishes the conference. The conference controller must configure a directory number, or range of directory numbers, in the Cisco CallManager Administration graphical user interface (GUI). The conference controller provides the directory number to the participants, and at the appointed time, participants dial the directory number to join the conference. Participants may leave the conference by hanging up. If the conference controller hangs up, the conference will continue if there are least two participants on the bridge.



The figure and table shown here describe the software and hardware conferencing resource limits.

Table: Software and Hardware Conferencing Resource Limits

Conference Resource	Limitations	Examples
Software installed with Cisco IP Voice Media Streaming application on a supported CCM server platform	G.711 only Up to 128 full-duplex streams are configurable	48 users in a single conference 16 conferencing resources with 3 users in each conference
Catalyst 6000 WS-X6608-T/E1 Configured in Cisco CallManager Administration with port MAC addresses	G.711, G.723, G.729a or GSM/FR 32 conference resources per port	32 users in a single conference on a single port 10 conferences on a single port with 3 users in each conference
	GSM/EFR 24 conference resources per port	24 users in a single conference on a single port. 8 conferences on a single port with 3 users in each conference
Catalyst 4000 WS-X4604-GWY	G.711 only 24 conference resources	Maximum of 4 conferences with 6 participants in each. (Conference restricted to each digital signal processor [DSP] SIMM. Each module has 4 SIMMs with 6 DSPs on each.)

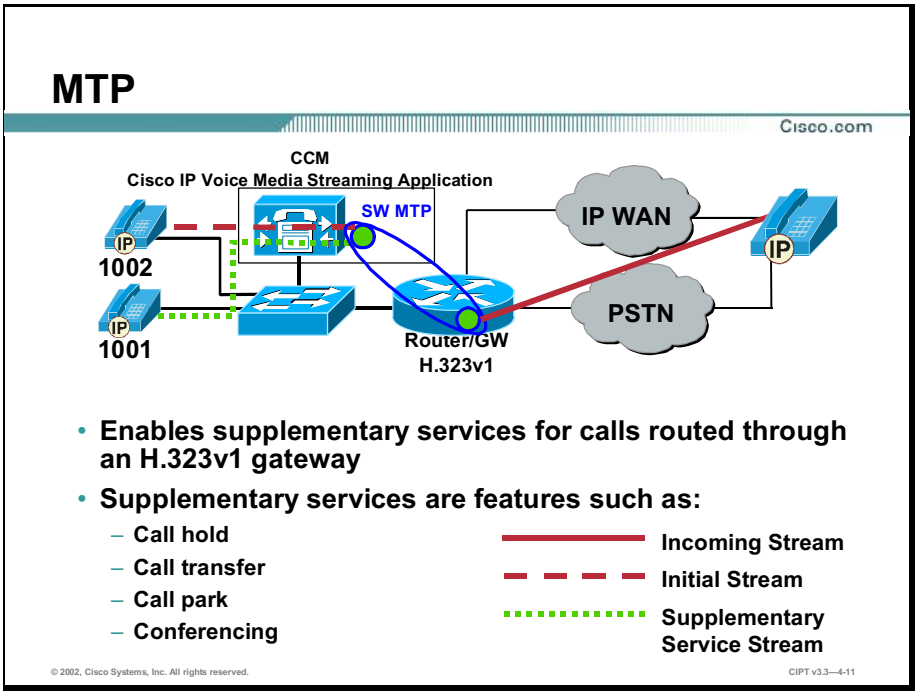


In this figure, the software conference resources are listed in the left column. Hardware conference resources are added to this window. In this example, the MAC address of the Catalyst 6000 series port must be added as a conference resource. The port must be pointed toward the Cisco TFTP server to obtain the configuration file and a list of the CCMs within the Cisco IP telephony network to use for registration.

Users within the cluster can use the ad hoc conference feature. Other users can use the Meet-Me conference feature when a directory number, or directory number range, is configured on the Meet-Me Number/Pattern Configuration page.

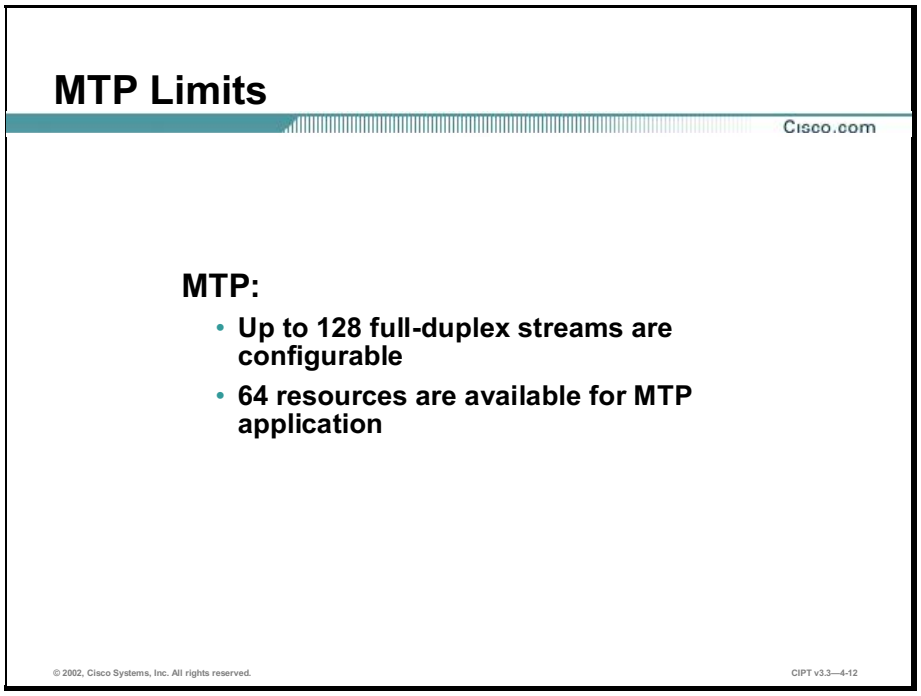
Media Termination Point Resources

This topic examines the MTP resources.



An MTP is a software device that provides supplementary services for calls routed through an H.323v1 gateway. These supplementary services include: call hold, call transfer, call park, and conferencing. They are not available when a call is routed to an H.323v1 endpoint.

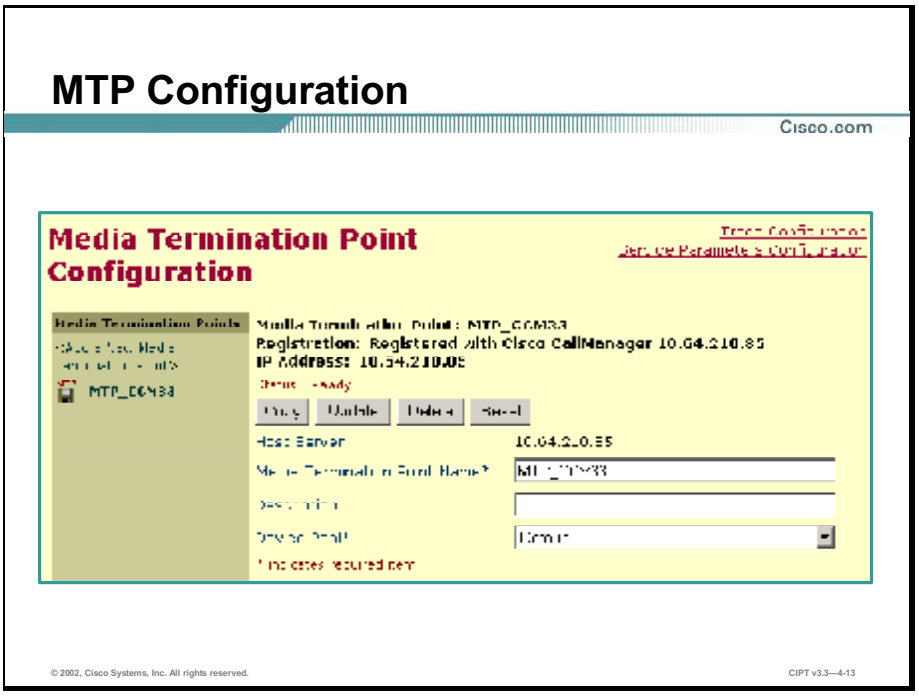
H.323v1 endpoints do not support empty capability sets, and they require an MTP to provide supplementary services. H.323v2 endpoints support empty capability sets, which enable CCM to extend supplementary services without an MTP.



The figure and the table shown here describe the MTP limits.

Table: MTP Limits

Resource Type	Limitations
MTP Installed with the IP Voice Media Streaming application on a supported CCM server platform	G.711 only Up to 128 full-duplex streams are configurable 64 resources are available for MTP application



To configure MTP, you must verfiy that these prerequisites are met:

- Configure servers
- Configure device pool

To configure or add an MTP, choose **Service>Media Resource>MTP** from the Cisco CallManager Administration console.

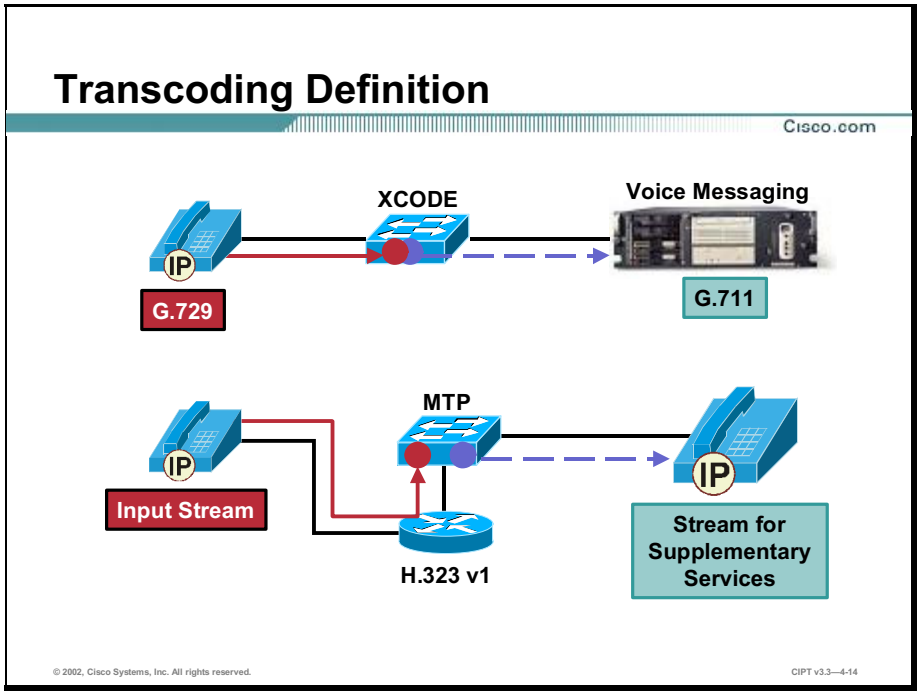
Note	Add only one MTP device for each MTP application.

Table: MTP Configuration Items

Field	Description
Host Server	Choose the server to run MTP.
MTP Name	Enter an MTP name, up to 15 alphanumeric characters.
Description	Enter a description for MTP.
Device Pool	Choose a device pool with the highest priority in the CCM group or choose **Default**.

Transcoder Resources

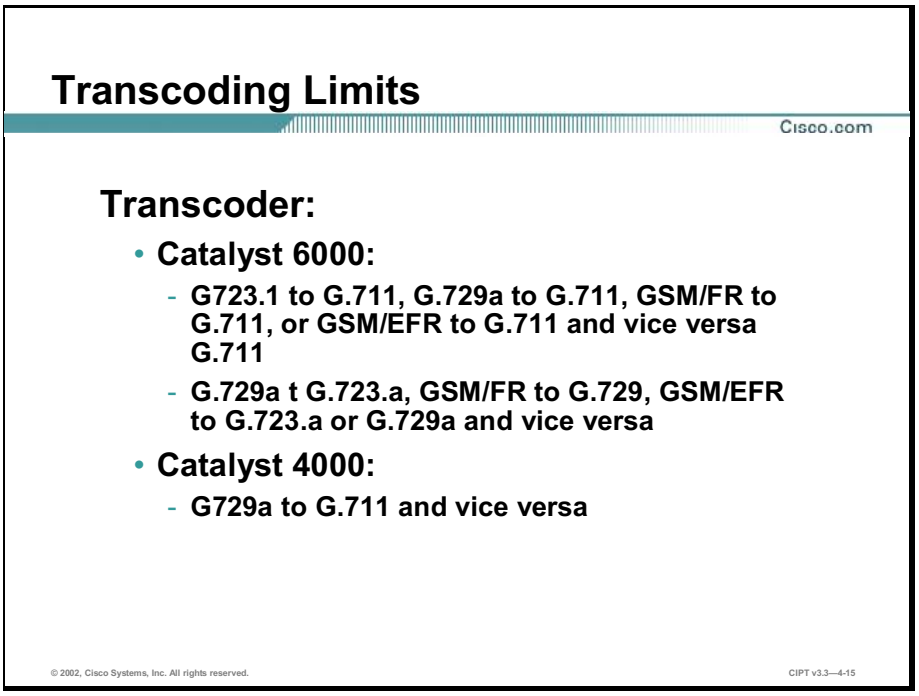
This topic defines transcoder resources and examines transcoder limitations.



A transcoder (XCODE) device takes the output stream of one coder-decoder (codec), converting the data streams from one compression type to another compression type. For example, a transcoder can take an output stream from a G.711 codec and convert it to a G.729 input stream that is accepted by a G.729 codec in real time. Transcoders for CCM convert between G.711, G.723, G.729, and GSM codecs. A transcoder device provides additional capabilities and may be used to enable supplementary services for H.323 endpoints.

This figure shows a transcoder device enabling communication between two different codecs providing an MTP for H.323v1 endpoints.

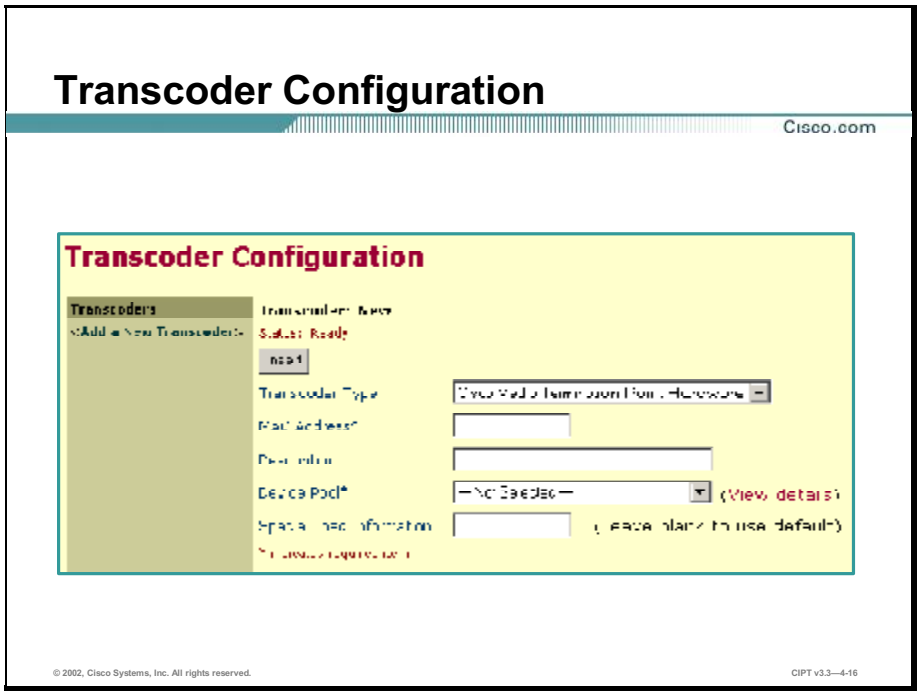
CCM invokes a transcoder device when the two devices are using different codecs and are not able to communicate.



The figure and table shown here describe the MTP and transcoder resource limits.

Table: MTP and Transcoder Resource Limits

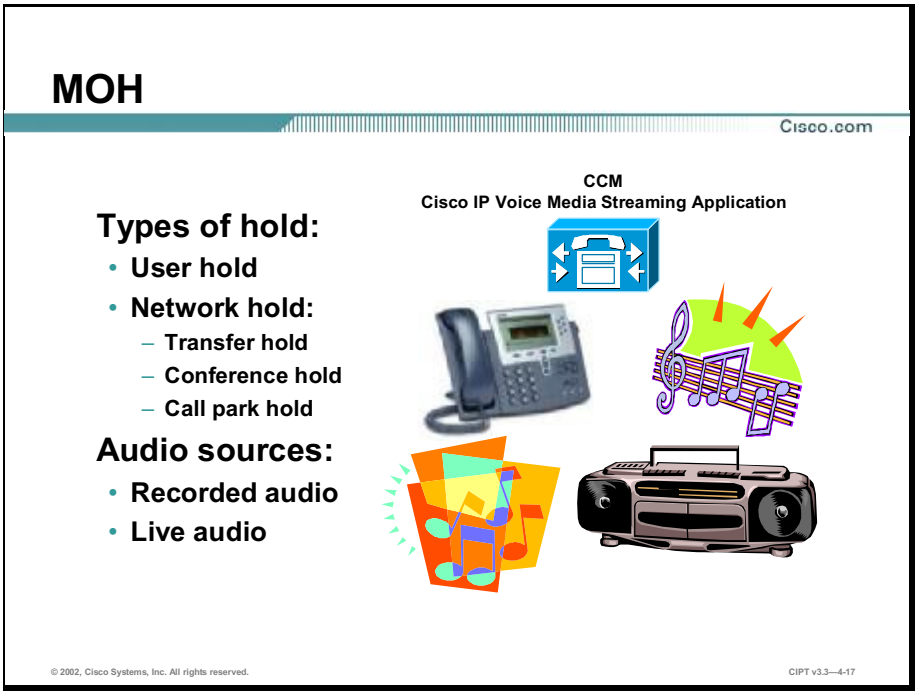
Resource Type	Limitation
Catalyst 6000 WS-X6608-T/E1 Configured in CCM Administration with port MAC addresses Syntax Content Text	G.723 to G.711, G.729a to G.711, GSM/FR to G.711, or GSM/EFR to G.711 and vice versa. 24 transcoder resources per port.
	G.729a to G.723.a, GSM/FR to G.729, GSM/EFR to G.723.a or G.729a and vice versa. 16 transcoder resources per port.
Catalyst 4000 WS-X4604-GWY	G.729a to G.711 and vice versa 16 conference resources per physical module



You need the MAC address of the Catalyst 6000 series port to add a transcoder device. You need the host name of the device to configure a Catalyst 4000 series module.

Music On Hold Resources

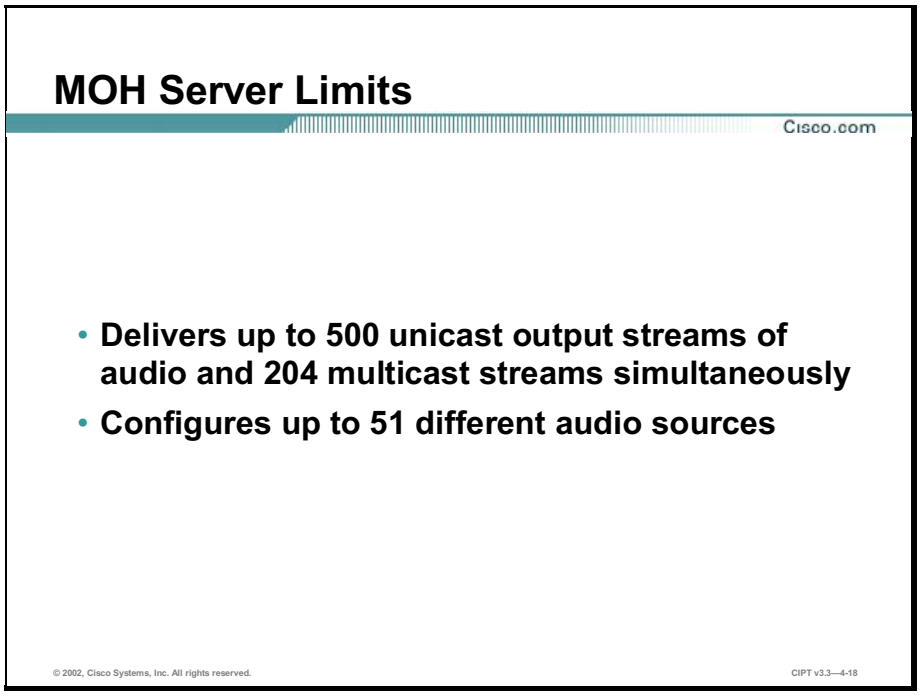
This topic examines the MOH resources installed and configured in CCM.



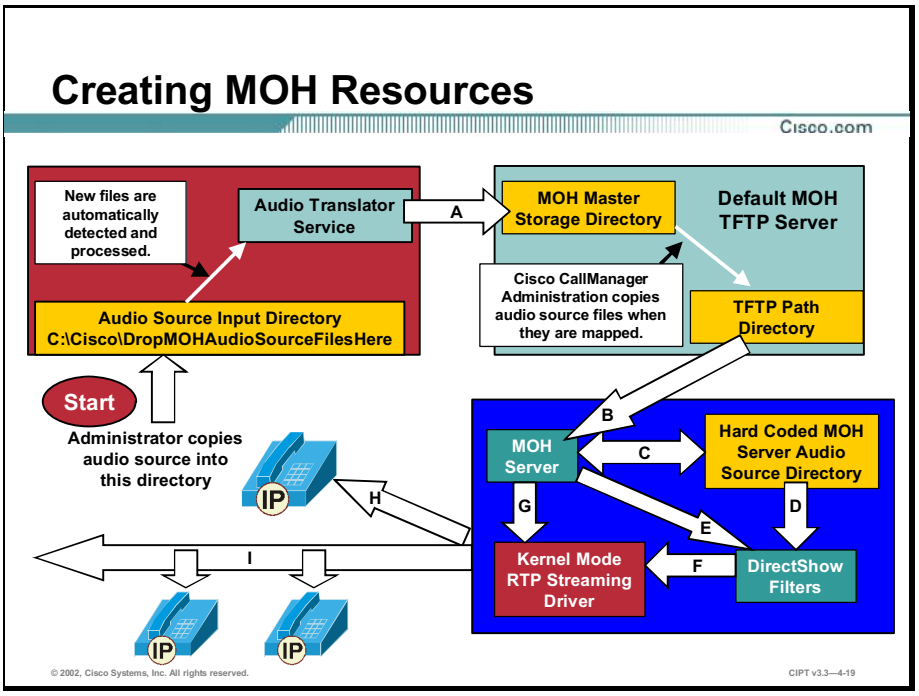
The integrated MOH feature places on-net and off-net users on hold with music from a streaming source. The MOH feature has two hold types:

- **User hold:** A user presses the **Hold** button or **Hold** softkey.
- **Network hold:** A user activates the transfer, conference, or call park feature, which automatically activates the hold.

MOH is customizable so that it plays specific recordings, based on the directory number used to place the caller on hold or the line number that the caller dialed. Recorded audio or a live audio stream also can be configured as audio sources.



The MOH server can simultaneously deliver up to 500 unicast and 204 multicast streams of audio output and can configure up to 51 different audio sources.



This figure shows the interaction between the audio translator, default MOH TFTP server, and the MOH server. The large boxes are the components in a cluster that may reside on a single server or three separate servers. This figure also shows how the MOH server processes the added audio source file.

When adding an audio source file, the network administrator drops the audio files into the C:\Cisco\DropMOHAudioSourceFilesHere directory path. Most standard WAV and MP3 files are valid input.

Note It takes approximately 30 seconds to convert a 3 MB MP3 file.

The file is automatically detected and translated, and the output and source files are moved into the default MOH TFTP server holding directory. This holding directory is the same as the default TFTPMOHFilePath with \MOH appended.

Note Cisco does not recommend using the audio translator service during production hours because the service will consume 100 percent of the CPU.

Then the network administrator assigns the audio source file to an audio source number. The proper audio source files are then copied into one directory to make them available for the MOH servers.

All of the MOH servers in the Cisco IP telephony cluster download the needed audio source files and then store the files in the hard coded directory, C:\Program Files\Cisco\MOH. The MOH server then streams the files using DirectShow and the kernel mode Real-Time Transport Protocol (RTP) driver as needed and/or requested by CCM.

Here is the explanation of the lettered arrows in this figure:

A. Create audio source files, move original source, create XML report

B. TFTP the needed audio source files

C. Validate and download

D. WAV files

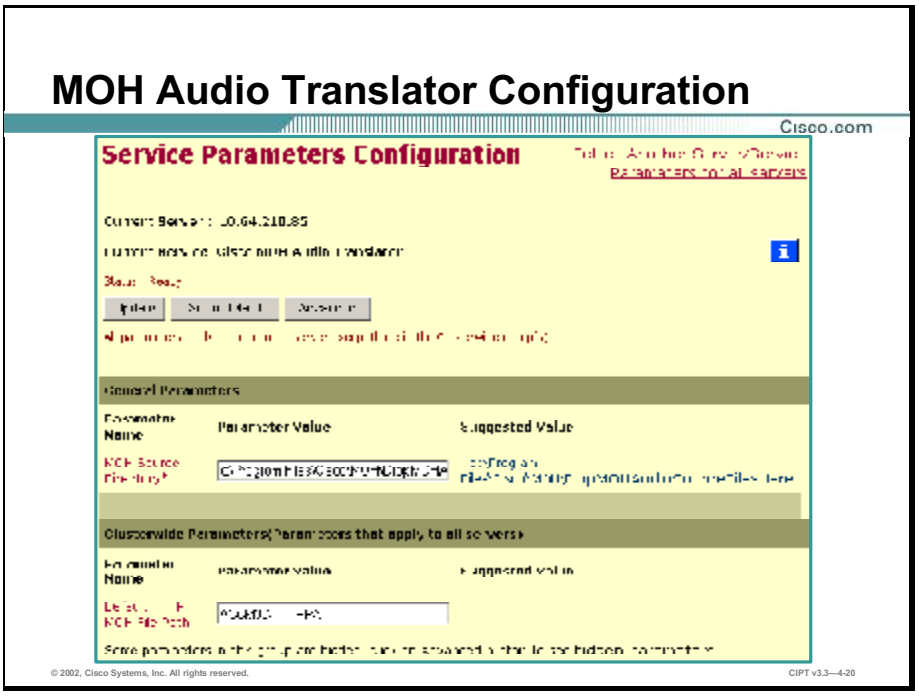
E. Controls

F. RTP data

G. Controls

H. Unicast RTP stream

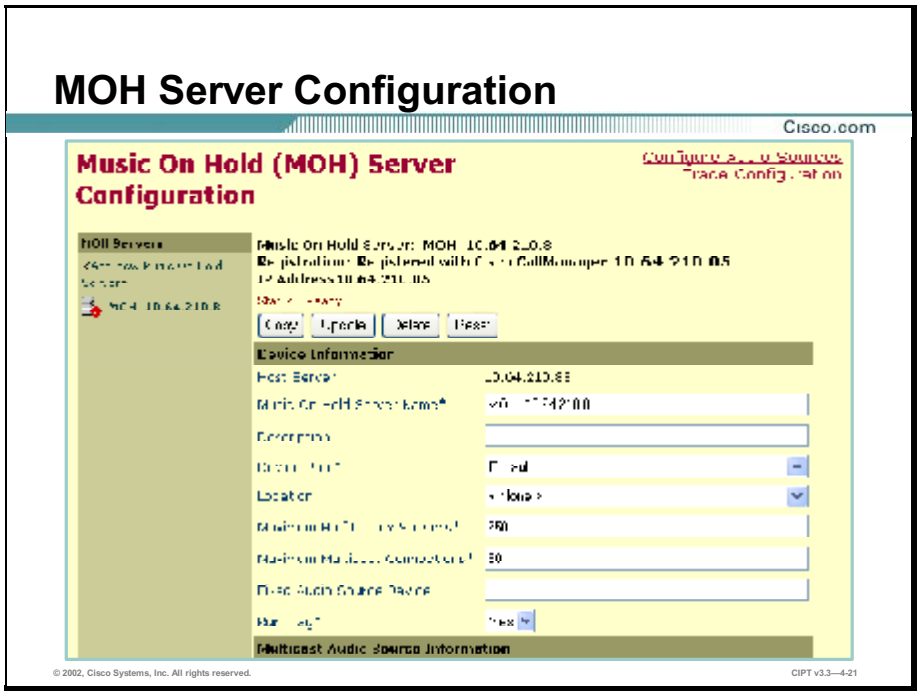
I. Multicast RTP stream



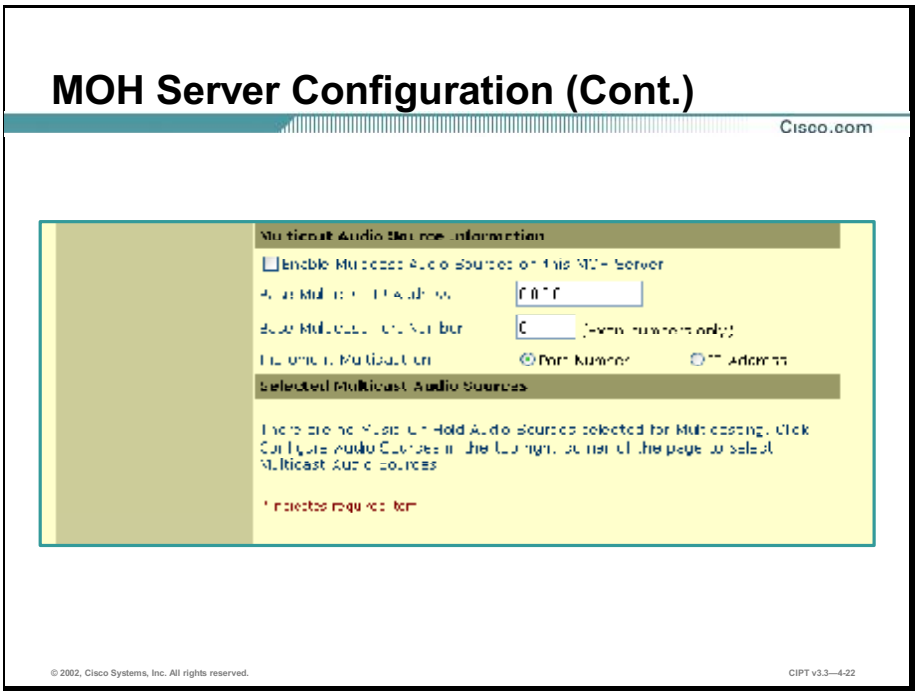
The audio files are stored on each server. Each server will also stream the files when required. The MOHSourceDirectory and the default TFTPMOHFilePath in the Cisco CallManager Administration Service Parameters Configuration page, are shown in this figure and are defined as:

- **MOHSourceDirectory:** This input directory indicates the directory where the audio source files are converted and made usable to the MOH server. The install program automatically sets this field. The default setting is: C:\Cisco\DropMOHAudioSourceFilesHere.

- **Default TFTPMOHFilePath:** This output Universal Naming Convention (UNC) path name must indicate the default MOHTFTP server share. The install program automatically sets this field, which is a service-wide setting.

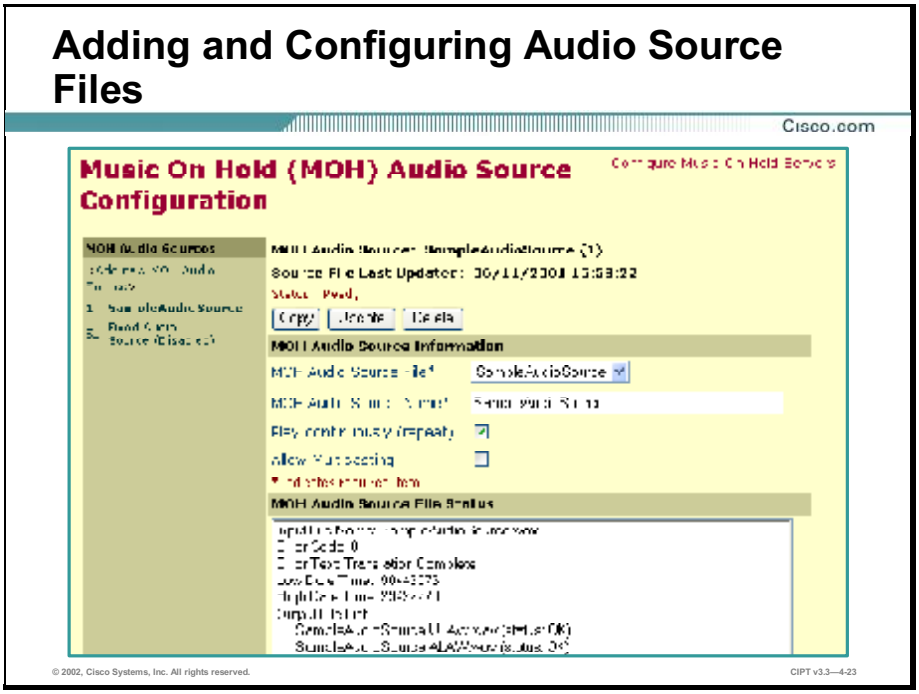


This figure shows the MOH server configuration page. The MOH server can be configured for unicast or multicast.



Choose **Help**>**For this page** on the Cisco CallManager Administration Service Parameters Configuration page to ensure that all required settings are complete, as shown here.

Adding and Configuring Audio Source Files

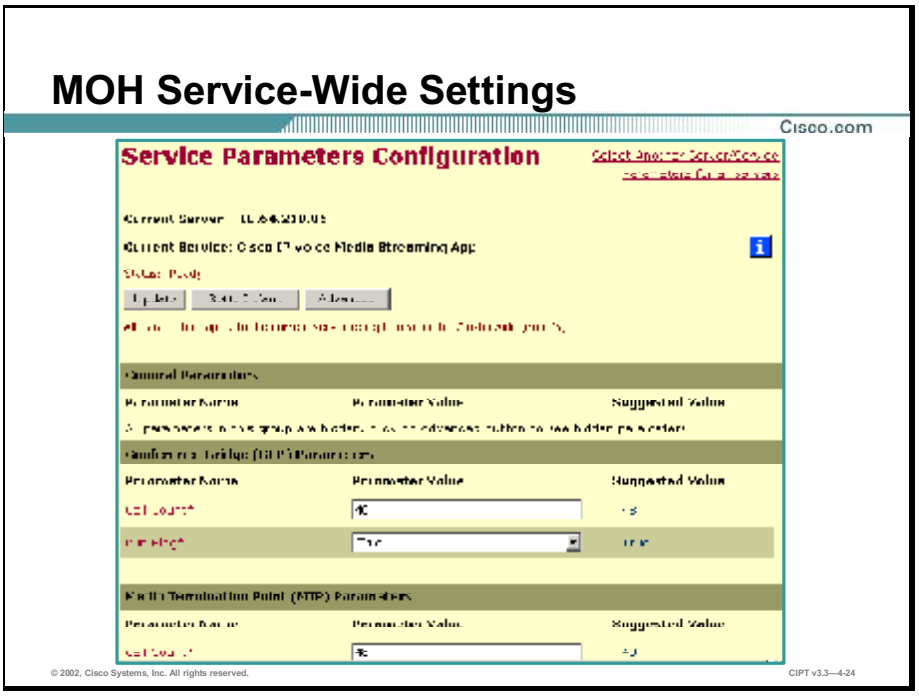


When all audio sources are added or updated (except for the fixed audio source), the changes will affect all of the MOH servers. All of the processed audio sources will appear in the MOH Audio Source File drop-down menu.

The Play continuously (repeat) check box should always be checked. If multicast capabilities are necessary, you must check the **Allow Multicasting** check box. If the Play continuously (repeat) and Allow Multicasting check boxes are both unchecked, the audio file stops playing after it reaches the end and the network administrator will have to stop and start the server to reset the MOH server.

The MOH Audio Source File Status window shows the conversion status and indicates if the audio file translated correctly or if it had any errors.

MOH Service-Wide Settings



To set the MOH service-wide settings, open the Service Parameters Configuration page, choose an MOH server, and select the Cisco IP Voice Media Streaming App option. The Service Parameters Configuration window for MOH displays, as shown here.

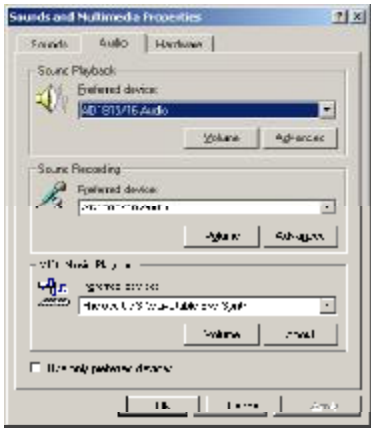
Note The other service parameters on this page are for MTP and software CFB resources.

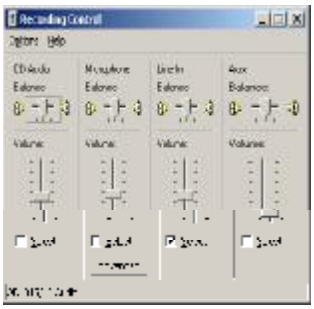
The Supported MOH Codecs field is set to the codecs that are supported by the MOH servers in the cluster. This field defaults to G.711 ulaw during the installation. You can enable multiple codecs by holding down the **Ctrl** key to select the codecs.

The Default TFTPMOH IP Address is set to the IP address or computer name of the default MOH TFTP server.

Finding the Fixed Audio Source Name

Cisco.com





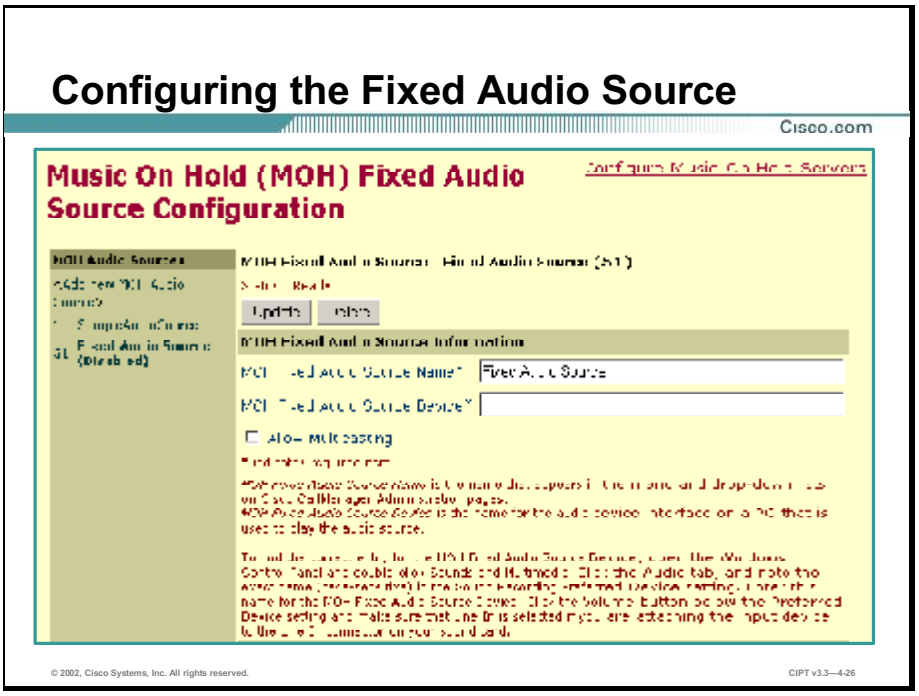
CIPT v3.3—4-25

To find the name of the fixed audio source, use the Control Panel to open the Sounds and Multimedia Properties window, and verify that the proper input source is selected.

To open the Sounds and Multimedia Properties window, open the Control Panel and choose the **Sounds and Multimedia** option. Select the **Audio** tab. You can use any sound recording device name that appears in the Preferred device menu.

To open the Recording Control window, click the **Volume** button in the Sound Recoding area. Verify that the Line In, Microphone, or CD Audio option is selected.

Configuring the Fixed Audio Source



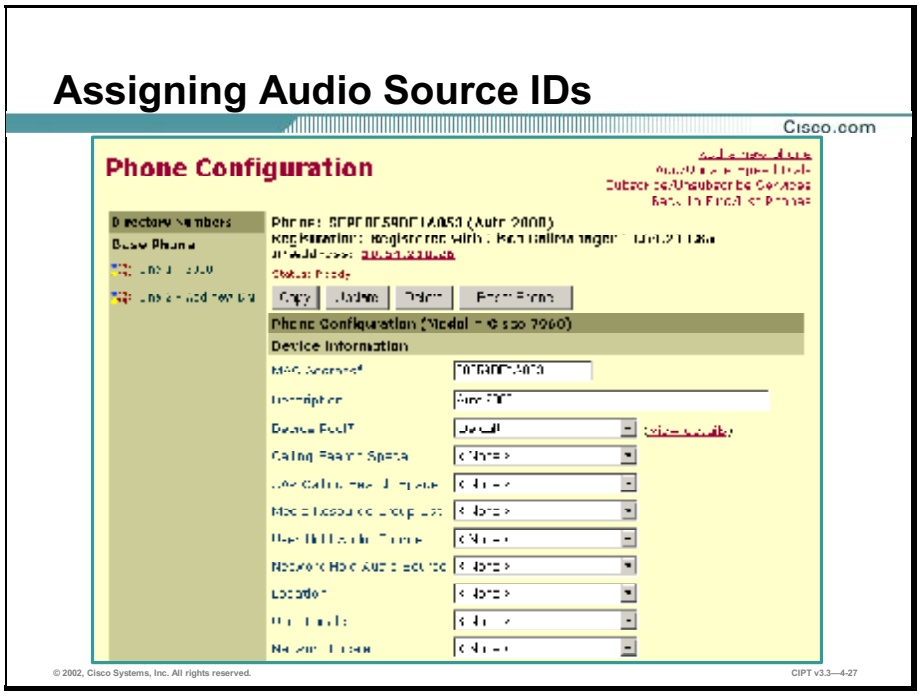
The Fixed Audio Source Name is case sensitive and must be entered exactly as it appears in the Sounds and Multimedia Properties window, including any spaces or symbols that appear in the name.

If the Allow Multicasting check box is checked, and the G.729 codec is enabled, 5 to 7 percent of the CPU will be consumed. This setting is global for all MOH servers. If the fixed audio source does not exist on a server, it cannot be used.

You can override the Fixed Audio Source Name, on a per MOH server basis, via the MOH Server Configuration page.

The selected fixed audio source that appears on the left side of the window in this figure is available as an option.

The Fixed Audio Source option affects all of the MOH servers that have an MOH Fixed Audio Source Device by the selected name. If the device does not exist, it cannot be used.



An audio source ID represents an audio source on the MOH server. The audio source can either be a file on a disk or a fixed device from which a source stream obtains the streaming data. Each audio source (represented by an audio source ID) can stream in unicast and multicast mode.

There are two types of hold:

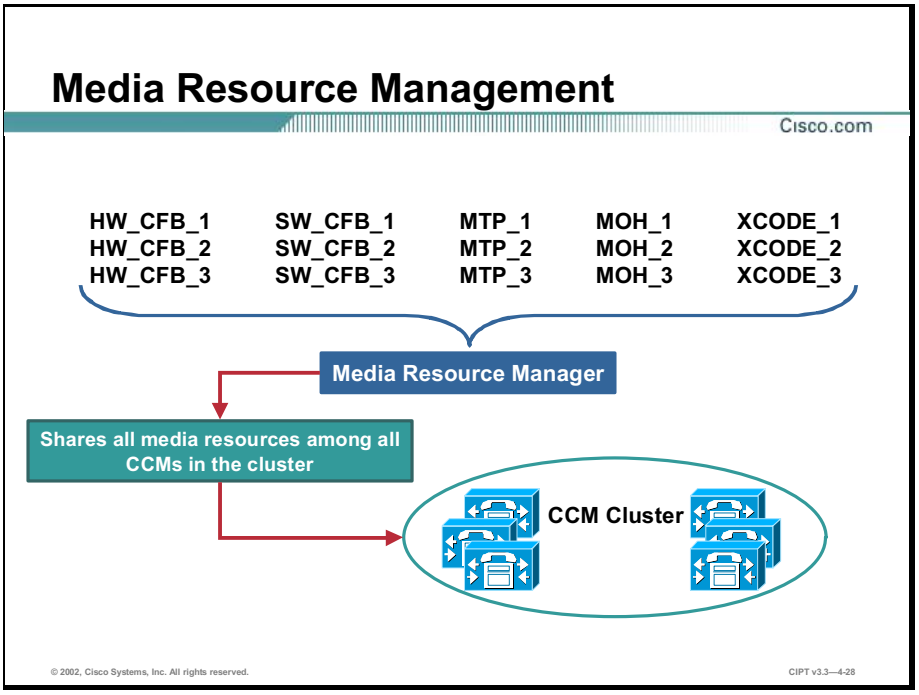
- **User hold:** To specify the audio source that is played when a user initiates a hold action, choose an audio source from the list that displays on the User Hold Audio Source drop-down menu. If you do not choose an audio source, CCM uses the audio source that is defined in the device pool, or the system default, if the device pool does not specify an audio source ID.

- **Network hold:** To specify the audio source that is played when the network initiates a hold action, choose an audio source from the list that displays from the Network Hold Audio Source drop-down menu. If you do not choose an audio source, CCM uses the audio source that is defined in the device pool, or the system default, if the device pool does not specify an audio source ID.

The device that activates the hold will determine which audio source ID the caller will listen to.

Media Resource Management

This topic examines media resource management within a Cisco IP telephony solution using media resource groups (MRG) and media resource group lists (MRGL).

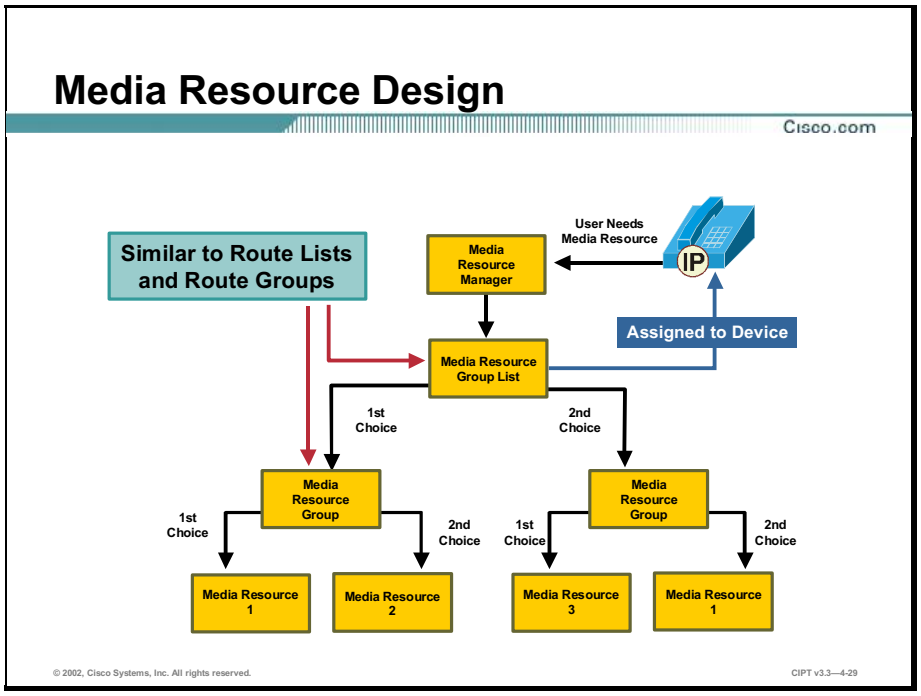


The Media Resource Manager (MRM) is an integral component of CCM. The MRM controls and manages the media resources within a cluster, allowing all CCMs within the cluster to share media resources. This figure shows the MRM controlling all of the media resources that are shared within a CCM cluster.

The MRM enhances CCM features by making it easier for CCM to deploy transcoder, conferencing, MTP, and MOH resources. MRM distribution throughout the CCM cluster uses these resources to their full potential, making the CCM cluster more efficient and more economical.

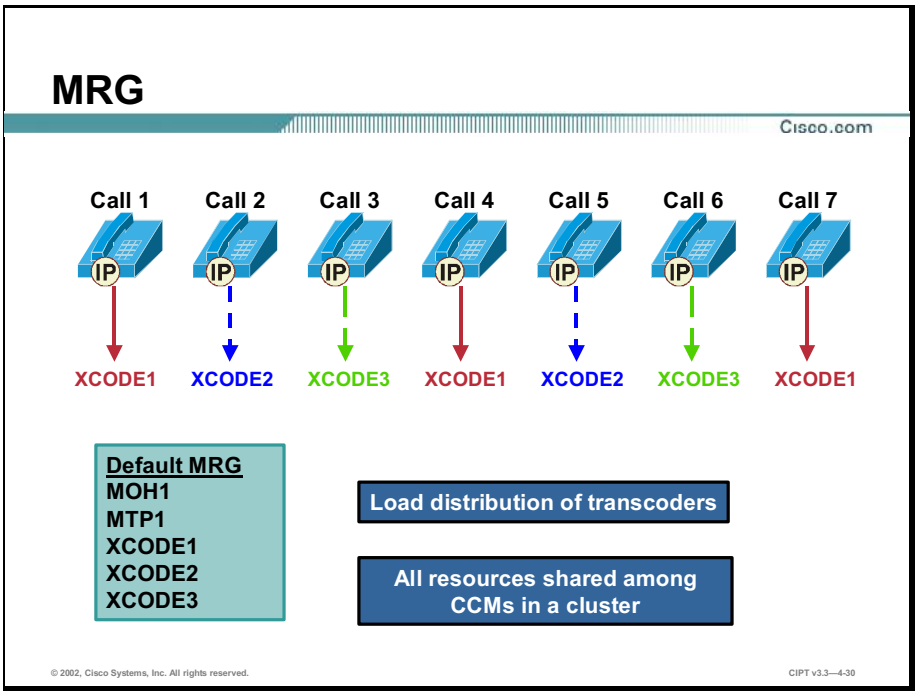
The reasons that resources are shared include:

- To enable both hardware and software devices to coexist within a CCM
- To enable CCMs to share and access the resources that are available in the cluster
- To enable CCM to perform load distribution within a group of similar resources
- To enable CCM to allocate resources based on user preference



This figure shows the hierarchical ordering of media resources and how MRGs and MGRLs are similar to route groups and route lists.

When a device needs a media resource, it searches its own MRGL first. If a media resource is not available, the device searches the default list, which includes all of the media resources that have not been assigned to an MRG. After a resource is assigned to an MRG, it is removed from the default list.



MRGs define logical groupings of media servers. MRGs can be associated with a geographical location or site, and they can control the usage of servers or the desired type of service.

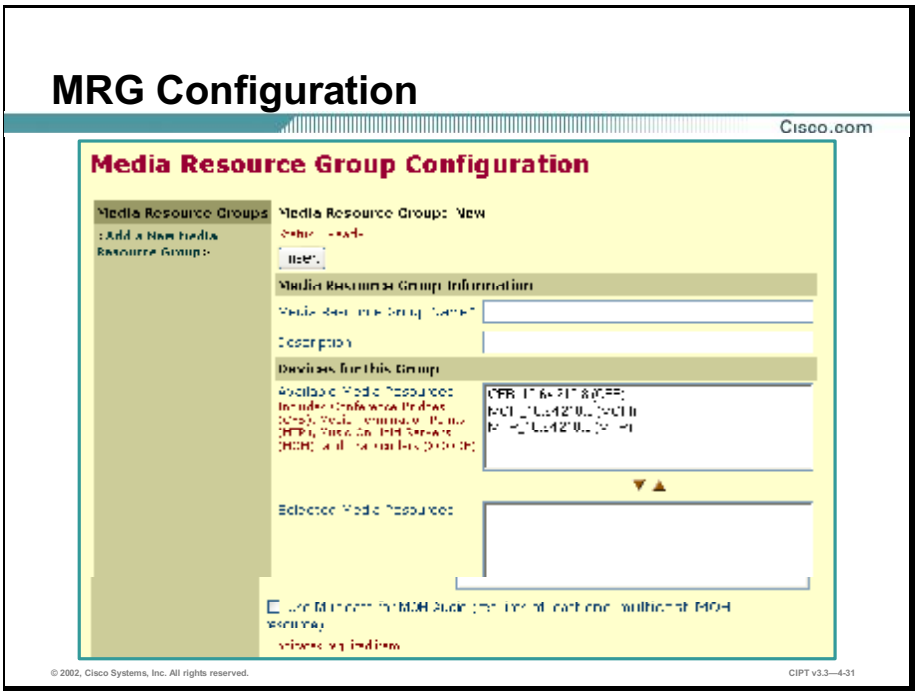
CCM provides a default list of media resources. The default list of media resources includes all of the media resources that have not been assigned to an MRG. If media resources have been configured but no MRGs have been defined, all media resources are on the default list, and all media resources are available to all CCMs within a given cluster.

This figure shows how media resources are allocated to devices when they are listed in an MRG. Using this figure, the default media resource for a CCM comprises the following media resources: MOH1, MTP1, XCODE1, XCODE2, and XCODE3. The MRM distributes the load evenly among the transcoder resources in its default MRG for calls requiring a transcoder resource. This is the allocation order for incoming calls that require a transcoder resource:

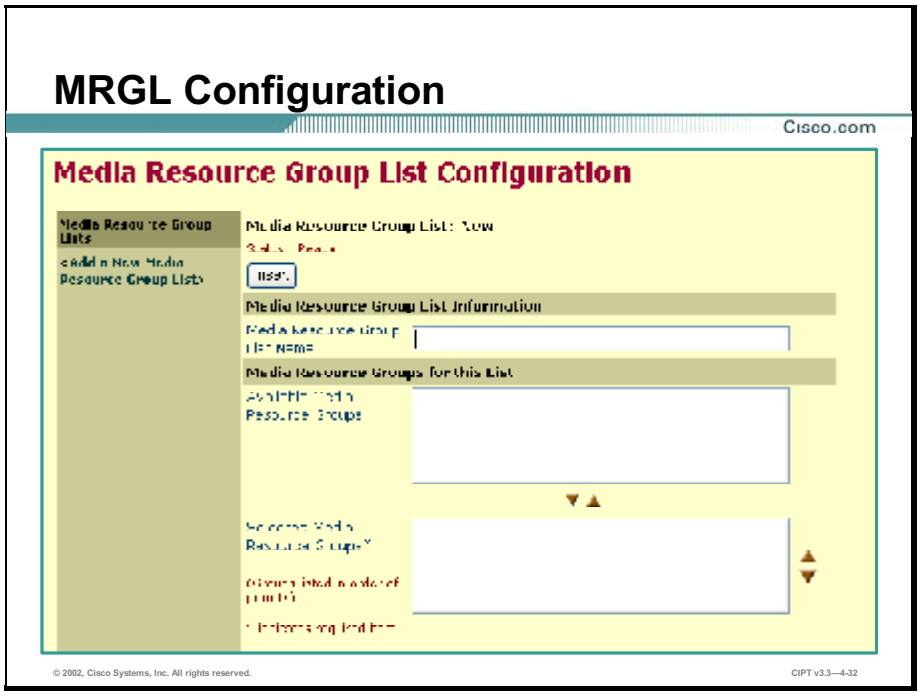
- Call 1 uses XCODE1
- Call 2 uses XCODE2
- Call 3 uses XCODE3
- Call 4 uses XCODE1
- Call 5 uses XCODE2
- Call 6 uses XCODE3
- Call 7 uses XCODE1

Note This order assumes that all transcoder resources use the same type of hardware

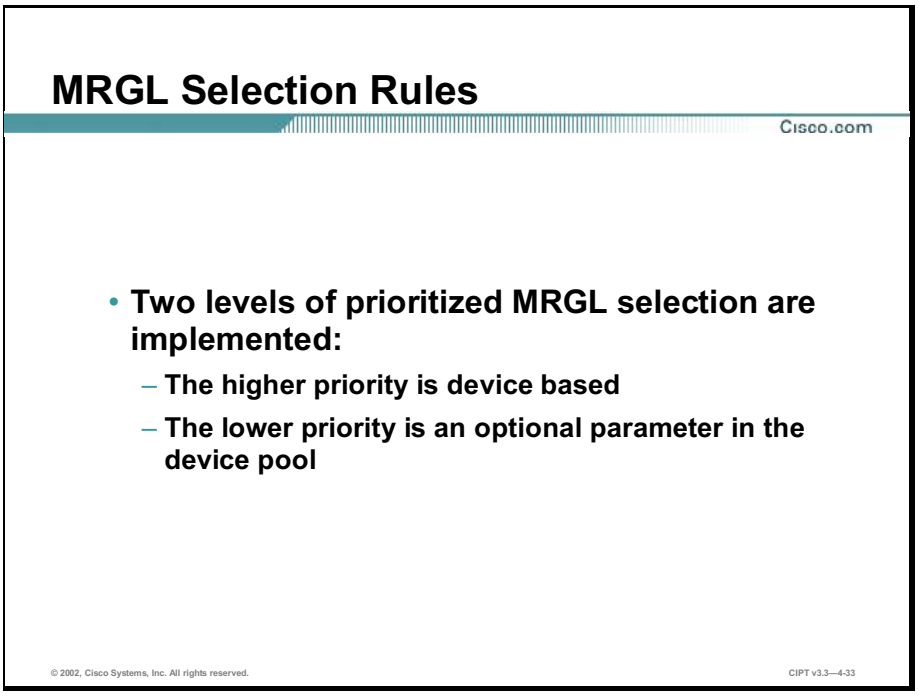
MRG Configuration



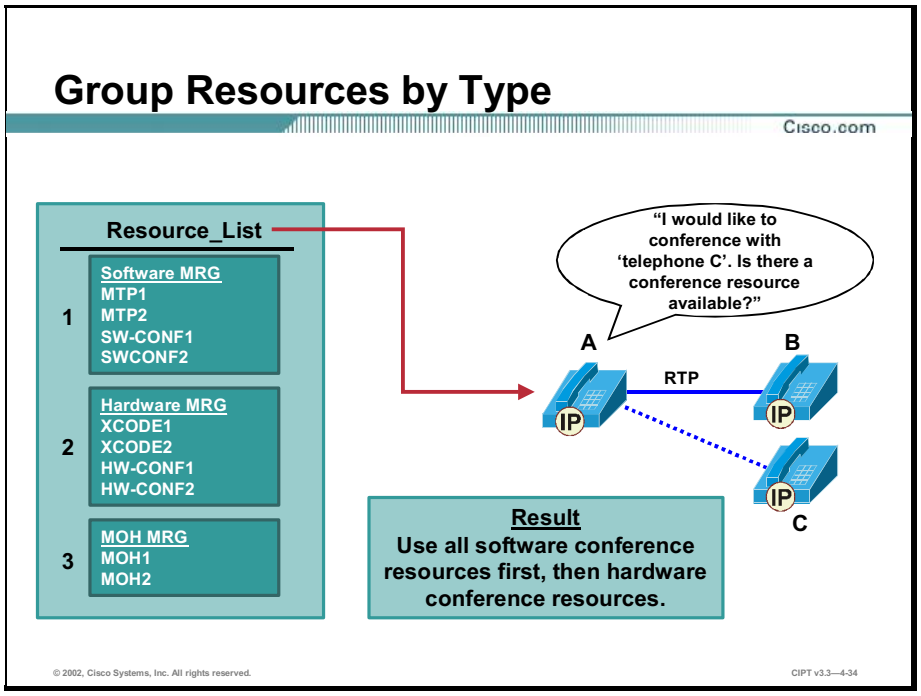
Configuring an MRG is similar to configuring a route group. Enter a name and description for the MRG and then add the media resources.



Use the MRGL Configuration page to configure MRGLs. Enter a name for the MRGL and then add the MRGs.



There are two levels at which MRGLs can be assigned to devices. The highest priority MRGL level is configured at the device. For example, an IP Phone is configured on the Phone Configuration page in Cisco CallManager Administration. The lower priority level is an optional parameter of the device pool. If an MRGL is not configured at the device level, it will use the MRGL configured at the device pool level first, and then, if there are no resources available, it will try to use resources in the default list. If a device does have an MRGL configured at the device level, that MRGL is used first. When there are no resources available from that MRGL, the device attempts to use the media resources on the default list.



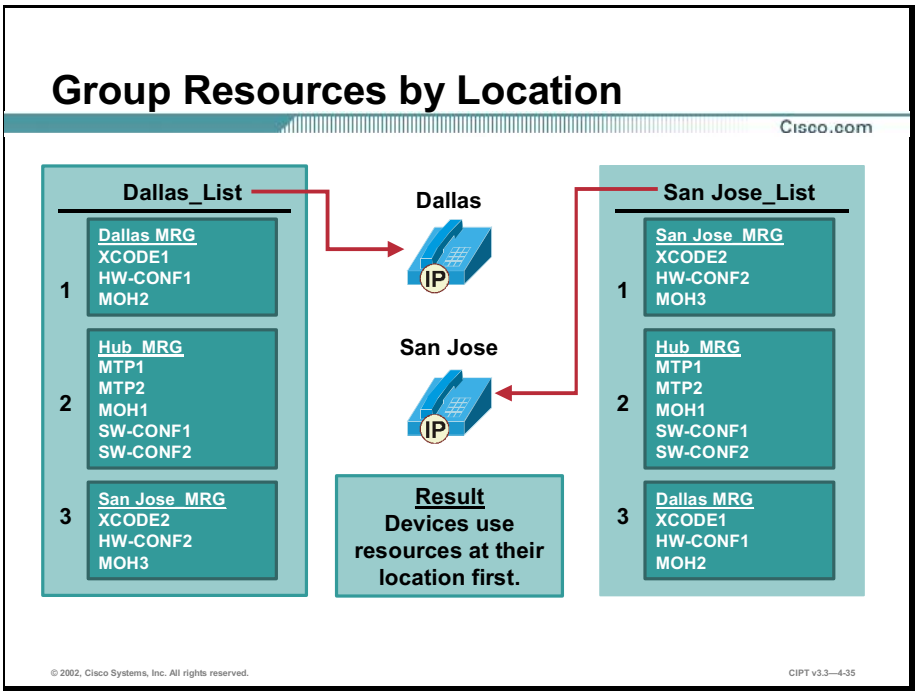
This figure shows how conference resources are allocated when resources are grouped by type and the software conference resource group is listed *before* the hardware conference resource group in the MRGL.

The media resources are assigned to three MRGs as listed:

- **Software MRG:** MTP1, MTP2, SW-CONF1, and SW-CONF2
- **Hardware MRG:** XCODE1, XCODE2, HW-CONF1, and HW-CONF2
- **MOH MRG:** MOH1 and MOH2

Create an MRGL, Resource_List, and assign the MRGs in this order: software MRG, hardware MRG, and MOH MRG.

In this arrangement, when a conference is needed, CCM allocates the software conference resources first. The hardware conference resources are not used until all of the software conference resources are exhausted.



This figure shows media resources that are grouped by location. Devices use the media resources in their location before using the media resources at the central site (hub).

This example is for multiple-site WAN deployments using centralized call processing. All CCM and software resources are located at the central site. For devices at the Dallas, Texas and San Jose, California locations, it is more efficient to use media resources that are physically located at their location rather than using a resource across the WAN.

Media resources are assigned to these three MRGs:

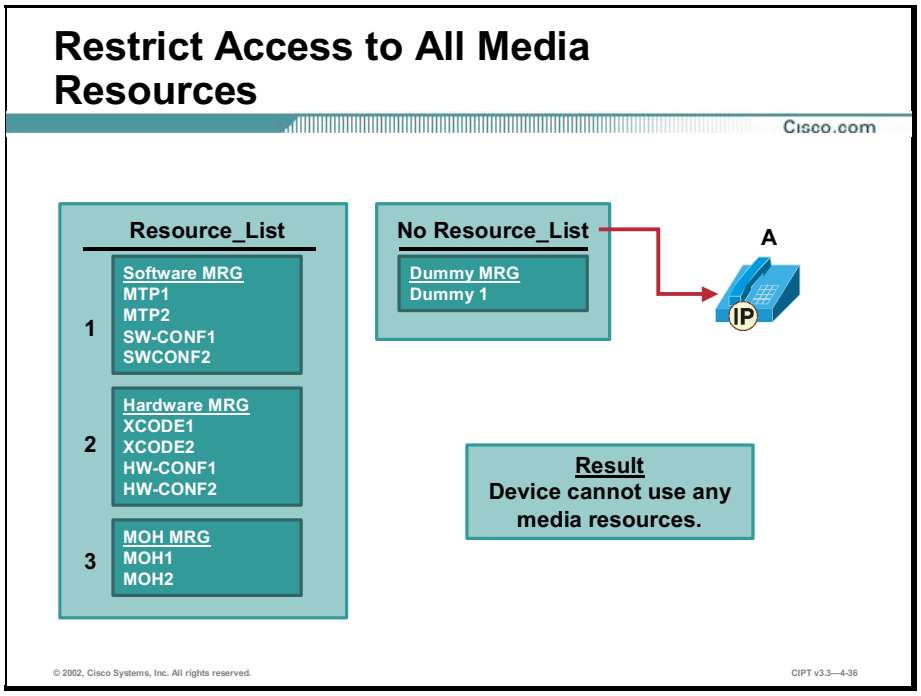
- **Hub MRG:** MTP1, MTP2, MOH1, SW-CONF1, and SW-CONF2
- **Dallas MRG:** XCODE1, HW-CONF1, and MOH2
- **San Jose MRG:** XCODE2, HW-CONF2, and MOH3

Create a Dallas_List MRGL and assign the MRGs so that the resources are available in this order: local hardware resources first (Dallas MRG), software resources second (Hub MRG), and distant hardware resources third (San Jose MRG).

Create a SanJose_List MRGL and assign the MRGs so that the resources are available in this order: local hardware resources first (San Jose MRG), software resources second (Hub MRG), and distant hardware resources third (Dallas MRG).

Assign an IP Phone in Dallas to use the Dallas_List and an IP Phone in San Jose to use the SanJose_List.

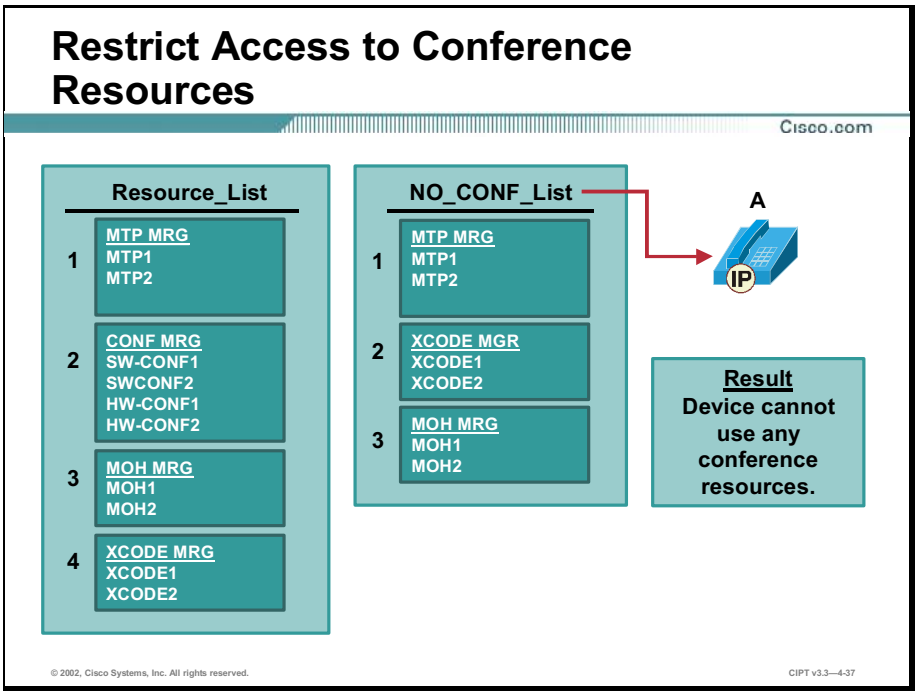
With this arrangement, the IP Phone in Dallas will use the Dallas_List resources before using the SanJose_List resources.



This figure shows how to restrict the media resources available to a device by assigning an MRGL that has a dummy media resource.

To verify that a device cannot access media resources, ensure that all media resources are assigned to an MRG. Add a dummy media resource to the dummy MRG, and add that MRG to the NoResource_List MRGL. Assign the telephone device, IP Phone A for example, to the NoResource_List.

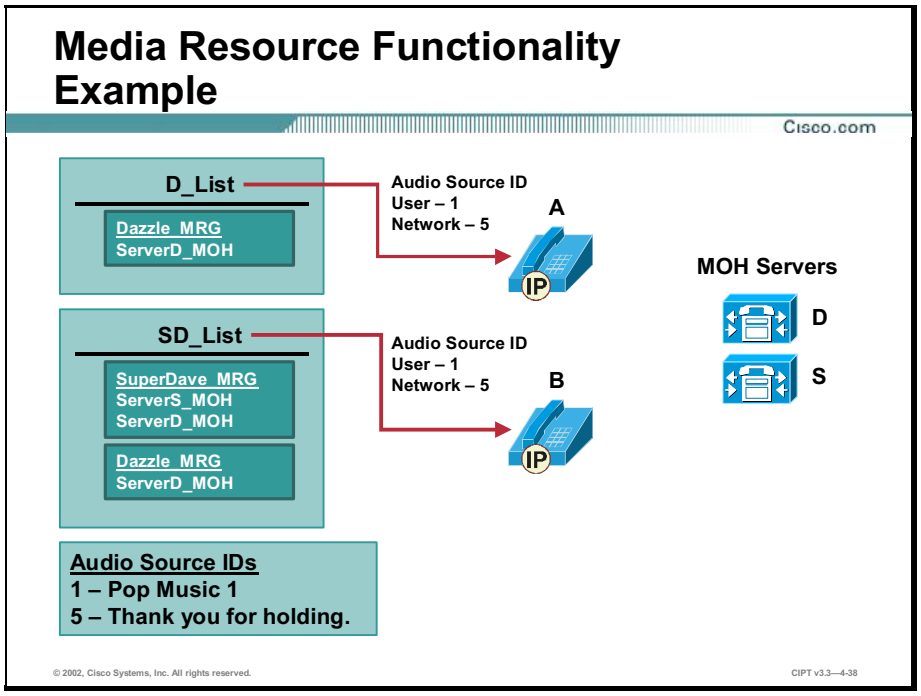
The IP Phone cannot use any media resources when configured this way because the only device in the NoResource_List is a dummy media resource, which the IP Phone will attempt to use.



This figure shows how to restrict the conference resources available to devices by changing the configuration of the MRGs and MRGLs.

Create an MRGL, Resource_List, with all of the media resources. Create an MRGL, NO_CONF_LIST, and assign MRGs to it in this order: MTP MRG, XCODE MRG, and MOH MRG. In the device configuration, assign the name NO_CONF_LIST for the MRGL.

The device cannot use conference resources. Only the MTP, XCODE, and MOH resources are available to the device.



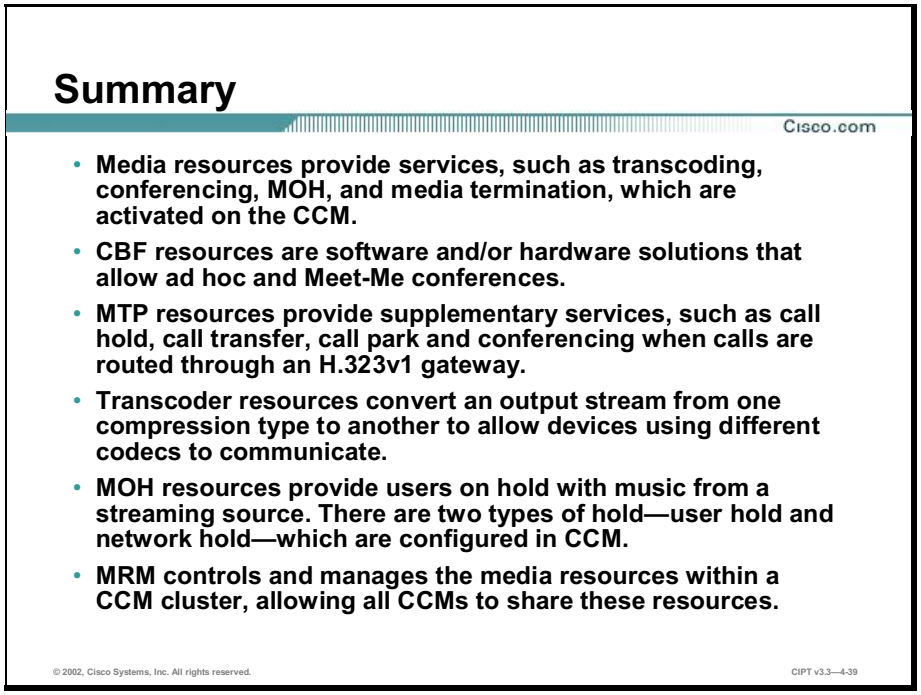
This list describes the configuration setup shown in this figure:

- **Two MRGs:**
  - Dazzle_MRG is composed of the MOH server D, labeled ServerD_MOH.
  - SuperDave_MRG is composed of a prioritized list of MOH servers, S and D, which are labeled ServerS_MOH and ServerD_MOH, respectively.
- **Two MRGLs:**
  - D_List consists of the Dazzle_MRG.
  - SD_List consists of the SuperDave_MRG and Dazzle_MRG (prioritized order).
- **Two audio source IDs:**
  - Audio source ID 1 plays the **Pop Music 1** Audio Stream.
  - Audio source ID 5 plays the **Thank you for holding** Audio Stream.
- **Two Cisco IP Phones:**
  - Cisco IP Phone A is assigned the MRGL D_List and the audio source ID 1, Pop Music 1 (for user hold), and audio source ID 5, Thank you for holding (for network hold).

- Cisco IP Phone B is assigned MRGL SD_List and audio source ID 1, Pop Music 1 (for user hold), and audio source ID 5, Thank you for holding (for network hold).

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Softkey Template lesson

References

For additional information, refer to this resource:

- Anne Smith, Chris Pearce, Delon Whetton, John Alexander. *Cisco CallManager Fundamentals: A Cisco AVVID Solution.* San Jose, California, Cisco Press; 2001, ISBN: 1-58705-008-0

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of these services does an MTP resource provide for an H.323v1 type gateway?

A) transcoding services

B) MOH

C) conferencing

D) supplementary services

Q2) When is it recommended to run the audio translator?

A) any time of the day

B) during peak call-processing hours

C) during off-peak hours

D) none of the above

Q3) Which of these statements best describes MRGLs?

A) an ordered list of media resources

B) an ordered list of media gateways

C) an ordered list of media resource groups

D) none of the above

Q4) Which of these services do media resources provide?

A) MOH

B) unicast CFB

C) media streaming application server

D) transcoding

E) multiplexing

Q5) Which of these are needed to configure Catalyst 6000 series hardware CFB?

A) MAC address

B) IP address

C) port address

D) Meet-Me number

Q6) Which of these items takes the output stream of one codec and converts it from one compression type to another?

A) transcoder device

B) MTP

C) CFB

D) device pool

Softkey Template

Overview

This lesson will teach you that there are various softkey configurations that are associated with the applications that Cisco IP Phones (models 7960 and 7940) support. You will learn two types of softkey configurations: standard and nonstandard.

Importance

This lesson benefits those students who want to learn how to configure softkeys on Cisco IP Phones for improved functionality.

Objectives

Upon completing this lesson, you will be able to:

- Define softkey templates
- Configure nonstandard softkey templates
- Add application softkeys to nonstandard softkey templates
- Modify softkey positions in a nonstandard template
- Assign softkey templates to Cisco IP Phones
- Delete softkey templates

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Navigation in Cisco CallManager Administration
- Cisco IOS and Cisco Catalyst operation system command-line basics

Outline

This lesson includes these topics:

- Overview
- Overview of the Softkey Template
- Configuring Nonstandard Softkey Templates
- Adding Application Softkeys to Nonstandard Softkey Templates
- Modifying Softkey Positions
- Assigning Softkey Templates to Devices
- Deleting Softkey Templates
- Summary
- Lesson Review

Overview of the Softkey Template

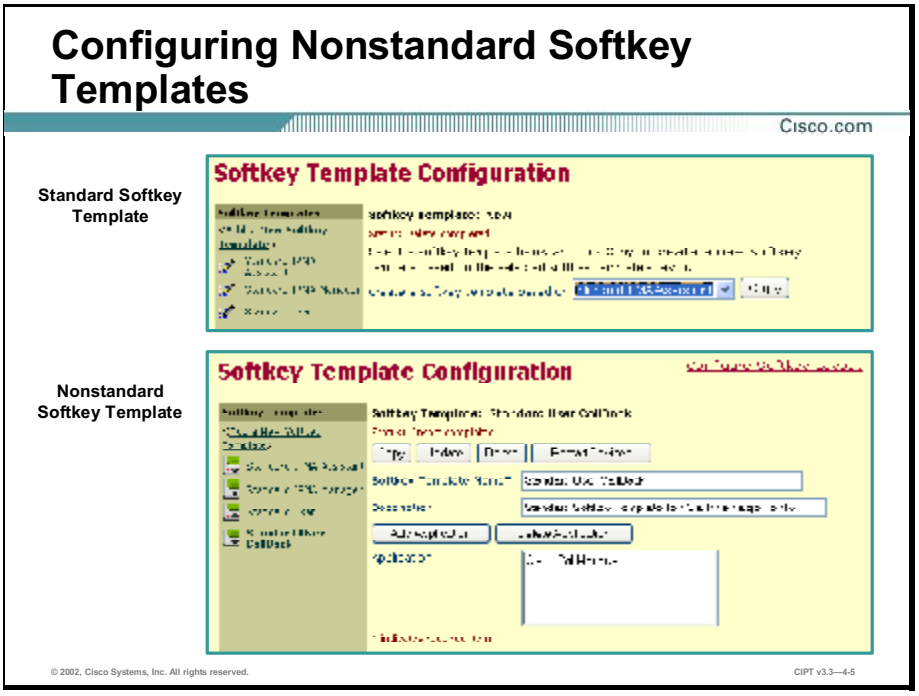
This topic provides an overview of softkey templates.

Configuring the softkey template allows you to manage the available applications on Cisco IP Phones (models 7960 and 7940). You can program these softkeys with many of the functions and features of Cisco CallManager (CCM).

The softkey template has three standard templates: the Standard IP Manager Assistant (IPMA), the Standard IPMA Manager, and the Standard User. You cannot delete or modify these standard templates. Applications that support softkeys can have one or more of the standard softkey templates associated with them.

Configuring Nonstandard Softkey Templates

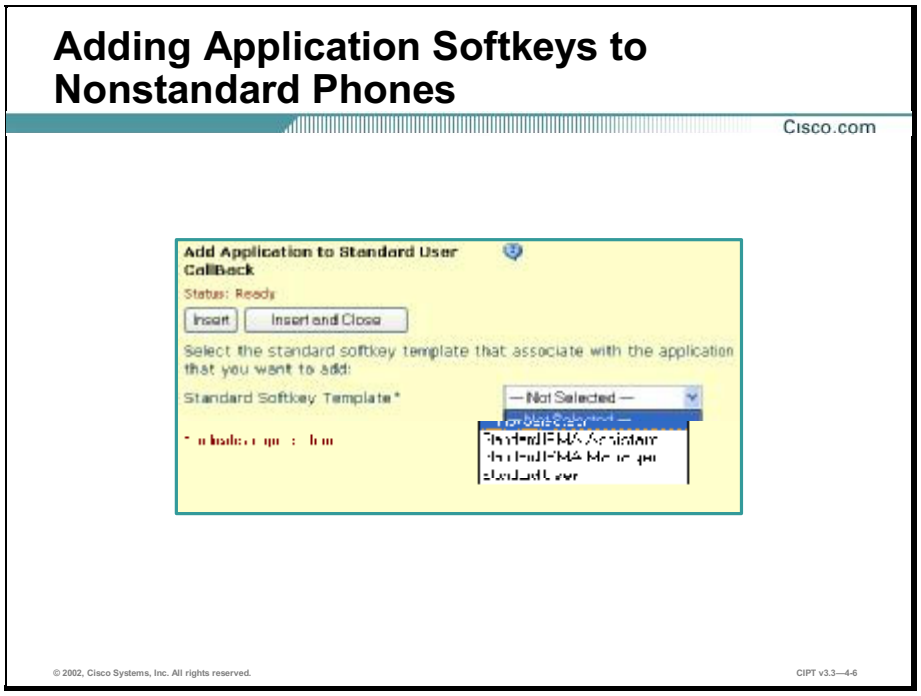
This topic describes configuring a nonstandard softkey template.



To create a nonstandard softkey template, you must first copy an existing standard template and make the modifications to this copy. Softkey templates are available by choosing Device Settings and then Softkey Templates from the Device menu. You then choose a template and click the **Copy** button to create a new template. The Softkey Template Configuration window will display the Softkey Template Name, Description, and Application associated with the softkeys. You must rename the template with a new descriptive name. After you have entered a unique name, click the **Insert** button. The standard template is copied, and the Softkey Template Configuration window refreshes to display the new softkey template.

Adding Application Softkeys to Nonstandard Softkey Templates

This topic describes the procedures for modifying a nonstandard softkey template.

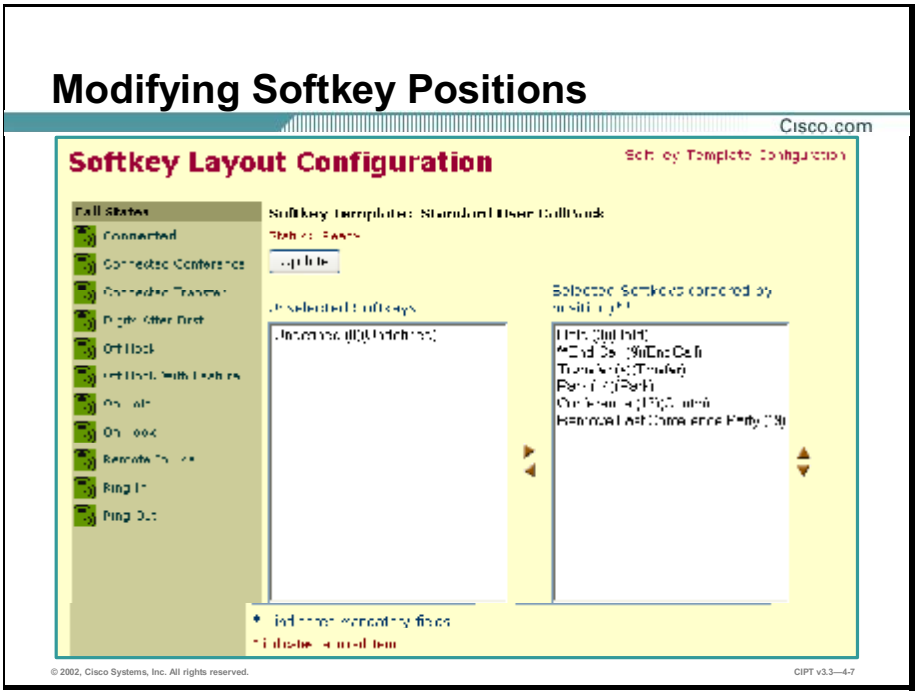


You can customize a nonstandard softkey template by modifying it. Standard softkey applications contain preconfigured softkeys for Cisco IP Phones. At this point, you can select the softkeys associated with the template.

You can add application softkeys to a nonstandard template by selecting the nonstandard template and clicking the **Add Application** button. When the Add Application window displays, you can select the Standard Softkey Template that you want to add to the nonstandard softkey template. Next, you click **Insert and Close**, and then click **Update**. This process will associate the standard template softkey configuration with the nonstandard template. If the number of softkeys exceeds 16, an error is displayed that states that you must remove some of the softkeys before continuing.

Modifying Softkey Positions

This topic describes the modification of softkey positions on Cisco IP Phones.

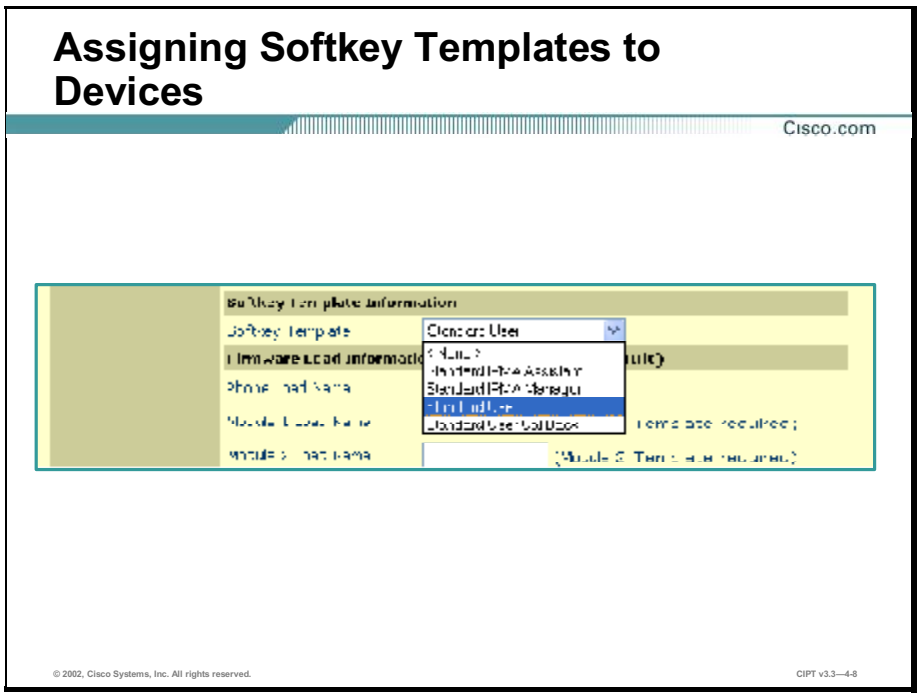


You can configure softkey positions in a nonstandard softkey template to customize the appearance of the softkeys on Cisco IP Phones. In the Softkey Templates field, select the template in which you want to modify the softkey positions. In the upper-right corner of the window, you will select the Configure Softkey Layout link. The Softkey Layout Configuration window displays Call States on the left and the Button Layout on the right. Select the softkeys that you want displayed. You then use the up and down arrows to rearrange the positions of the selected softkeys. To save the modifications that you have made to the template, click **Update**.

Note	After making modifications to softkey templates, you must restart the devices that are using the template.

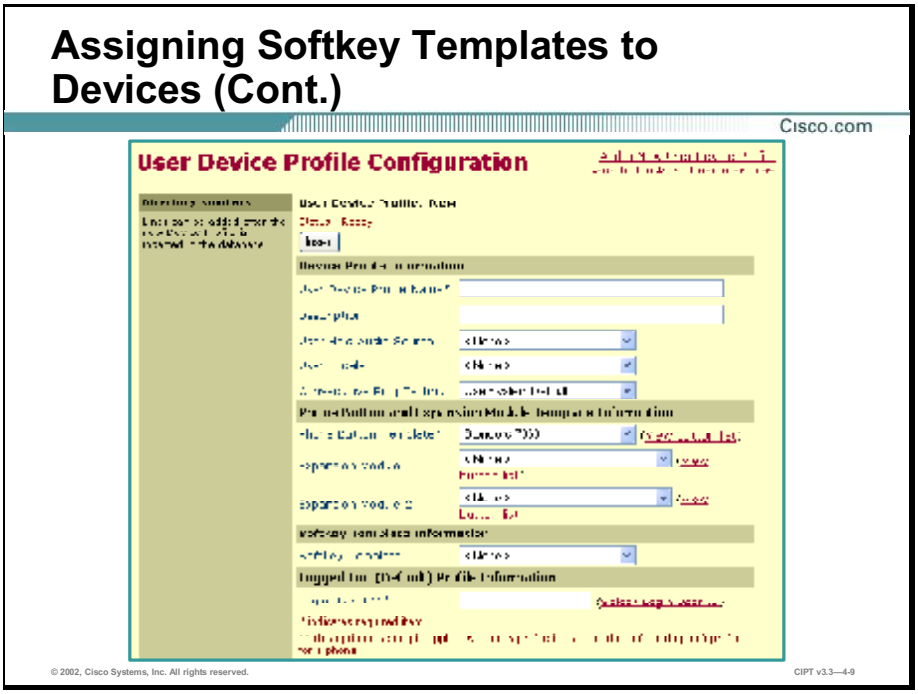
Assigning Softkey Templates to Devices

This topic describes assigning softkey templates to devices.



You can assign softkey templates to devices several ways. The template can be assigned in the device pool settings, on the device itself, or through a user profile.

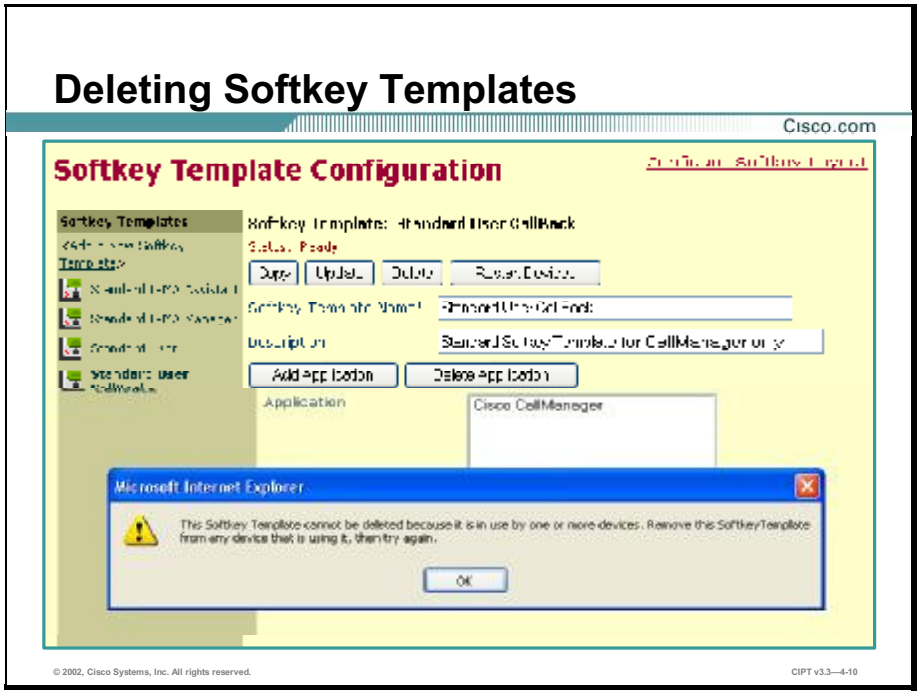
Assigning Softkey Templates to Devices (Cont.)



The User Device Profile Name and the Phone Button Template fields are required to configure a User Device Profile. You can customize the user device by adding a custom User Hold Audio Source.

Deleting Softkey Templates

This topic describes the process for deleting softkey templates.



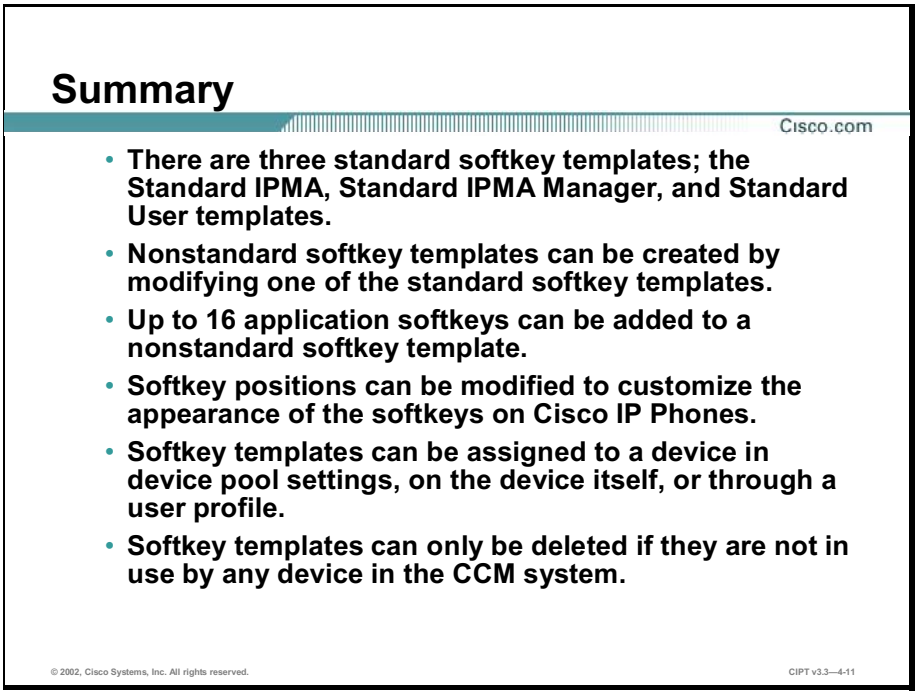
If you want to delete a softkey template, the template cannot be in use by any device in the CCM system. If the softkey template is assigned to a device pool, user profile, or Cisco IP Phone, you will receive an error message stating that the template is in use. You must remove the template from all devices before the template can be deleted.

To delete a softkey template, you select the template from within the softkey template by going to Device, and choosing Softkey Template from the main menu. You then choose the template that you want to delete and click **Delete**.

Note	Standard templates cannot be deleted. Only nonstandard templates can be deleted.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Features lesson

References

For additional information, refer to these resources:

- The Help files within Cisco CallManager Administration

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which two models of Cisco IP Phones can accept softkey templates? (Choose two.)

A) 7960

B) 7940

C) 7910

D) 7905

Q2) Where are softkey templates located?

A) Device Menu

B) Service Menu

C) Tools Menu

D) Plug-Ins Menu

Q3) How do you create a nonstandard softkey template?

A) copy the template from a standard template

B) create the template from the beginning

C) you cannot create a nonstandard template

D) add the template to the application

Q4) What must you do after making a modification to a softkey template?

A) restart the device

B) reboot the server

C) reboot the gateway

D) reboot the voice router

Q5) Which three of these areas can you use to assign a softkey template to a device? (Choose three.)

A) device pools

B) user profile

C) device

D) Template Configuration window

Q6) What can impact and prevent the deletion of a softkey template?

A) The template is associated with a device.

B) The nonstandard template is associated with a standard template.

C) The standard template is associated with a nonstandard template.

D) None of these.

Features

Overview

This lesson will teach you about the many features, such as call park, call pickup, callback, and IP Manager Assistant (IPMA) available on Cisco CallManager (CCM). Administrators need to understand the various options available for Cisco IP Phones to ensure that all of the desired features and functions stay properly configured. You will learn about these options, which will lead to solid planning and implementation of the IP Phone service.

Importance

This lesson benefits those students who want to learn the specific CCM features that will determine how a customer wants to deploy IP telephony. This lesson provides information on how to configure and subscribe to a Cisco IP Phone service.

Objectives

Upon completing this lesson, you will be able to:

- Configure the basic IP Phone features of CCM
- Configure the advanced IP Phone features of CCM
- Describe Cisco IPMA manager and assistant features
- Configure the shared line appearance
- Configure and subscribe to a Cisco IP Phone service

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Navigation within Cisco CallManager Administration
- Cisco IOS command-line basics

Outline

This lesson includes these topics:

- Overview
- Basic IP Phone Features
- Advanced IP Phone Features
- Cisco IP Manager Assistant
- Shared Line Appearance
- Cisco IP Phone Services
- Summary
- Lesson Review

Basic IP Phone Features

This topic discusses the basic features of IP Phones.

Cisco CallManager (CCM) extends supplementary and enhanced services, such as hold, transfer, forward, conference, multiple-line appearances, automatic-route selection, speed dial, last-number redial, and other features to Cisco IP Phones and gateways. These services are configured in the CCM database.

When you put a call on hold, the call remains active even though you and the other party cannot hear one another. You can answer other calls while a call is on hold. Engaging the hold feature generates music or a beeping tone. You should avoid putting a conference call on hold for this reason.

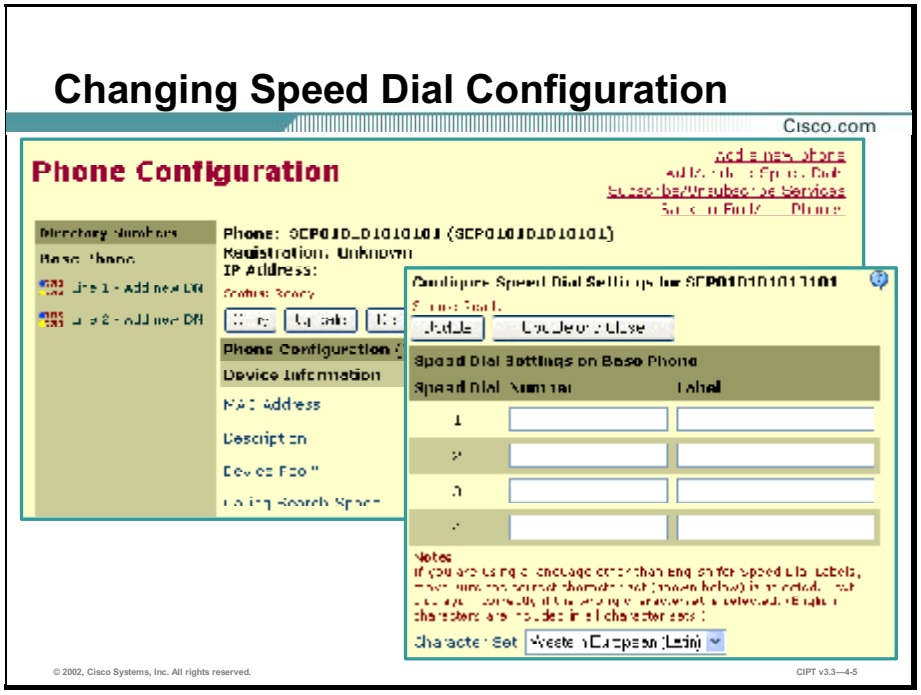
To redial the most recently dialed number, press the **Redial** softkey. Doing so without lifting the handset activates the speakerphone or headset. To redial a number from a line other than your primary line, select the desired line button and then press **Redial**.

Use call forwarding to:

- **Send incoming calls to another number:** Use call forwarding to send calls to another number where they can be answered (for example, if the user is going to be working in an alternate office).

- **Send incoming calls directly to voice mail:** Use call forwarding to send calls directly to the voice-mail system. The desk telephone will not ring when calls are routed to voice mail through the call-forwarding feature.

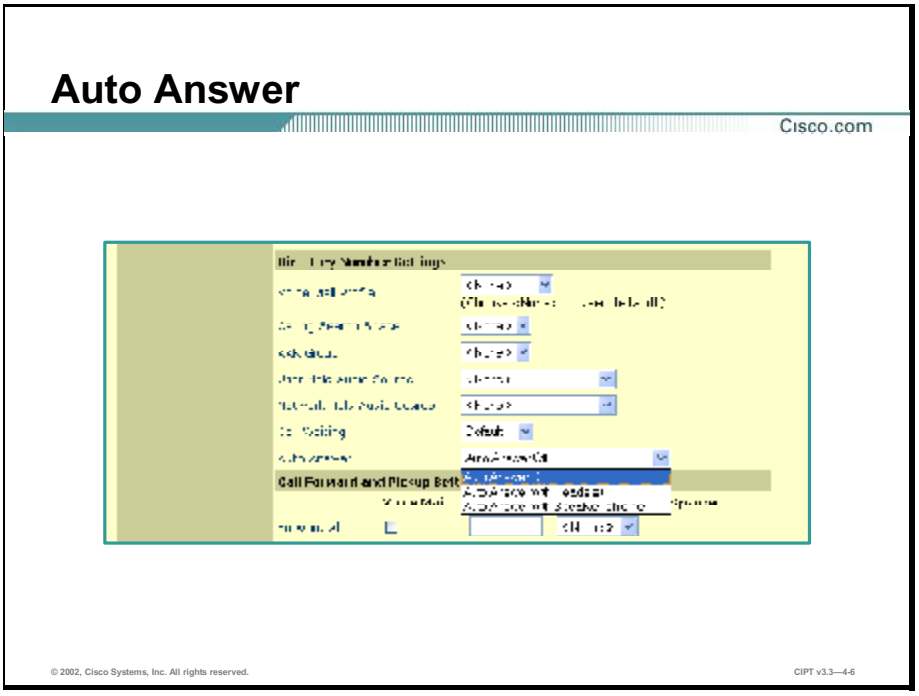
Reference	For more information on these and additional features go to: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/ip_7960/user_gd/iph60get.htm



CCM has the ability, through the administrator console, to select the devices and IP Phone settings needed to change and update the speed-dial configuration of the IP Phone.

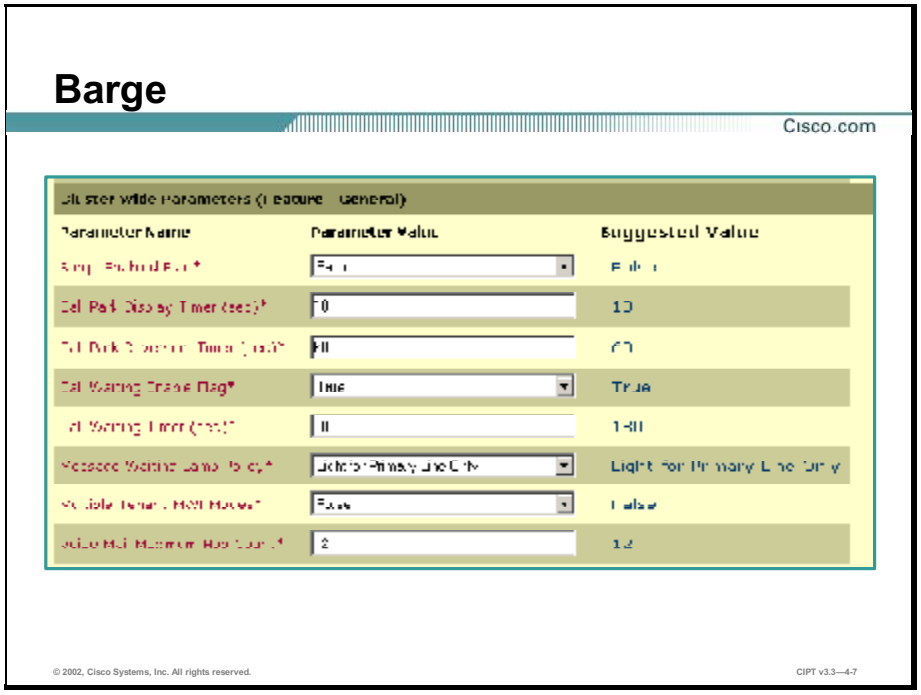
Advanced IP Phone Features

This topic discusses the advanced IP Phone features.



Auto Answer is a feature that causes the speakerphone or headset to go off hook automatically when an incoming call is received. You can program this feature on a telephone-by-telephone basis.

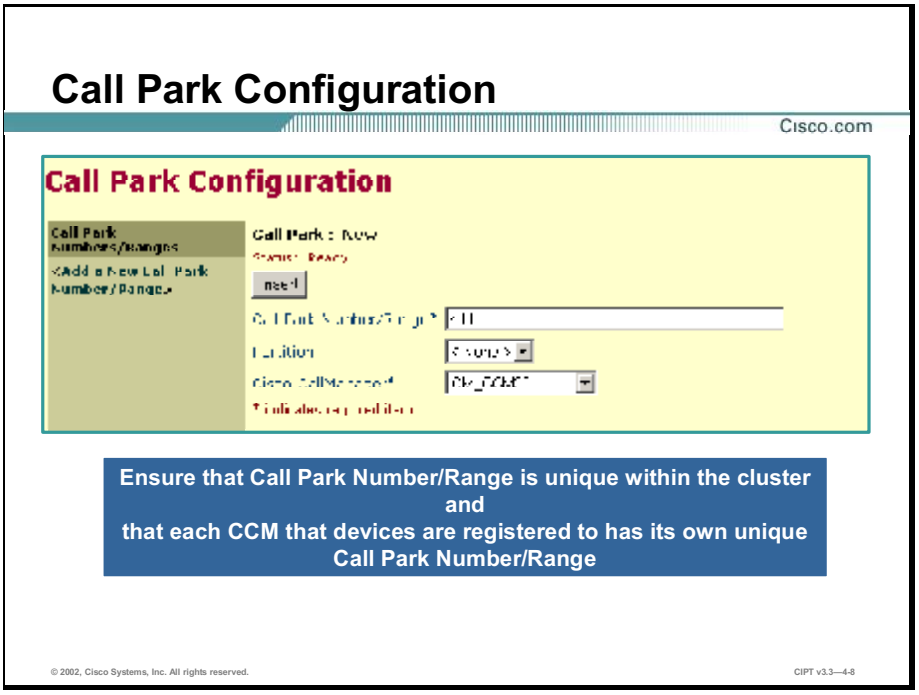
Choose the device that you want to enable, and then choose **Auto Answer** under the DN Settings. You can select Auto Answer Off, Auto Answer with Headset, or Auto Answer with Speakerphone.



Barge adds a user to a call that is already in progress. The barge feature supports shared lines only. You can press the Barge softkey to automatically add the user (initiator) to the shared-line call (target). The users currently on the call will receive a tone.

To initiate the BargeEnabled service parameter, choose **Service>Service Parameters** from the Cisco CallManager Administration window. When the service parameters configuration window displays, you can select a CCM server and the CCM service. The Cluster Wide Parameters lists the Barge Enabled Flag service parameter. You can change the parameter value to true to enable barge, and click the **Update** button.

The barge feature has some restrictions. The feature supports only Cisco IP Phone models 7940, 7960 and G.711 voice coding.



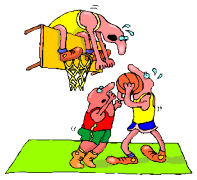
A call park number or range must be configured for each CCM in the cluster. When you invoke the call park feature, it is assigned a call park code (directory number [DN]). The user will use this code to pick up the call from another IP Phone on the same CCM that the original IP Phone is registered to. When you assign the call park DN or range to a partition, you can limit access to the call park feature based on the device calling search space. You should ensure that the call park number or range is unique throughout the CCM cluster.

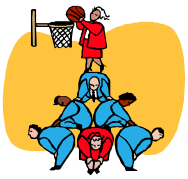
Example

The ABC Department Store with an overhead system is using the call park feature. A call for an employee on the floor comes in to a cashier desk. The cashier can park the call, announce the call park code on the overhead system and the employee on the floor can pick up the call using the call park code on a nearby telephone.

Call Pickup/Group Call Pickup

Cisco.com





Call pickup:

- **Allows a user to answer a call that is ringing on any telephone in their call pickup group**

Group call pickup:

- **Allows a user to answer a call that is ringing on any telephone, if they know the call pickup group associated with that call**

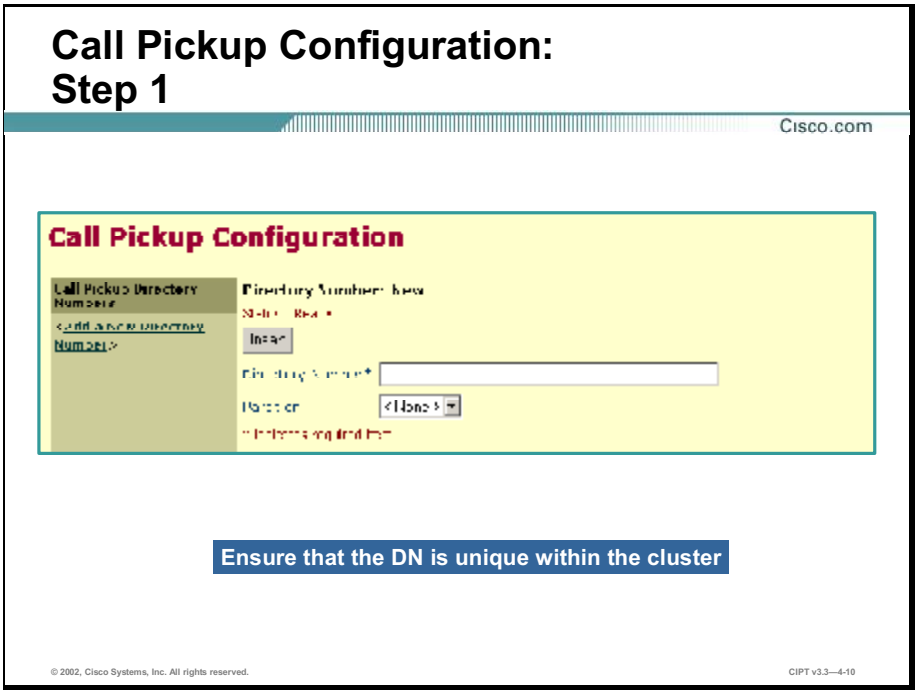
CIPT v3.3—4-9

Call groups enable users (who have been configured as part of a group) to answer calls that come in on a DN other than their own. The features that use these call groups are:

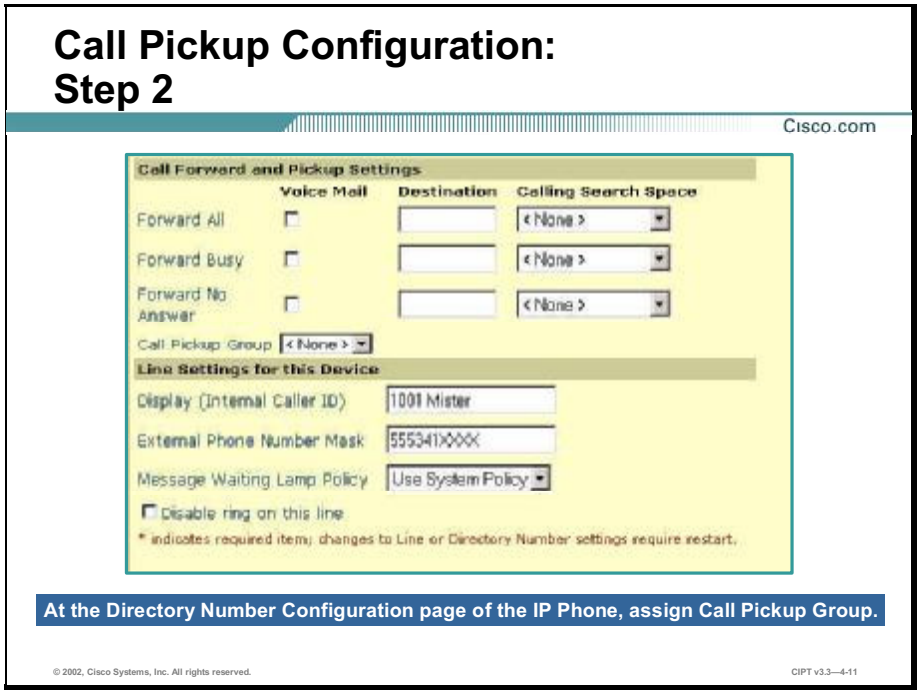
- **Call pickup:** Enables users to pick up incoming calls on any telephone within their own group. When the user presses the **Call Pickup** button or **PickUp** softkey, CCM automatically dials the appropriate call pickup group number.

- **Group call pickup:** Enables users to pick up incoming calls within their own group or in another group. Users press the **Group Call Pickup** button or **GpickUp** softkey and dial the appropriate group number for call pickup.

You use the same procedures to configure both of these features. The group call pickup numbers apply to lines or DNs.



The first step to configure a call pickup group is to create a DN. You can assign a partition to the DN that allows access to the DN of the pickup group that is based on the calling search space of the device. You need to ensure that the DN is unique within a cluster.

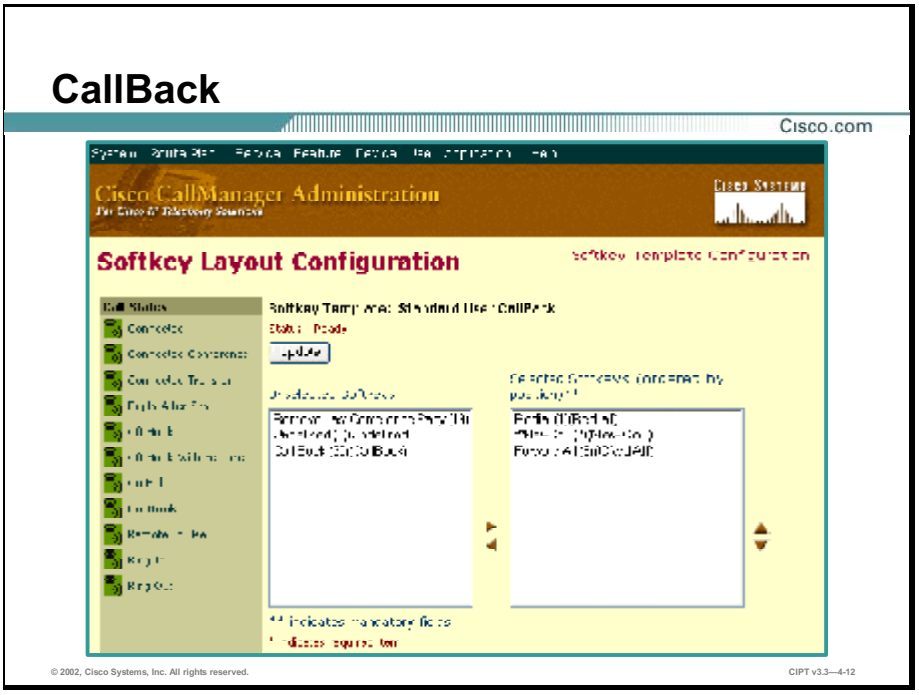


After configuring the DN, you assign the call pickup DN to a line or DN of an IP Phone. On the Directory Number Configuration page in Call Forward and Pickup Settings, choose the call pickup group DN from the menu. Repeat this for all other DNs that are to be assigned to the call pickup DN group.

The purpose of call pickup is to enable a group of users who are seated near each other to cover incoming calls as a group. Only Cisco IP Phones that are configured in a pickup group can use these features.

Example

The ABC Company sells two widgets, one geared to consumers and the other geared to enterprises. The sales staff is broken into two call pickup groups, 1234 for consumers and 5678 for enterprise. When a call comes into the bank of Cisco IP Phones in call pickup group 1234, any one of the IP Phones assigned to the consumers group can answer it by pressing the **PickUp** softkey. The calls destined for group 5678 can be answered by any of the IP Phones configured in the enterprise group. You can use distinctive ringer options to differentiate between the two groups of IP Phones.



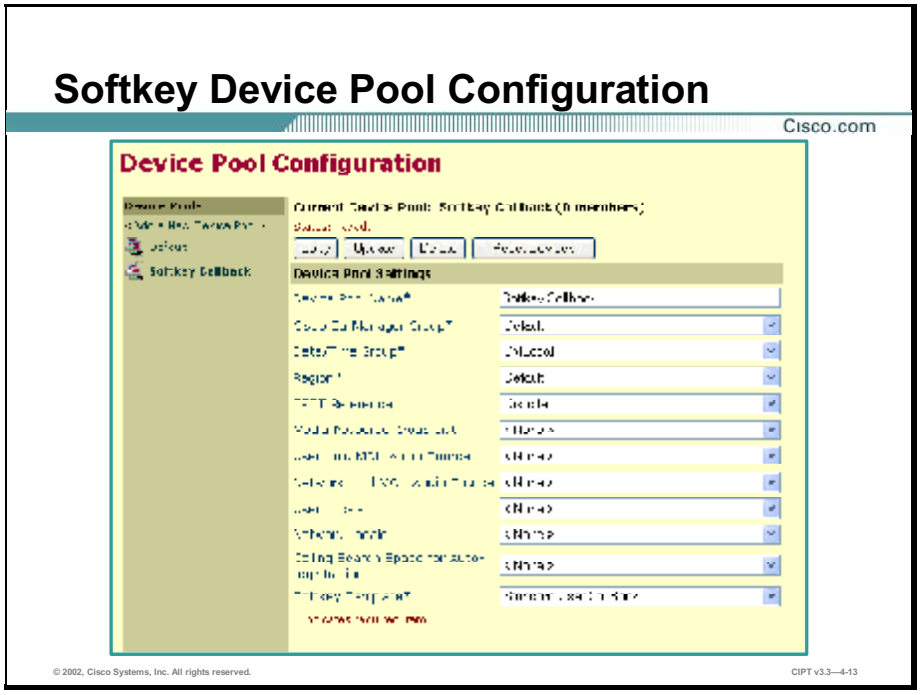
You can activate the callback feature for the following types of scenarios.

Example

IP Phone user A calls IP Phone user B in the same cluster. If IP Phone B is busy, or there is no answer, IP Phone user A activates the callback feature through CallBack softkey. When IP Phone B becomes available, IP Phone A will receive an audio alert and visual notification.

The telephone states that are supported are Busy, Call Forward Busy, or No Answer. The No Answer state could include Call Forward No Answer to a voice-mail system or to another extension. The calling IP Phone should be a model 7960 or 7940 that supports softkeys.

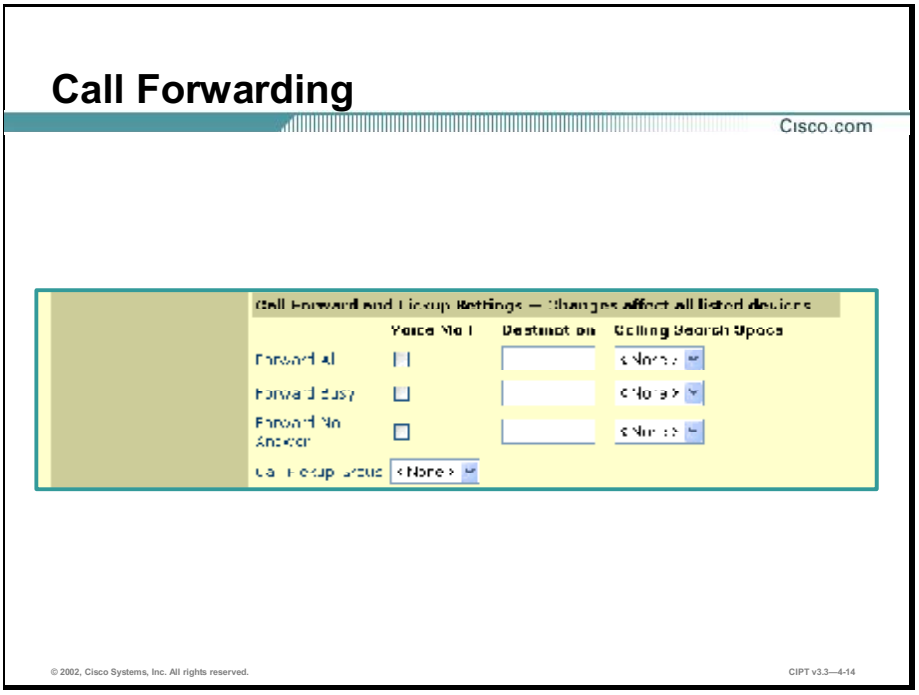
To configure the callback feature, choose the softkey template (Standard User Template), copy and insert the template, and name it Standard User Callback. Next, configure the softkey layout by choosing the On Hook call state and the callback option. Then, choose Ring Out, include callback (by making sure that it is at the top of the list), and click **Update.**



You can update the window and choose the **Device Pool** menu to set all users. From the Softkey Template menu, choose the **Standard User CallBack** template and set it to Default if you want to enable callback for all users. Click the **Update** button. Check **Cisco Extended Functions and Update** under the Service Activation menu.

To ensure proper functionality, make certain that these applications are configured and running properly:

- **CCM:** There should be at least one CCM running in the cluster. (It does not have to be running on the same server.)
- **Cisco computer telephony integration (CTI) Manager:** There should be at least one Cisco CTI Manager running in the cluster. (It does not have to be running on the same server.)
- **Cisco Database Layer Monitor:** There should be one Cisco Database Layer Monitor running on the same server as Cisco Extended Functions.
- **Cisco Real-Time Information Server (RIS) Data collector:** There should be one Cisco (RIS) Data collector running on the same server as Cisco Extended Functions.



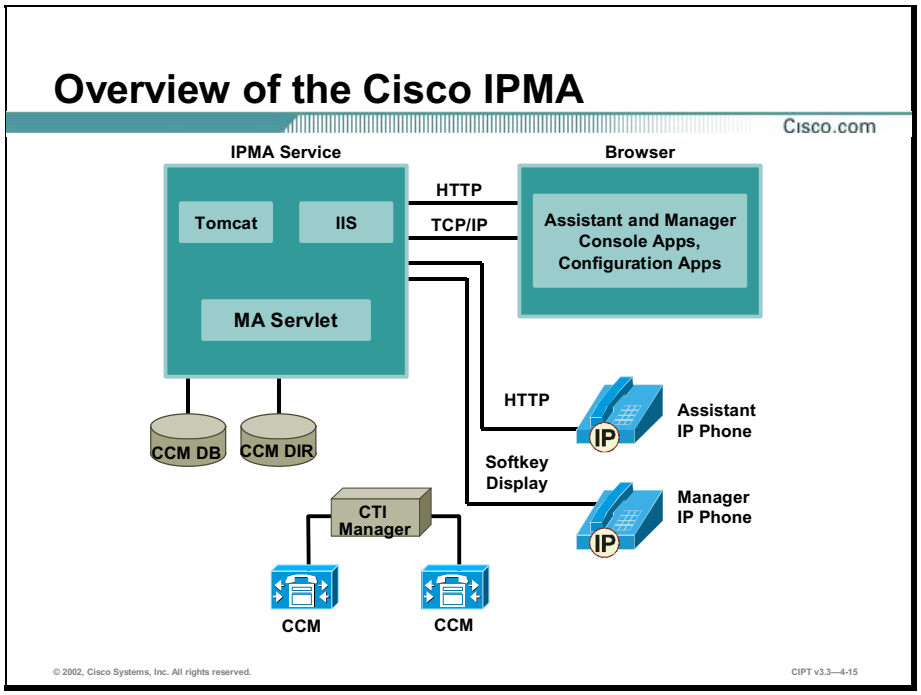
Call Forward allows a user to configure a Cisco IP Phone, so that all calls destined for that IP Phone ring at another telephone. There are three types of call forward:

- **Forward All:** Forwards all calls
- **Forward Busy:** Forwards calls only when the line is in use
- **Forward No Answer:** Forwards calls when the telephone is not answered after the configured number of rings

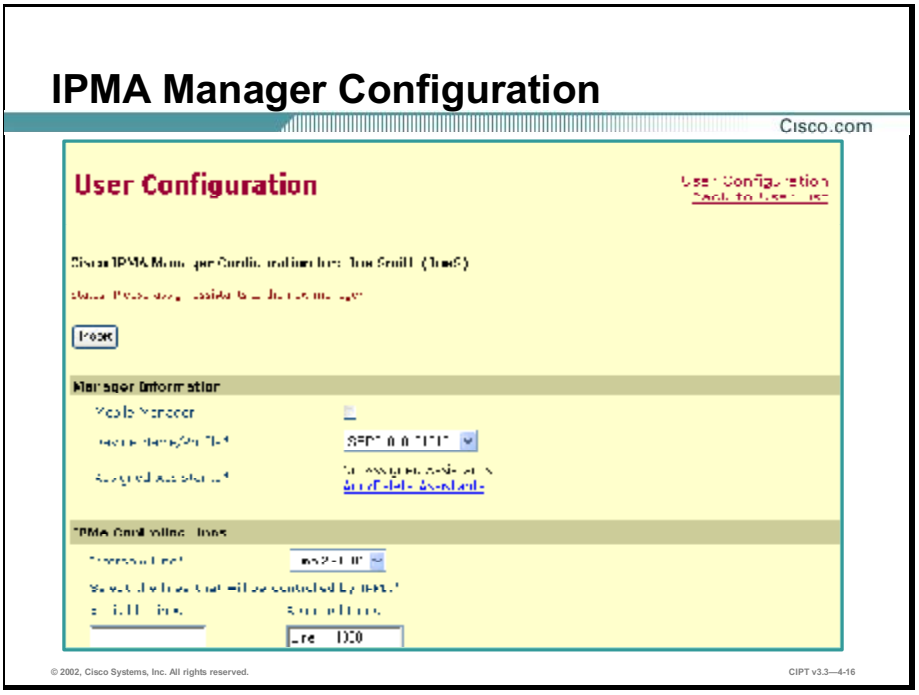
You can configure call waiting in the Directory Number Configuration window in Cisco CallManager Administration.

Cisco IP Manager Assistant

This topics includes an overview of the Cisco IP Manager Assistant (IPMA).



The Cisco IPMA is a feature that allows company managers and assistants to effectively work together. Assistants can have proxy lines set up on their devices to answer and manage calls for the manager. This service intercepts calls made to the managers and routes them to the assistant or to preconfigured targets based on preconfigured call filters.



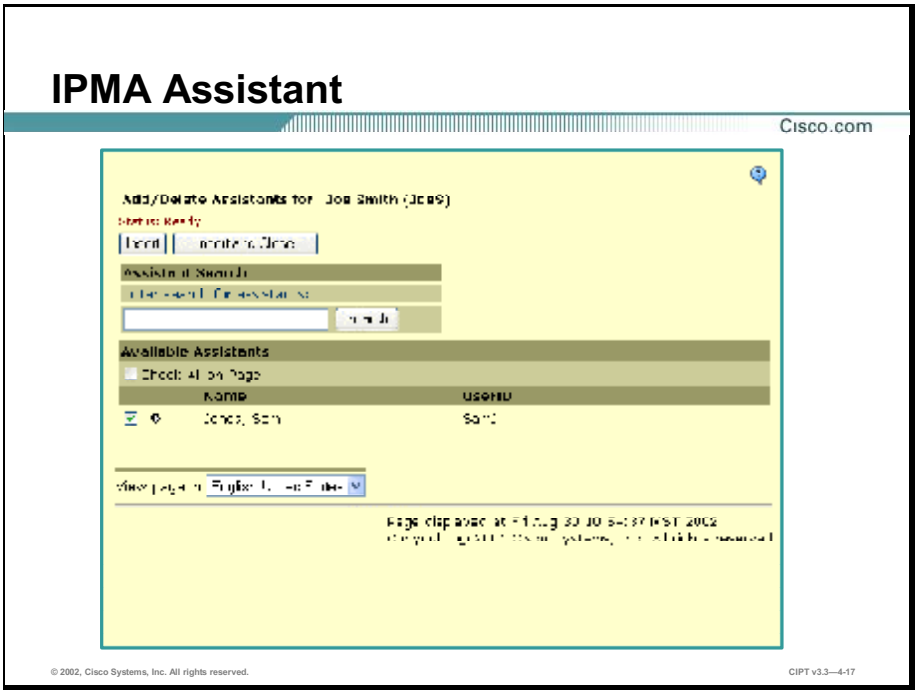
A manager is defined as the user whose incoming calls are intercepted by the routing service and handled by the assistant. These features are under the control of the manager in the process of the call routing:

- **Intercom:** The ability to place and receive intercom calls to, and from, the assistant are part of the intercom capabilities.
- **Assistant Selection:** The ability to select from a pool of available assistants. This is an IP Phone service.
- **Assistant Backup:** The ability for a manager to receive backup from an available assistant.
- **Call Filtering:** The ability to filter calls based on who is calling. Calls can be set up to automatically route to an assistant. Filtering, and the selection of filter modes, can be done through the IP Phone service or the Cisco IPMA Manager Configuration page on the desktop.
- **Assistant Watch:** This gives the manager the ability to see the calls that are being handled by the assistant on behalf of the manager. This ability can be invoked from an application softkey.
- **Do Not Disturb (DND):** This dynamically disables the ringer on the IP Phone but allows calls to be presented to the device to be answered if the user desires. The state of the feature is displayed in the Phone Display Status window.
- **Send All Calls:** Dynamically routes all calls to the Send All Calls assistant or target.

- **Immediate Divert:** Calls that are ringing at the manager IP Phone can be diverted with a click of an application softkey.

- **Intercept Call:** Calls ringing at the assistant IP Phone can be intercepted with a click of an application softkey.

- **Transfer to Voice Mail:** Calls to the manager IP Phone can be immediately sent to voice mail with a click of an application softkey.

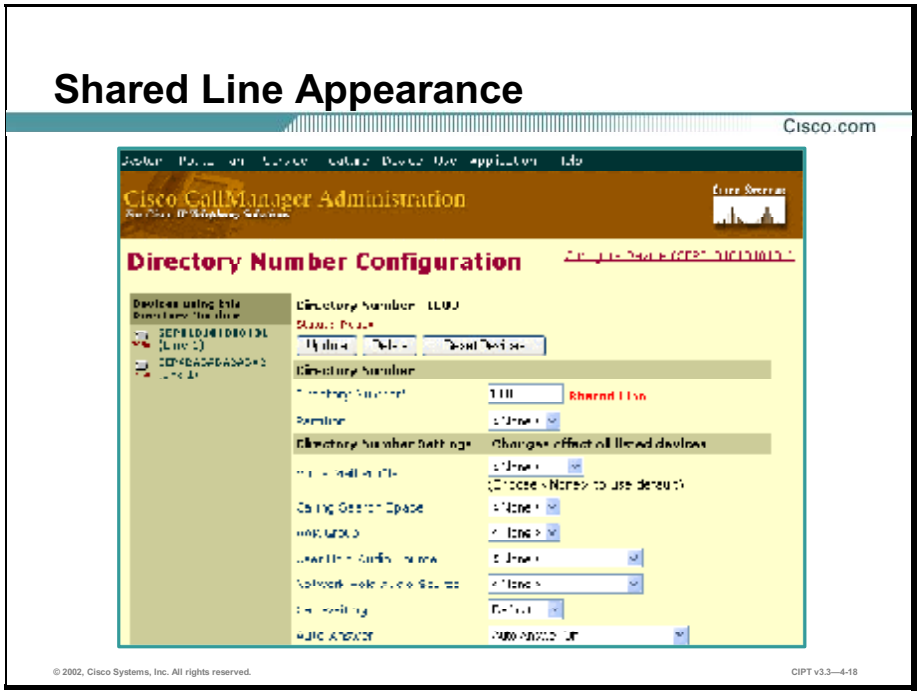


An assistant is defined as the user that handles calls on behalf of the manager. The features that are under the control of the assistant in the process of the handling the calls that are being routed to the assistant include:

- **Intercom:** The ability to place and receive intercom calls to, and from, the assistant, as part of the intercom capabilities.
- **Distinctive ringing:** You can configure a distinctive, audible ringing tone for personal calls versus calls for the manager and outside calls.
- **Call handling from the desktop:** You can view the state of the manager to help the assistant better handle the calls. The assistant can handle calls for up to five managers at a time through the Assistant console.
- **Keyboard shortcut accessibility:** Keyboard shortcuts are fully accessable through the Assistant console. These shorcuts are completely configurable through the Assistant Preference page.

Shared Line Appearance

This topic discusses the shared line appearance feature.



CCM considers a DN on more than one device in the same partition as a shared line appearance. In a shared line appearance, you can set up a shared line; for example, a DN appears on line 1 of a manager telephone and also on line 2 of an assistant telephone. Another example of a shared line would be a single incoming 800 number that is set up to appear as line 2 on every help desk telephone in an office.

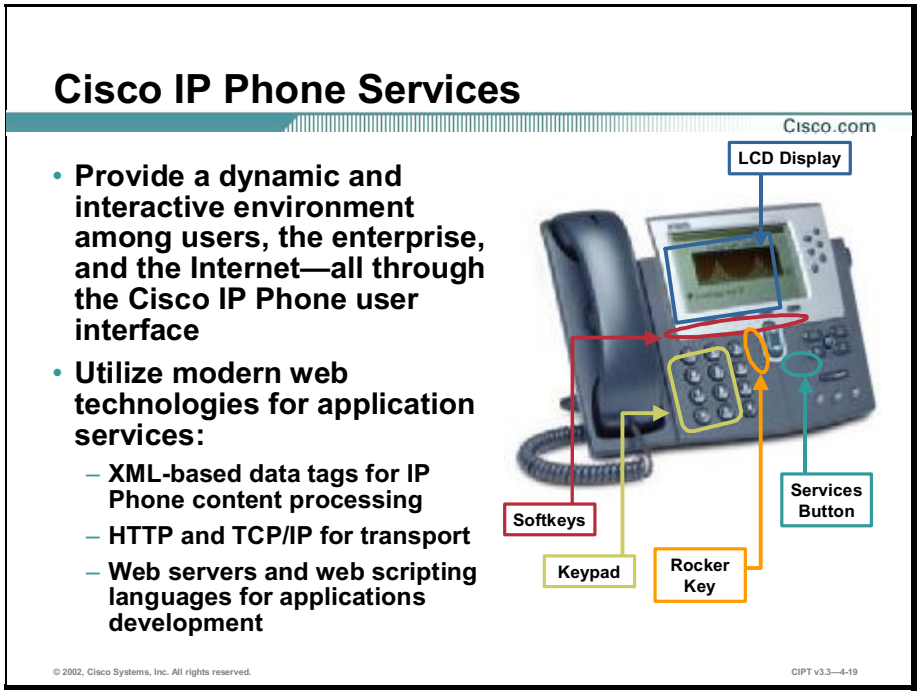
These suggestions may be helpful when using shared line appearances with CCM:

- You can create a shared line appearance by assigning the same DN and partition to different lines on different devices.
- If other devices share a line, the words Shared Line display in red next to the DN in the Configure a Line Number window in Cisco CallManager Administration.
- If you change the Calling Search Space, Call Waiting, or Call Forward and Pickup settings on any device that uses the shared line, the changes are applied to all of the devices that use that shared line.
- To stop sharing a line appearance on a device, you can change the DN or partition number for the line and update the device. (Delete removes the DN on the current device only. The deletion does not affect the other devices.)

- Do not use shared line appearances on any IP Phone that will be used with the Attendant console.
- Do not use shared line appearances on any Cisco IP Phone 7960 that requires the Auto Answer capability.

Cisco IP Phone Services

This topic discusses the Cisco IP Phone Services feature available in CCM.



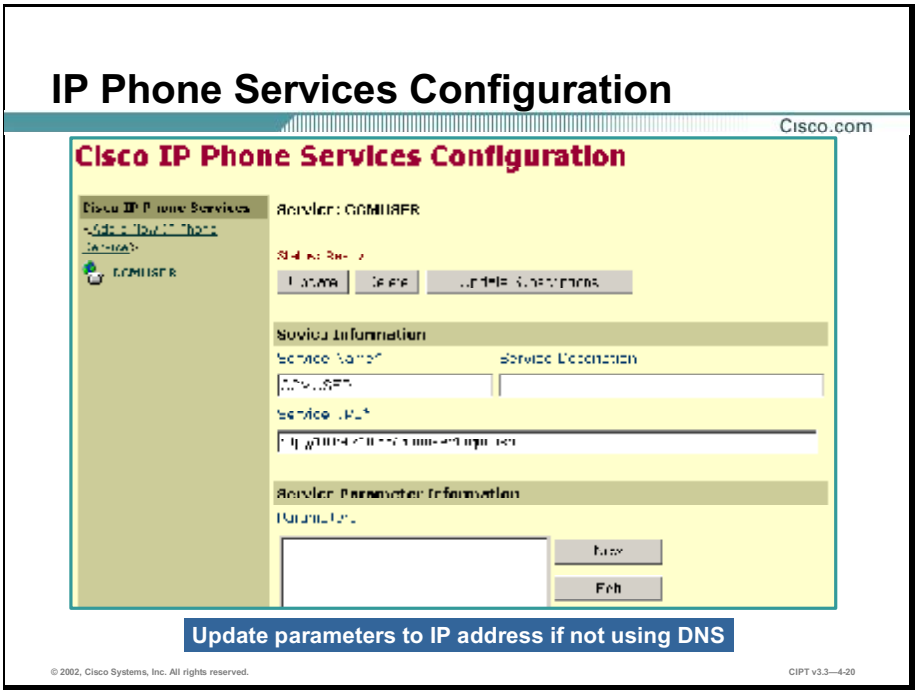
Cisco IP Phone services are XML applications that enable the display of interactive content with text and graphics on Cisco IP Phone models 7960 and 7940. You can create customized Cisco IP Phone applications for your site using the Cisco IP Phone Services Software Developer's Kit (Cisco XML SDK).

Note The SDK is available to registered and unregistered users at: http://www.cisco.com/warp/public/570/avvid/voice_ip/cm_xml/cm_xmldown.html

Cisco IP Phone Services display content on the IP Phone 133 X 65 liquid crystal display (LCD). You can press the Services button to display the list of the services that the IP Phone has subscribed to. The user can navigate the services and provide input via:

- Softkeys
- Rocker key (to scroll up and down)
- Keypad

Note For information about the Cisco XML SDK, refer to these links:
http://www.cisco.com/go/developersupport/
http://www.cisco.com/warp/public/cc/pd/unco/ippps/

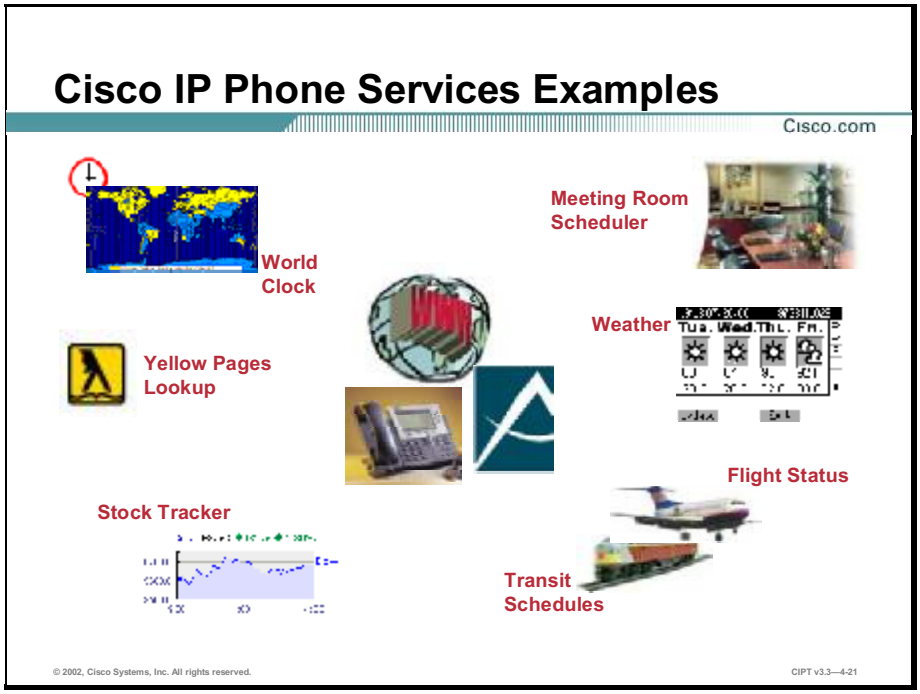


You can add services to CCM by using the Cisco IP Phone Services Configuration page. After services are configured in Cisco CallManager Administration, users or administrators can subscribe to these services for the devices that they have access to.

This list describes the information that must be configured for each service:

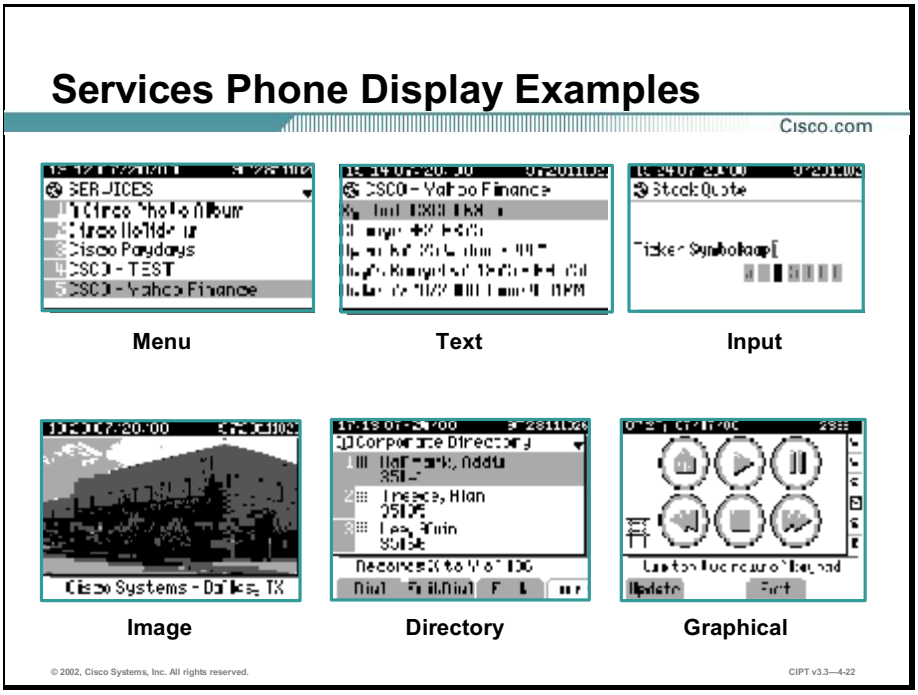
- URL of the server that provides the content.
- Service name and description—this helps users decide whether they want to subscribe to the service.
- A list of parameters that are appended to the URL when it is sent to the server (Optional).

Parameters serve to customize a service. Some examples of parameters include stock ticker symbols, city names, zip codes, or user IDs.



The services illustrated in the figure are listed here:

- Weather check
- Yellow pages telephone number lookup
- Mass transit schedules
- Stock ticker check
- Flight status
- Meeting room scheduler
- World Clock

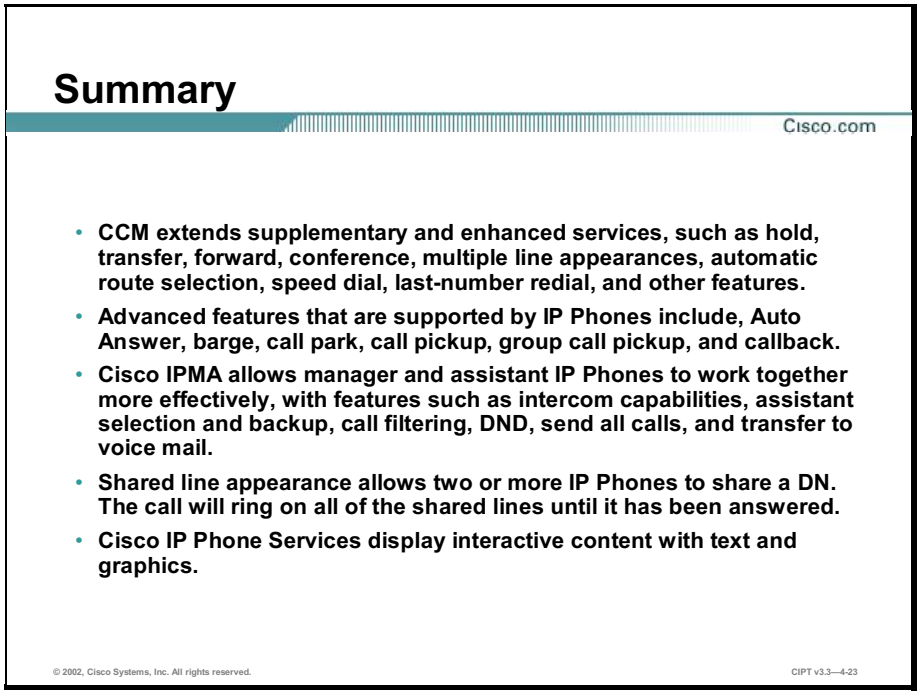


This list describes the Cisco IP Phone displays in this figure:

- **Menu:** A menu enables the user to scroll through the list of menu items and make choices.
- **Text:** The text from a web page can be delivered for the user to view.
- **Input:** Input enables the user to enter information using the keypad.
- **Graphical:** The services can display graphics, as well as text.
- **Image:** The services can deliver images in black, white, and shades of gray. Color images will be available when Cisco releases a Cisco IP Phone with a color display.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Cisco IP Telephony Users lesson

References

For additional information, refer to these resources:

- The Help files within Cisco CallManager Administration
- Additional lists and configuration of the features are available on the Cisco web site: www.cisco.com

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of these provide the configured call park range or DN?

A) publisher server

B) primary CCM

C) backup CCM

D) none of the above

Q2) Who is responsible for configuring all of the Cisco IP Phone services available?

A) end users

B) PBX administrators

C) local CO technician

D) CCM administrator

Q3) Which of these features forwards a call to voice mail?

A) call forward

B) redial

C) barge

D) hold

Q4) Which of these features is NOT an option with shared line appearances?

A) DND

B) auto answer

C) call forward

D) redial

Q5) Which three of these features are configurable for the manager IP Phone in the IPMA configuration? (Choose three.)

A) DND

B) SAC

C) call filtering

D) call handling from the desktop

Cisco IP Telephony Users

Overview

This lesson teaches you how to use Cisco CallManager (CCM) to configure users and associate devices (telephones, Cisco SoftPhones, device profiles) to users. You will learn how to customize user access.

Importance

Adding users and associating users to devices allow for directory searches from a Cisco IP Phone 7940 or 7960, WebAttendant, and billing association. In addition, allowing users to configure IP Phone options increases their productivity.

Objectives

Upon completing this lesson, you will be able to:

- Describe CCM user management
- Use Cisco CallManager Administration to add and associate users to a device
- Activate the Call Forward option
- Configure the speed dial option
- Subscribe to Cisco IP Phone services
- Configure personal address books
- Configure the Message Waiting Lamp policy
- Configure device locale
- Configure web page locale

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Navigation in Cisco CallManager Administration

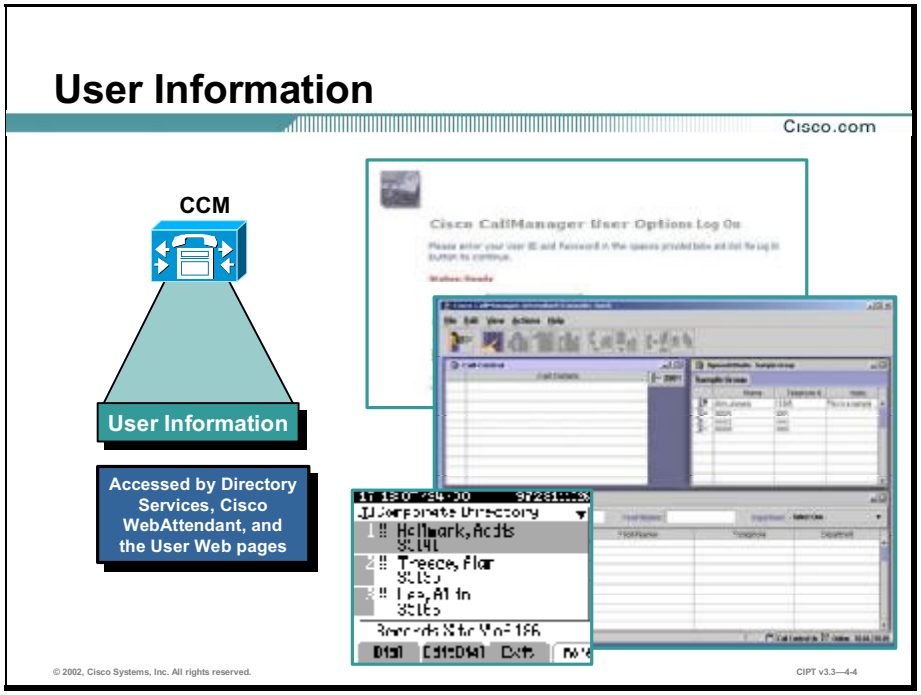
Outline

This lesson includes these topics:

- Overview
- Adding a User
- User Log On and Device Selection
- Call Forward
- Speed Dials
- Cisco IP Phone Services Subscription
- Personal Address Book
- Message Waiting Lamp Policy
- Personalize Device Locale
- Personalize CCM User Options Web Page Locale
- Summary
- Lesson Review

Adding a User

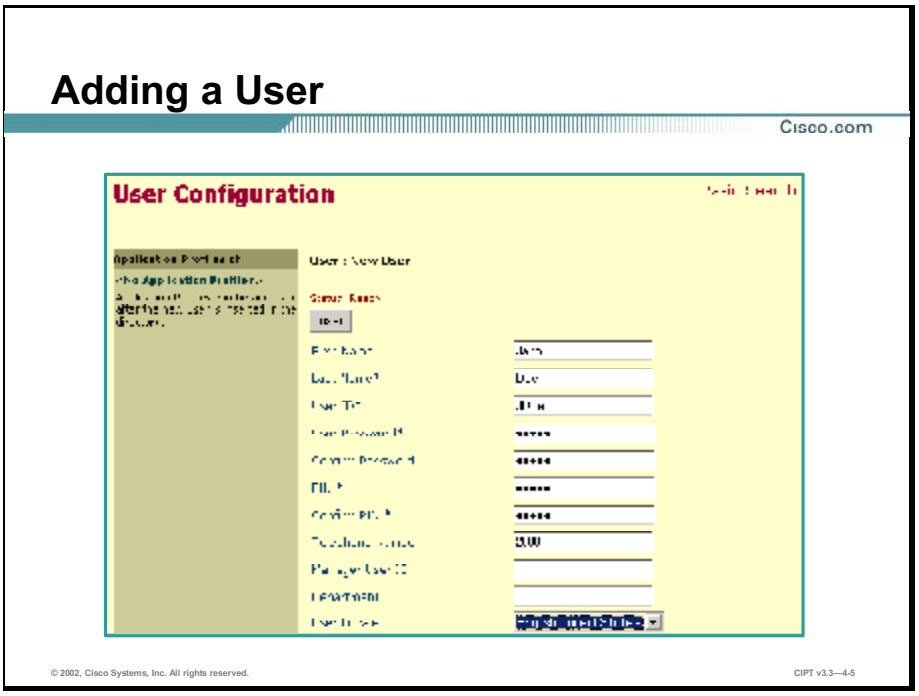
This topic discusses how to add a user and associate a user to a device.



The User area in Cisco CallManager Administration allows you to display and maintain information regarding Cisco CallManager (CCM) users. Generally, completing user information is optional; the devices will function whether or not you complete the user information. However, the user information you enter is accessed by Directory Services, Cisco WebAttendant, and the Cisco IP Phone Configuration pages. If you want to provide these features to your users, you must complete the information in the User area for all users, including the directory numbers(DNs). You can use user information for resources such as conference rooms, other areas with telephones, or Cisco WebAttendant.

After you associate users with a device, and the name and DN of that device, users can change their speed dial and forwarding numbers on the web.

The Global Directory for CCM (release 3.0 and later) contains every user in a CCM directory. CCM uses Lightweight Directory Access Protocol (LDAP) to interface with a directory containing user information. The Global Directory is an embedded directory supplied with CCM, and its primary purpose is to maintain the associations between users and devices. You can access the Global Directory by using either a basic or an advanced user search.



The following is an example of adding a user to the CCM directory database using Cisco CallManager Administration.

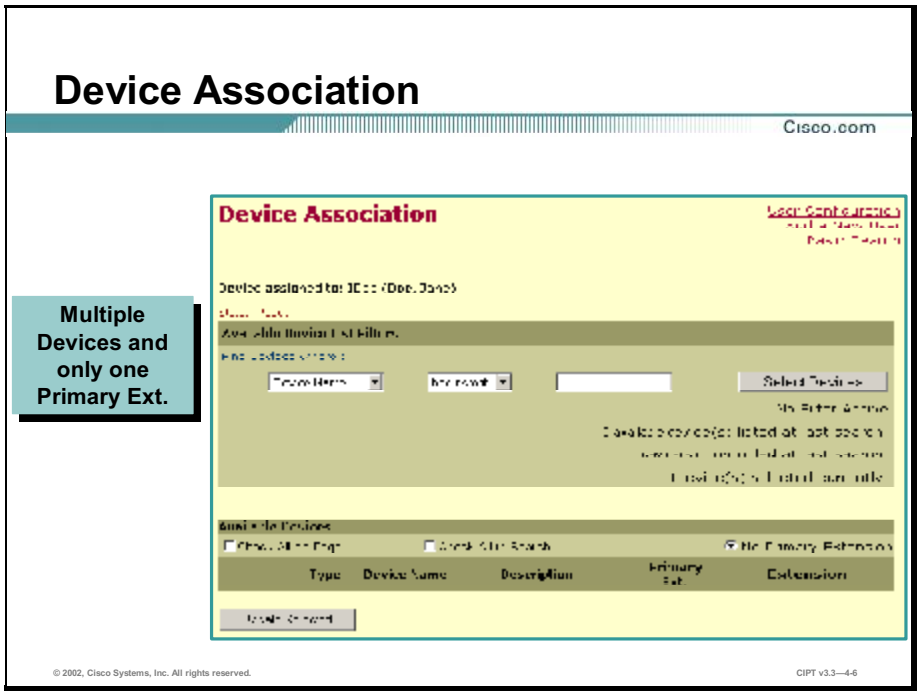
Before adding a user, gather the following user information:

- First Name
- Last Name
- User ID
- Telephone Number or DN
- Manager User ID
- Department

If the user is going to access the Cisco SoftPhone application, Auto Attendant, or any other computer telephony integration (CTI) application, check the Enable CTI Application Use check box.

When first setting up a user, assign a simple password (at least 4 characters) and a personal identification number (PIN), which must be at least 5 digits, for the user to use on the initial login. The user can then change both the initial password and PIN from the Cisco CallManager User Options page.

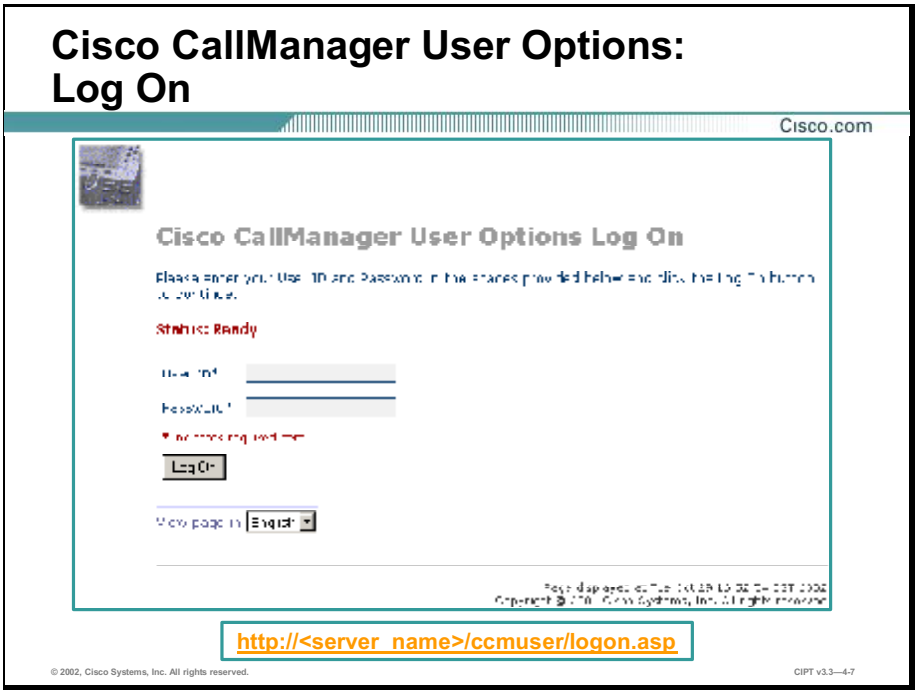
After the directory information is added, you can associate the user with a device or devices.



You can associate a user to many devices; however, only one of the devices can be the primary extension for that user. You can associate the user to multiple telephone devices and/or a Cisco SoftPhone device.

User Log On and Device Selection

This topic discusses how the user can log on and select a device from the Cisco CallManager User Options web page.

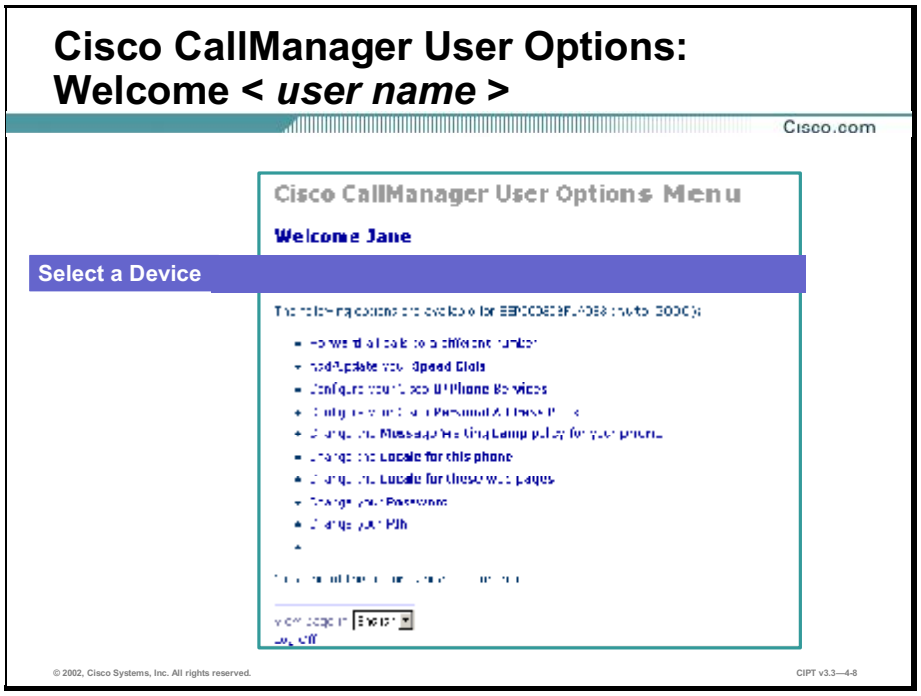


To open the Cisco CallManager User Options web page, enter this URL:

http://<server_name>/ccmuser/Logon.asp

At the Cisco CallManager User Options page, the user enters the User ID and Password. If this is the first time the user is logging on, the user should obtain the URL, User ID, and Password from the administrator.

From any page within the Cisco CallManager User Options, the user can change the language of the page by selecting the language (locale) from the View page in the menu.



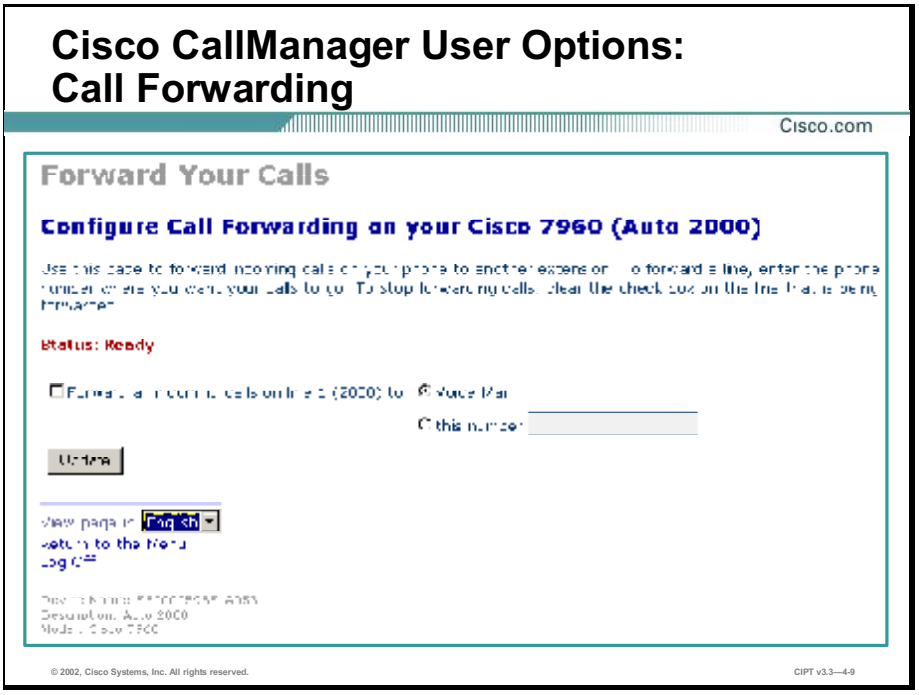
After logging on, the user can select an associated device to configure. The user can customize multiple associated devices by choosing more than one device.

Example

By providing a web location for users to customize IP Phone settings, users can be more productive in their work environment. For example, if a user is not going to be in the office to receive an important call, they can access the Cisco CallManager User Option page from home and configure call options. After accessing the Cisco CallManager User Options page, the user can configure their IP Phone to forward calls to their cellular telephone or any other DN, depending on the calling search space configured for Call Forward All. By using the Call Forward All option, the user will receive that important call.

Call Forward

This topic discusses how the user can forward all calls on an associated device by using the Cisco CallManager User Options page.



A user can forward all incoming calls on line 1 of a device to either voice mail or another number.

If the user is forwarding calls to another number, the calling search space of the device using Call Forward All will restrict which numbers will be valid. Also, if the number is forwarded off-net, the user must enter the number as if dialing from that telephone device.

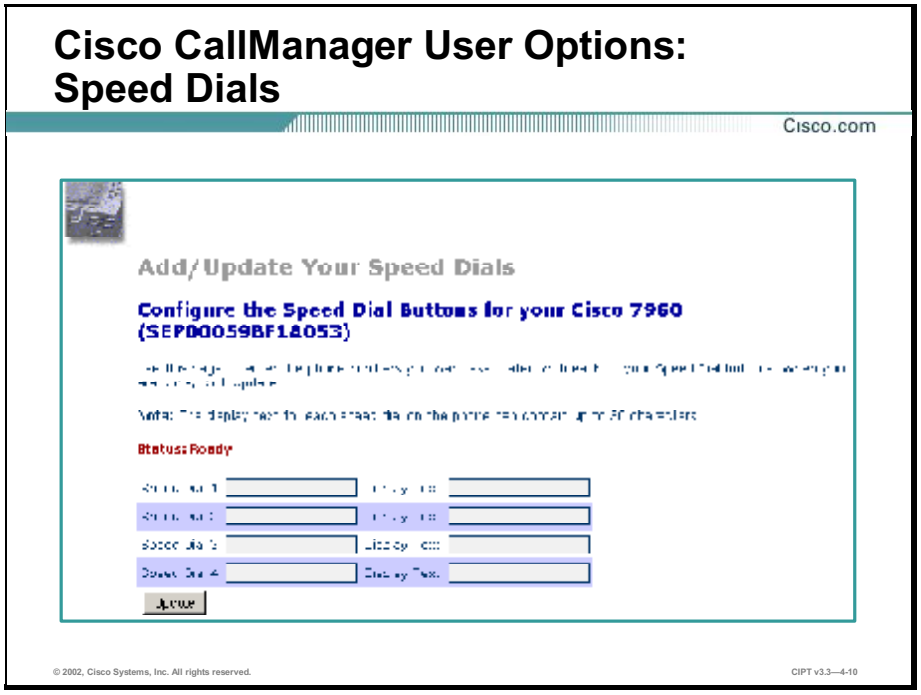
The Call Forward All feature can be very helpful to users. However, the Call Forward All feature can allow users to make personal long distance calls at company expense. To restrict access of the Call Forward All feature, apply a calling search space on the Directory Number Configuration page in the Call Forward All setting.

Example

A user may want to work from home and wants all calls to the office telephone to forward to the home number. If the user dials “92145551212” from the office to call home, the user must enter “92145551212” as the forwarding number.

Speed Dials

This topic discusses how the user can configure speed dial settings for a device using the Cisco CallManger User Options page.



Depending on the device, the number of speed dials is limited based on the Phone Button template. A user can enter numbers and text that allow for one button dialing. The speed dial number that is entered must follow the dialing rules of the Cisco IP telephony solution.

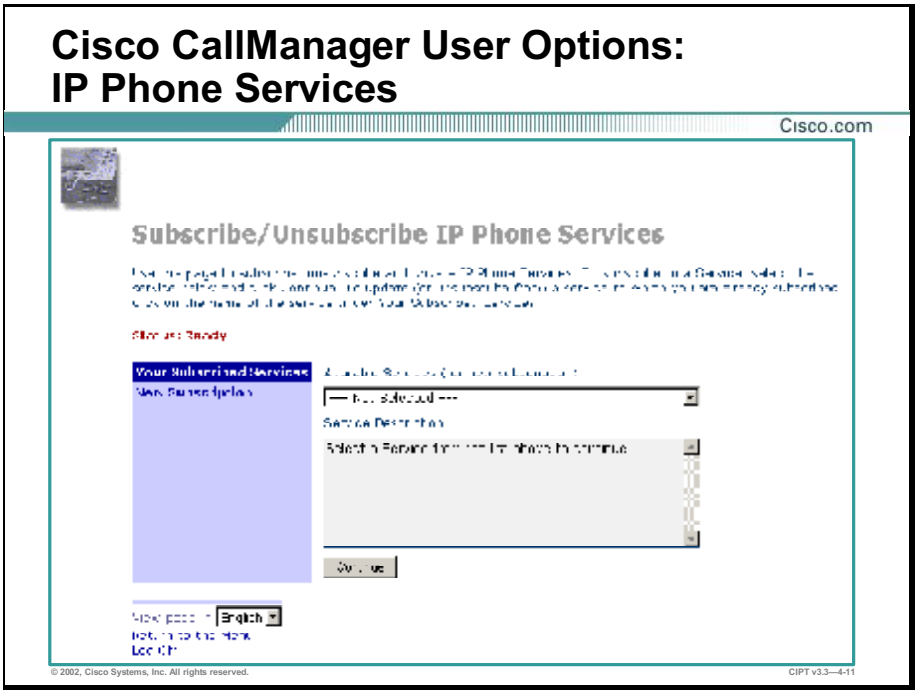
When programming speed dial, a user must enter the number that is used when all of the digits are entered. If the number 9 is dialed before entering the home telephone number, the 9 must be part of the speed dial number that a user enters.

Example

If an access code, such as 1234, then 9, is required, the user must enter the speed dial using these numbers. For example, if the home telephone number is 2145551212, the speed dial number must be “123492145551212.”

Cisco IP Phone Services Subscription

This topic discusses how the user can subscribe to available Cisco IP Phone services within a Cisco IP telephony solution.



The user can use the Subscribe/Unsubscribe IP Phone Services page in CallManager User Options to subscribe or unsubscribe to any of the Cisco IP Phone services that you have configured.

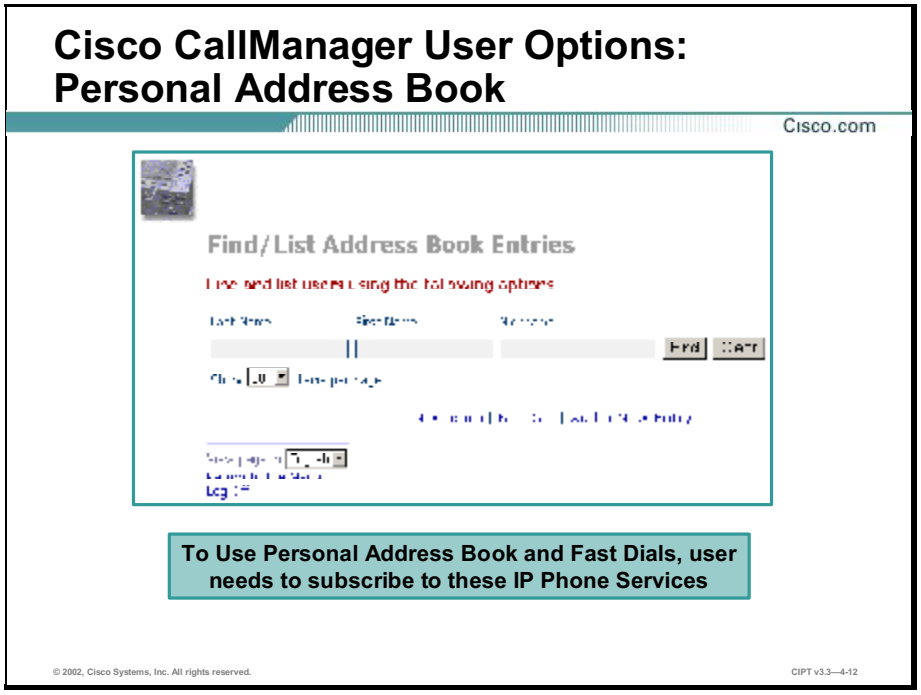
You can configure other services for user subscription. For example, you can configure any information on the web and some applications as well. Users can subscribe to services that store telephone numbers, meeting room availability, traffic reports, and more.

Example

If you have configured a service that looks up the stock price of a company, the user can subscribe to that service from the Subscribe/Unsubscribe IP Phone Services page in CallManager User Options. To view the stock price of a company, the user can press the services button on a Cisco IP Phone model 7960 or 7940 and view the stock price on the IP Phone liquid crystal display (LCD).

Personal Address Book

This topic discusses how the user can access the personal address book using the Cisco CallManager User Options.



The user can configure the personal address book and fast dials from the Personal Address Book page in the Cisco CallManager User Options. After adding these services, the user can access the personal address book and fast dials from their Cisco IP Phone.

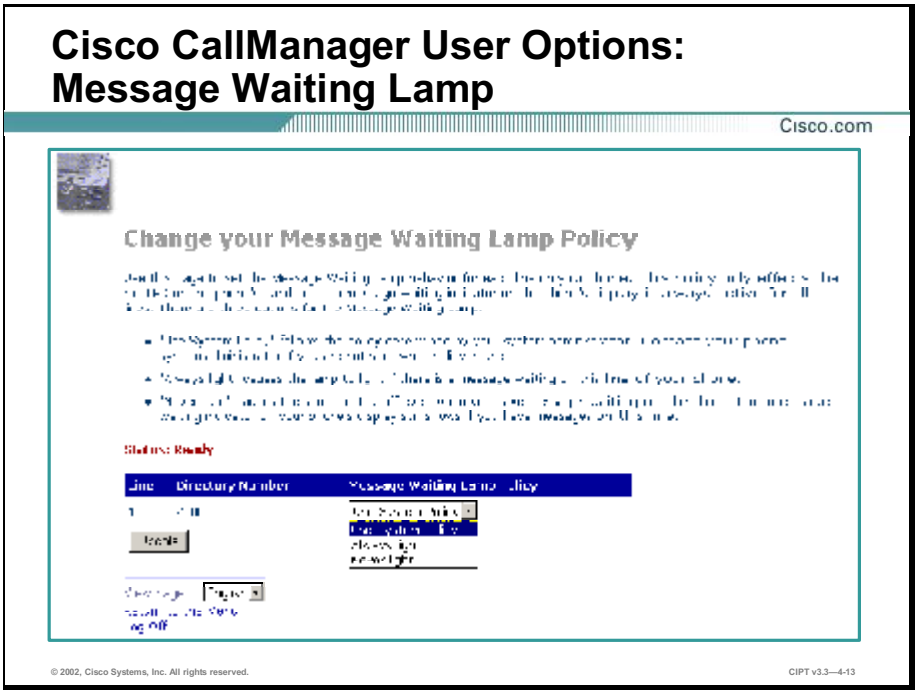
To access the personal address book and fast dials, the user presses the Services button on the IP Phone, and then selects either service.

Example

A user who does not have their PC, but has an IP Phone, can still access important telephone numbers by accessing their personal address book from the Cisco IP Phone. Also, if the user has configured the fast dials, they can dial any person in their fast dials list by pressing only three buttons on their IP Phone.

Message Waiting Lamp Policy

This topic discusses how the user can configure the Message Waiting Lamp (indicator) of a Cisco IP Phone using the Cisco CallManager User Options page.



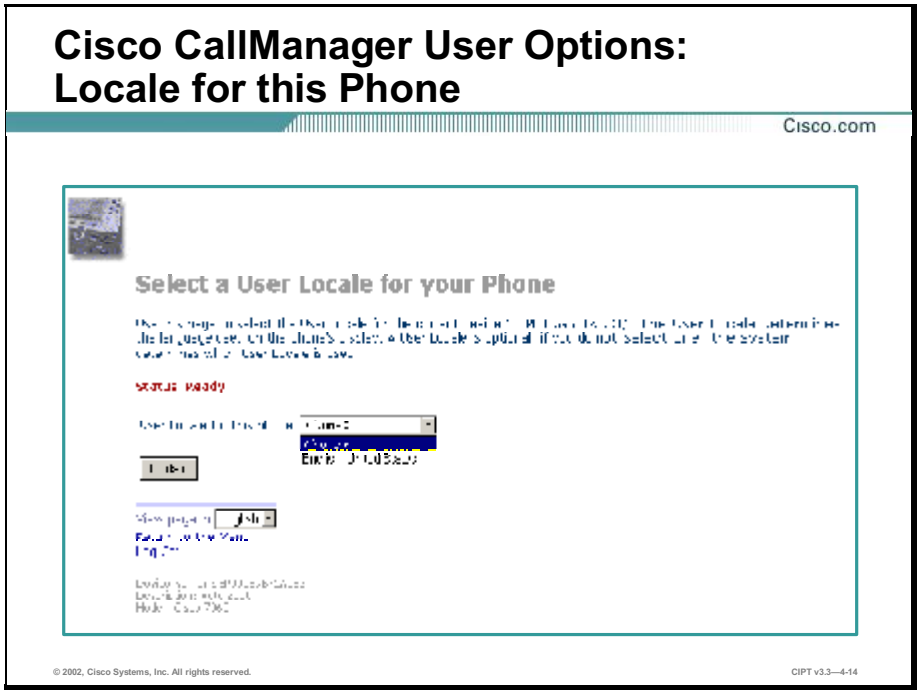
The user can set the Message Waiting Lamp Policy for a device. There are three settings that the user can configure: Use System Policy, Always light, or Never light. The default system policy is set to light the lamp. If the user wants to be sure that their message waiting lamp gets lit when a voice message is left, they should choose Always light policy.

Example

If a user is associated to multiple devices, but would like to know when a voice mail is left from only one of those devices, the user can set all other devices to Never light. By setting the other devices to Never light, the user will only be aware of a voice message from one device.

Personalize Device Locale

This topic discusses how the user can customize the language of the Cisco IP Phone LCD by using the Cisco CallManager User Options page.



The default language installed on the CCM is English. If other locals are required, you can download them from the Cisco website. If you download these languages, your users can customize the display text on their IP Phone to display in one of these languages or locales:

- English, United States
- Francais, France
- Deutsch, Deutschland
- Russki, Russia
- Espanol, España
- Italiano, Italia
- Dutch, Netherlands
- Norwegian, Norway
- Portuguese, Portugal

- Swensk, Sverige

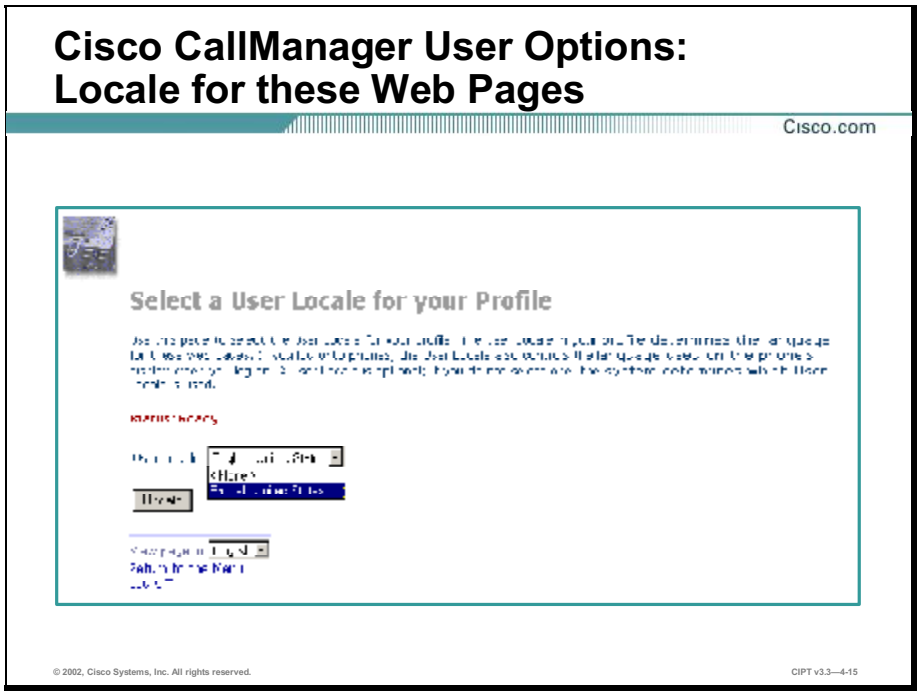
If a user locale is not selected, the system wide locale will be used.

Example

If a user speaks Russian and is using a telephone in Italy and the system wide locale for devices is Italia, the user can log on to the Cisco CallManager User Options page and set the locale for the device to Russia. The user can configure the IP Phone to display text in the desired language without administrator intervention.

Personalize Cisco CallManager User Options Web Page Locale

This topic discusses how the user can customize the language (locale) in which they view the Cisco CallManager User Option web pages.



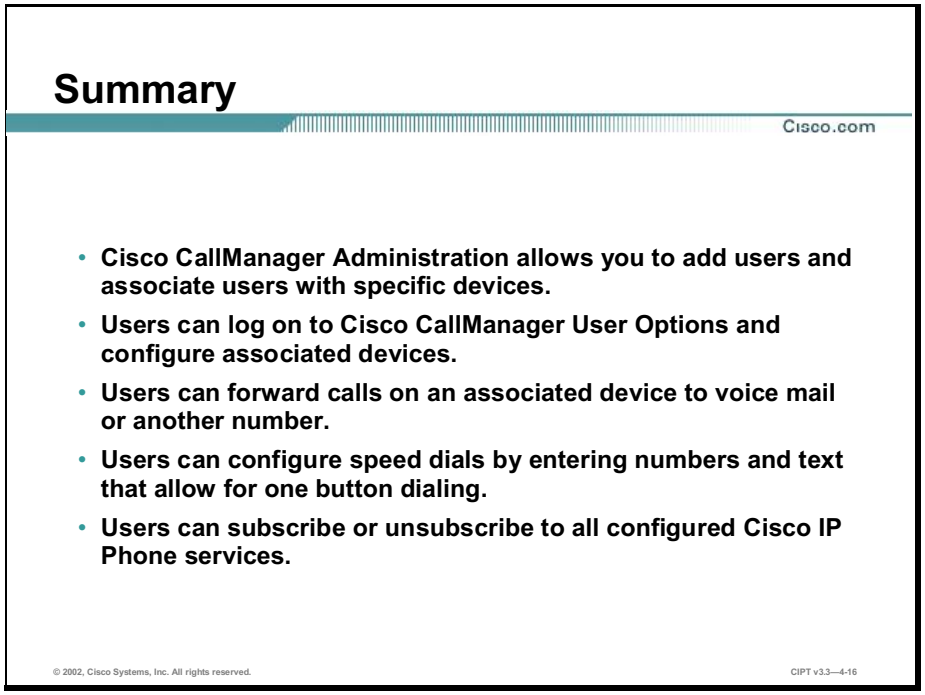
The default language installed on the CCM is English. If other locales are required, you can download them from the Cisco website. If you download these languages your users can customize the language of the IP Phone, but they may also customize the Cisco CallManager User Options web pages display. From the User Locale menu, the user can use the system wide locale setting you configure or select from one of the following languages.

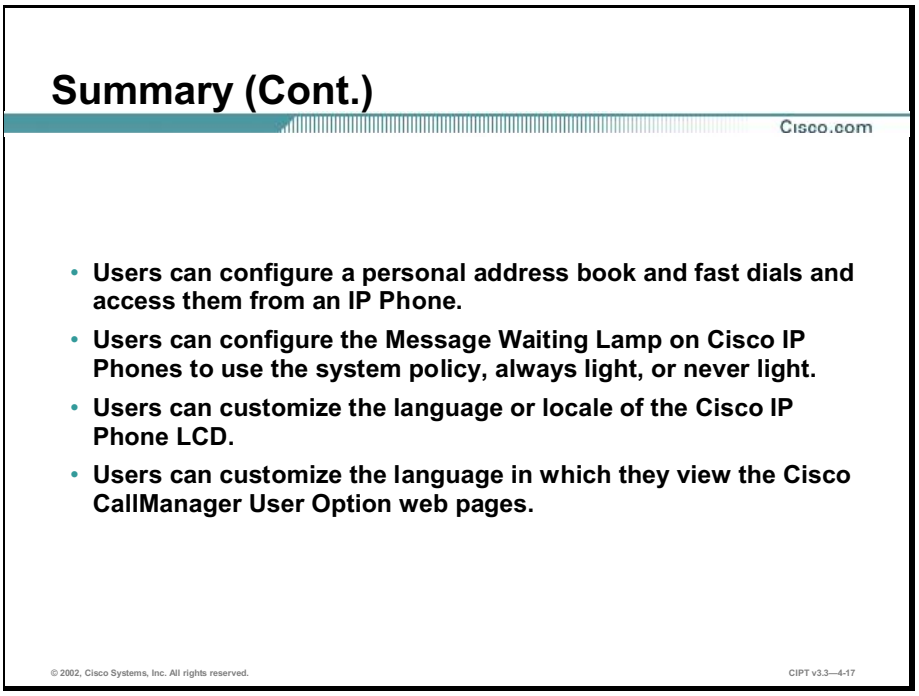
- English, United States
- Francais, France
- Deutsch, Deutschland
- Russki, Russia
- Espanol, España
- Italiano, Italia
- Dutch, Netherlands

- Norwegian, Norway
- Portuguese, Portugal
- Swensk, Sverige

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Applications module

References

For additional information, refer to these resources:

- The Help files within Cisco CallManager Administration

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of these fields is NOT required when configuring a user?

A) First Name

B) Last Name

C) User ID

D) Manager User ID

Q2) Which two of these fields must the user complete in order to log on to the Cisco CallManager User Options page? (Choose two.)

A) User ID

B) Password

C) PIN

D) Full Name

Q3) Which protocol does the CCM use to interface with the user database server?

A) X.500

B) LDAP

C) XML

D) TCP/IP

Q4) In order to allow a user to use the Cisco IP SoftPhone, which option must you select?

A) Enable SoftPhone Use

B) Enable XML Application Use

C) Enable Softphone Access

D) Enable CTI Application Use

Q5) What URL should you provide to users to allow access to the User Options page?

A) http://<server_name>/ccmuser/Logon.asp

B) http://<server_name>/ccmuser/Logon.htm

C) http://<server_name>/ccmadmin/Logon.asp

D) http://<server_name>/ccmadmin/Logon.htm

Q6) What option is a user NOT able to configure from the User Options page?

A) Call Forwarding

B) Message Waiting Lamp Policy

C) IP Phone Services

D) Voice Mail Retrieval

Q7) Using the default 7960 phone template, how many speed dials is a user able to configure on their 7960 Cisco IP Phone?

A) 2

B) 4

C) 6

D) 10

Q8) What programming language is used to support the user services on the 7940/7960 Cisco IP Phones?

A) X.500

B) LDAP

C) XML

D) TCP/IP

Q9) How many user locale languages are included in the default CCM installation?

A) 1

B) 2

C) 6

D) 15

5

Applications

Overview

This module discusses the applications that integrate with Cisco CallManager (CCM).

Upon completing this module, you will be able to:

- Describe how to configure the server and client Cisco CallManager Attendant Console components
- Describe and configure the Cisco IP SoftPhone and Extension Mobility
- Describe the features and functions of applications that can be integrated in a Cisco IP telephony solution

Outline

The module contains these lessons:

- CCM Attendant Console
- Cisco IP SoftPhone
- Cisco Voice over IP Integrated Applications

CCM Attendant Console

Overview

This lesson discusses the Cisco CallManager (CCM) Attendant Console, which is a plug-in application that comes with CCM.

Importance

Companies that want to have one individual handle all incoming calls can install and use the CCM Attendant Console at the receptionist desk. Unlike a manual console, the web-based CCM Attendant Console uses open standards and leverages familiar click-and-drag functionality.

Objectives

Upon completing this lesson, you will be able to:

- Identify and define the components of the CCM Attendant Console
- List the user and administrative features of the CCM Attendant Console
- Define the scalability and redundancy features of the CCM Attendant Console
- Configure CCM for the CCM Attendant Console
- Install and configure the CCM Attendant Console client

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Basic knowledge of CCM and IP Phones
- Basic understanding of the Cisco CallManager Administration page

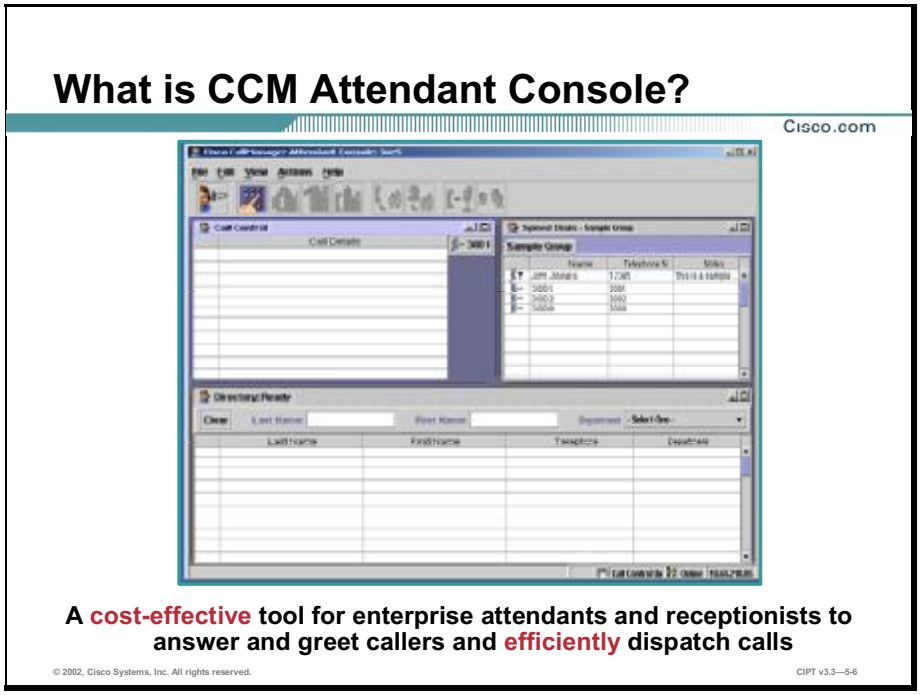
Outline

This lesson includes these topics:

- Overview
- Introduction to CCM Attendant Console
- CCM Attendant Console Features
- Scalability and Redundancy
- Server and Administration Configuration
- Client Installation
- Summary
- Lesson Review

Introduction to CCM Attendant Console

This topic introduces the Cisco CallManager (CCM) Attendant Console.



CCM Attendant Console is an application that supports the traditional role of a manual attendant console. Associated with an IP Phone, this application allows the attendant to quickly accept and dispatch calls to enterprise users.

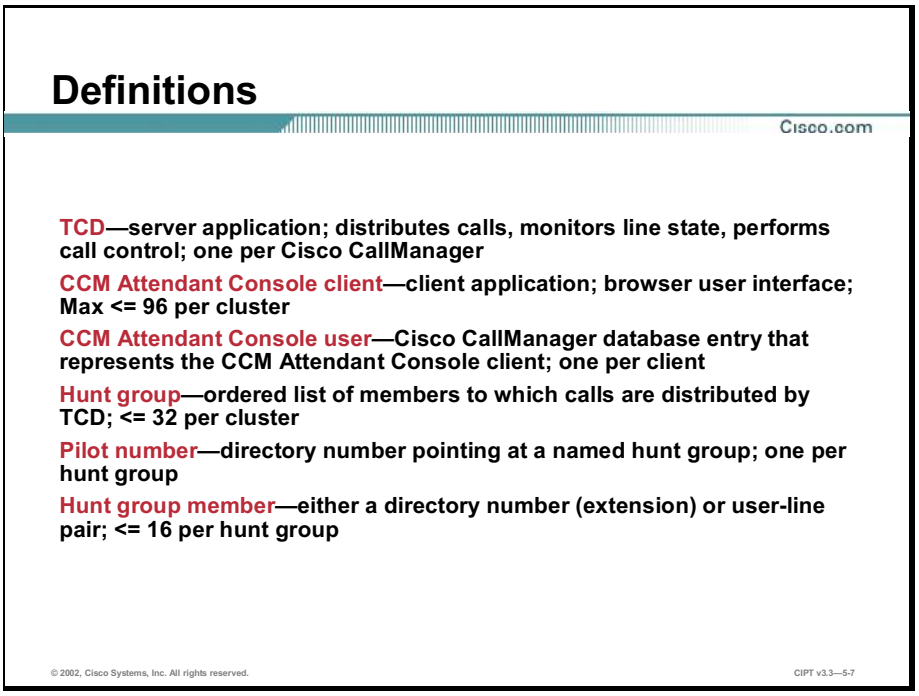
On startup, the Settings dialog box opens and prompts you for the Cisco CallManager (CCM) server name and the directory number of the telephone that you are using with the CCM Attendant Console. The CCM Attendant Console login dialog box opens and prompts you for your username and password.

The CCM Attendant Console graphical user interface (GUI) supports the following display resolutions: 800x600, 1024x768, 1280x1024, and 1600x1200. The CCM Attendant Console runs on Microsoft Windows 98, Windows Me, Windows 2000 Professional, or Windows NT 4.0 platforms.

Note Make sure that you have the latest Microsoft service packs installed on the PC.

CCM Attendant Console works with a Cisco IP Phone that is registered to a CCM system (one CCM Attendant Console for each IP Phone). Multiple CCM Attendant Consoles can connect to a single CCM system.

The application registers with and receives call-dispatching services from the Cisco Telephony Call Dispatcher (TCD) services on CCM.



This table defines some of the terminology used when referring to the CCM Attendant Console application.

Table: CCM Attendant Console Terms and Definitions

Term	Definition
TCD	Server application; distributes calls, monitors line state, performs call control; one per CCM
CCM Attendant Console client	Client application; web browser user interface; maximum 96 clients per CCM cluster
CCM Attendant Console user	CCM database entry; represents the CCM Attendant Console client; one per client
Hunt group	Ordered list of directory numbers to which TCD distributes calls; maximum 32 per CCM cluster
Pilot number	Directory number points to a named hunt group; one per hunt group
Hunt group member	Either a directory number (extension) or user-line pair; maximum 16 per hunt group

CCM Attendant Console Features

This topic introduces the user and administrative features of the CCM Attendant Console.

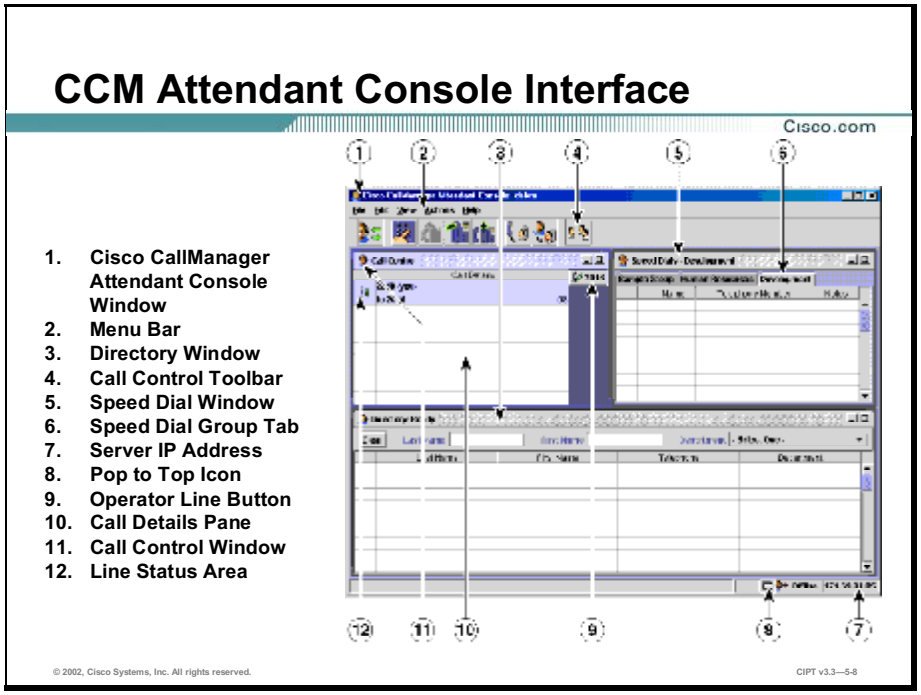


Table: CCM Attendant Console Interface

Number	Reference	Number	Reference
1.	Cisco CallManager Attendant Console Window	7.	Server IP Address
2.	Menu Bar	8.	Pop to Top Icon
3.	Directory Window	9.	Operator Line Button
4.	Call Control Toolbar	10.	Call Details Pane
5.	Speed Dial Window	11.	Call Control Window
6.	Speed Dial Group Tab	12.	Line Status Area

The CCM Attendant Console efficiently automates the user and the administrative operations of a manual attendant function. It has an intuitive and configurable GUI to handle calls and monitor line state. The CCM Attendant Console software allows the assignment of line state monitors without the need to physically label extender boxes with each line monitor change. You can monitor the line for each user, as opposed to monitoring only a select few, as in a time-division multiplexing (TDM)-based system. Monitoring each line is a benefit over traditional consoles and line extenders.

Advanced drag-and-drop capabilities and access to corporate Lightweight Directory Access Protocol (LDAP) directories offer clear advantages over traditional manual attendant stations.

In a system with hundreds or thousands of users, a CCM Attendant Console operator can accept calls and perform a directory lookup by selecting the field title in the Directory section and typing in the first few characters of the last name, first name, or department for the user. A directory search will return information that matches the query.

An operator can view the status of a user line (busy, idle, or ringing) and advise the caller of the line state. The operator can then transfer the call to the user by either initiating a traditional transfer sequence through the Transfer icon or dragging and dropping the call from the selected loop to the desired user record. The primary benefits of this user interface are quicker transaction times and increased customer satisfaction.

User features include the following:

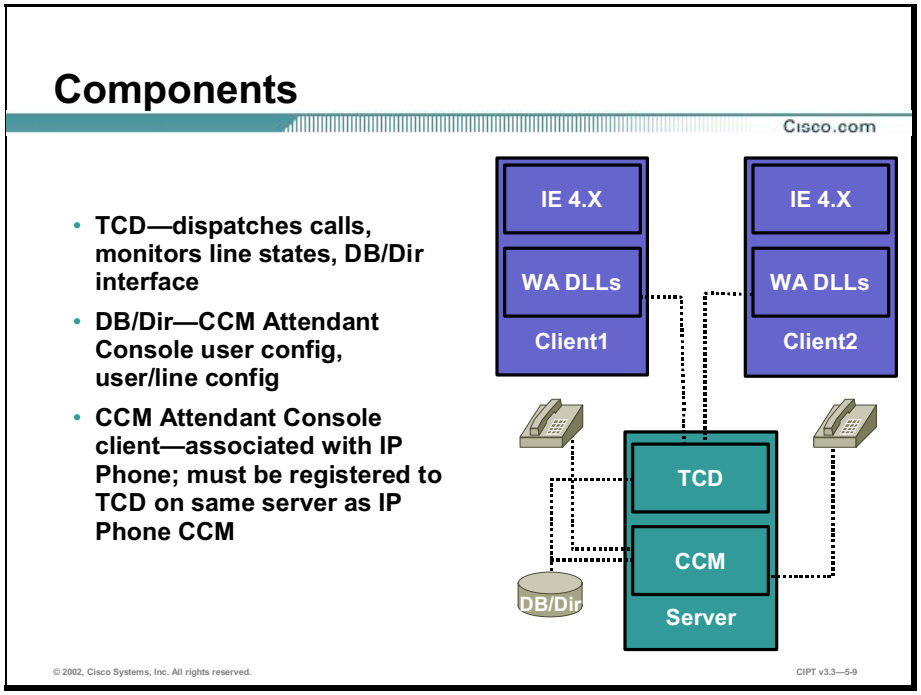
- Loop keys, which provide simultaneous management of all lines available on associated telephone
- Line states, such as idle, active, ringing, and unknown
- User label per line monitor key for easy reference to user
- Query, which searches by last name, first name, extension, or department
- Sort, which sorts by last name, first name, extension, or department

Administrative features include the following:

- Remote system and/or device installation and configuration through a Web browser
- Simultaneous line monitor by multiple operators, which provides simultaneous viewing of the line state of any line from the console user interface
- Call distribution from a single pilot number to multiple directory numbers or user-line pairs
- Simultaneous monitoring of inbound calls from multiple operator positions
- The creation of up to 16 pilot numbers or distribution groups

Scalability and Redundancy

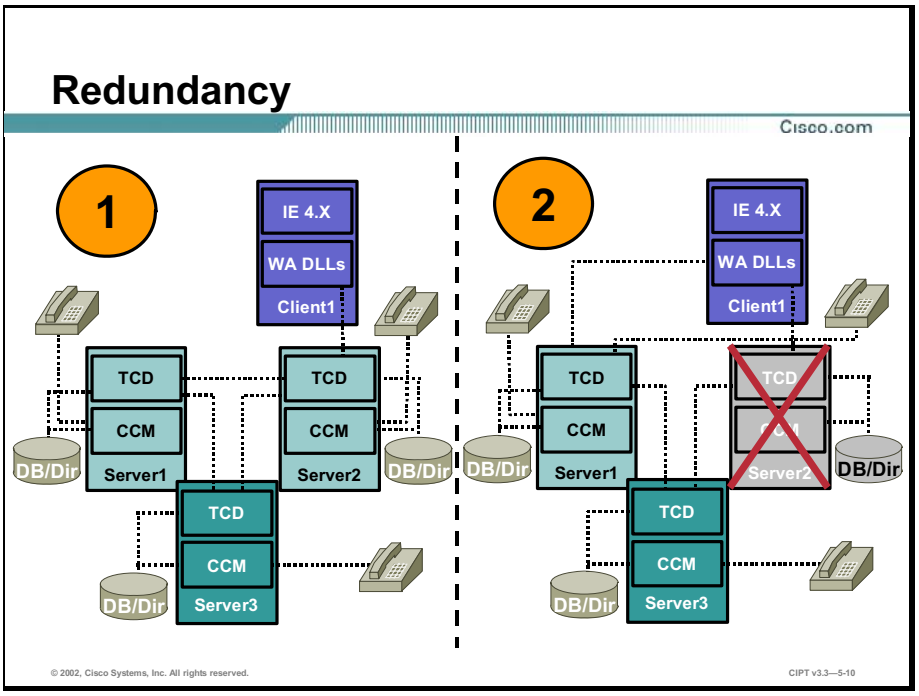
This topic discusses the scalability and redundancy of the CCM Attendant Console.



CCM Attendant Console is scalable. You can assign call distribution groups to any pilot number and can then assign the pilot number to one or more CCM Attendant Console loops. These loops represent answerable lines in a multiple-attendant system. Calls are queued to one or more on-line attendant loops, allowing scalability and distribution among multiple operators.

You can distribute the CCM Attendant Console among multiple CCMs in a cluster, and you can install it on any workstation that has an IP Phone in close proximity. The scalability highlights of the CCM Attendant Console are:

- 32 hunt groups (pilot numbers) per CCM cluster.
- 16 hunt group members (directory number and user line) per hunt group.
- Two hunting algorithms, which are Longest Idle and First Available.
- Configure as many call loops per CCM Attendant Console as there are lines on the controlled IP Phone device. You can assign any loop as a hunt group member.
- 96 CCM Attendant Consoles per CCM cluster.
- 512 (32 hunt groups x 16 hunt group members) simultaneous calls per cluster on a maximum of 96 configured CCM Attendant Consoles.



The CCM Attendant Console application registers with and receives call-dispatching services from the Cisco TCD. The Cisco TCD, a CCM service, provides communication among CCM servers, CCM Attendant Consoles, and the Cisco IP Phones used with the CCM Attendant Consoles.

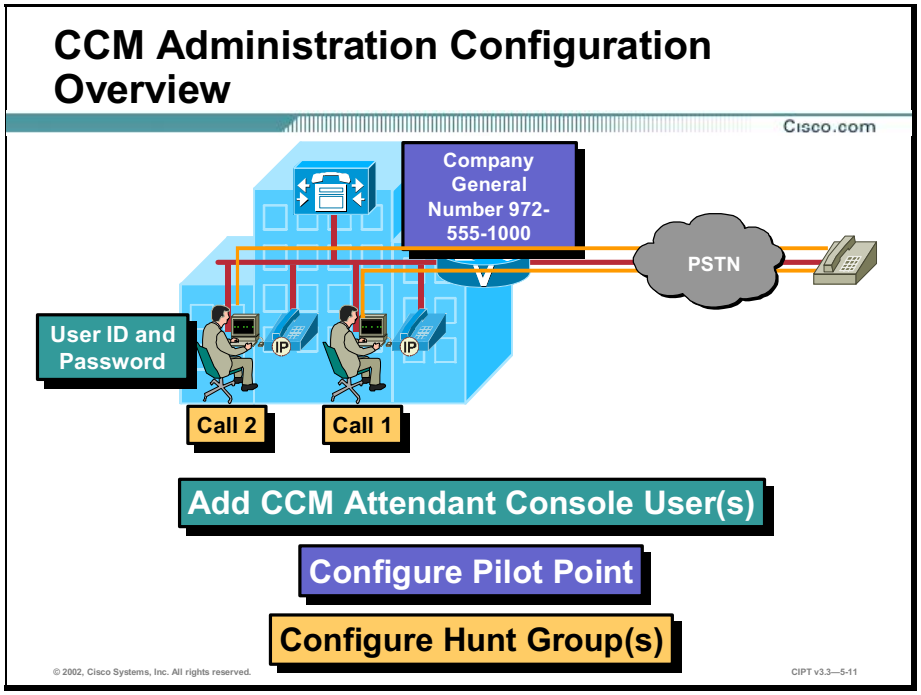
This sequence of events outlines the redundancy process used by the CCM Attendant Console.

- **Sequence one:** Normal operation
  - CCM Attendant Console Client 1 registers with the TCD component on Server 2. IP Phone 2, associated with the CCM Attendant Console, is also registered to Server 2.
- **Sequence two:** CCM failure
  - Server 2 fails, and IP Phone 2 now registers with Server 1.
  - Client 1 searches the TCDs on Servers 1 and 3 for the presence of IP Phone 2. Client 1 finds IP Phone 2 on Server 1.
  - Client 1 registers to TCD 1.

The CCM Attendant Console always registers to the TCD on the same CCM server that registers the associated IP Phone.

Server and Administration Configuration

This topic describes the CCM server portion of the CCM Attendant Console configuration.

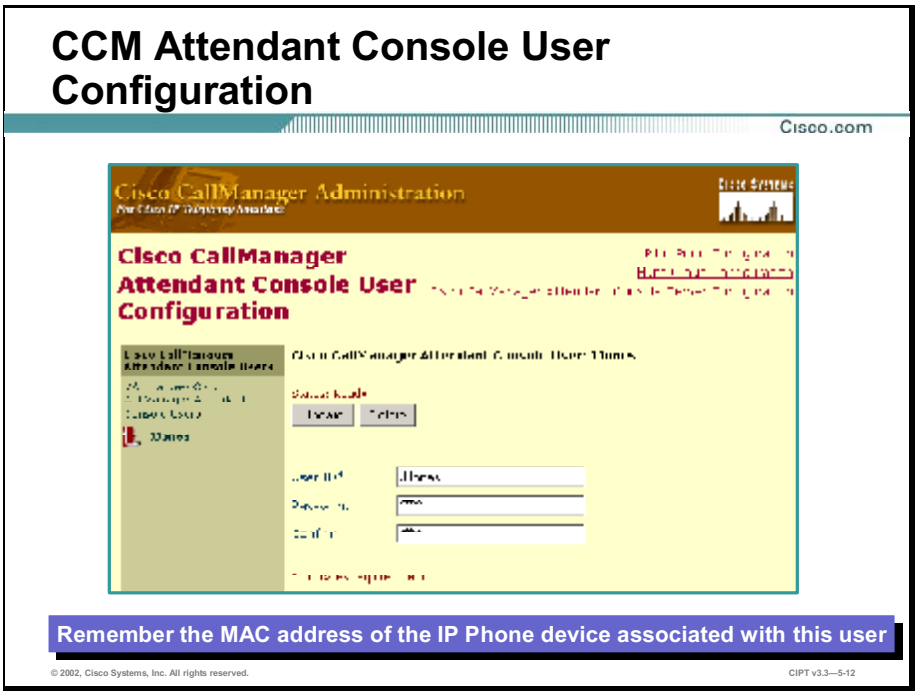


The configuration of the CCM server to support the CCM Attendant Console consists of three main phases:

- **Configure CCM Attendant Console users:** These individual users will use the CCM Attendant Console application. They are not the same as directory users that you configure in the User area of the Cisco CallManager Administration page.

- **Configure the pilot point for the CCM Attendant Console:** The pilot point is a directory number that provides access to CCM Attendant Console users indirectly through hunt groups. The pilot point usually maps to the general company number (switchboard number), but it can use a directory number outside of the Direct Inward Dialing (DID) range.

- **Configure hunt groups:** Hunt groups consist of CCM Attendant Console users or directory numbers. When adding a CCM Attendant Console user with multiple line numbers to the hunt group, you must specify which line to use. Directory numbers, configured in hunt groups, usually point to voice mail, IP Interactive Voice Response (IVR), or IP Auto Attendant (AA).



You must add users through the CCM Attendant Console User Configuration page and assign them a password *before* they can log into a CCM Attendant Console client.

To open the CCM Attendant Console Configuration page, access **Service>Cisco CM Attendant Console** in Cisco CallManager Administration. Then, in the upper-right corner of the pane, click the **Cisco CallManager Attendant Console User Configuration** link.

To create user accounts for each CCM Attendant Console user, enter the appropriate User ID and Password for each account and click the **Insert** button.

You must create one generic user, the “ac” user, and associate the attendant IP Phones and the pilot points with this user. When you configure the “ac” user, the CCM Attendant Console can then interact with the Computer Telephony Integration Manager (CTI Manager) service on the CCM server. Perform the following procedure to configure the “ac” user:

Step 1 Choose **User>Add a New User** in the Cisco CallManager Administration page.

Step 2 Enter **ac** in the First Name and Last Name fields.

Step 3 Enter **ac** in the User ID field.

Step 4 Enter **12345** in the User Password field.

Step 5 Enter **12345** in the Confirm Password field.

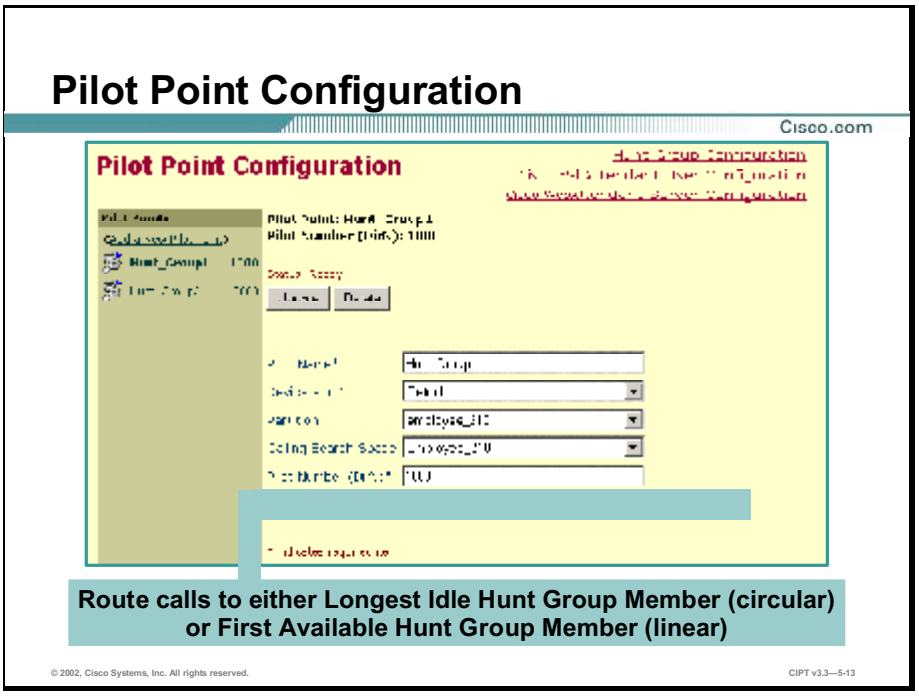
Step 6 Enter a personal identification number (PIN) and telephone number.

Step 7 Check the **Enable CTI Application Use** check box. You must check this box for the CCM Attendant Console to interact with CTI Manager.

Step 8 Click **Insert**.

Step 9 Associate all attendant IP Phones and pilot points with the “ac” user.

Caution If you do not configure the “ac” user and correctly associate the attendant devices, the CCM Attendant Console cannot interact with the CTI Manager and will not function.



You must configure pilot points and hunt groups through the Cisco CallManager Administration page before the Cisco TCD can route calls.

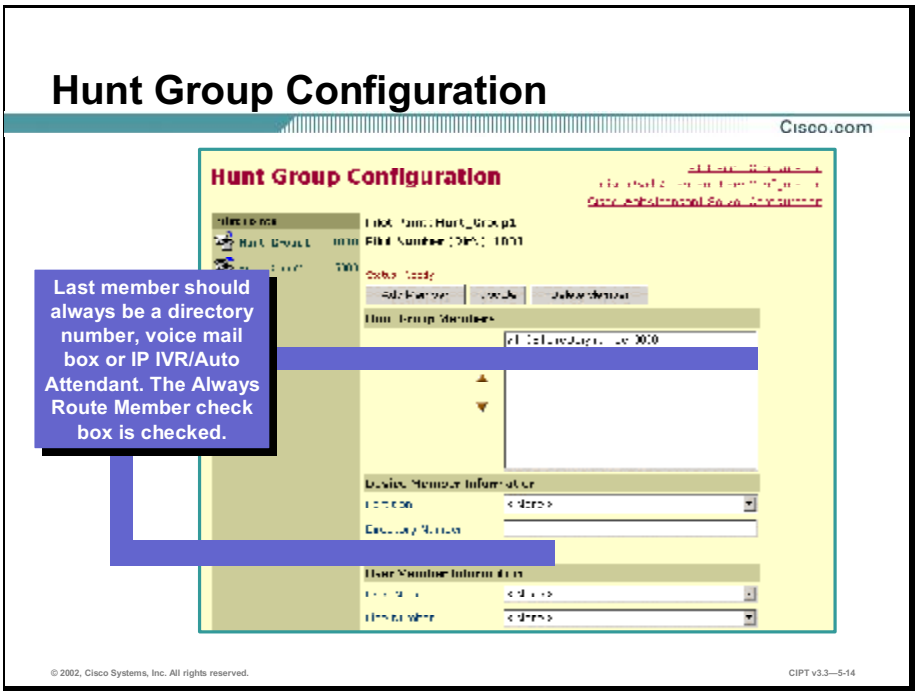
In Cisco CallManager Administration, access **Service>Cisco CM Attendant Console** to open the Pilot Point Configuration page as shown in the figure.

The Pilot Point Configuration Fields table defines the settings on the Pilot Point Configuration page.

Table: Pilot Point Configuration Fields

Field	Description
Pilot Name	Enter up to 50 alphanumeric characters, including spaces, to specify a descriptive name for the pilot point.
Device Pool	To view the valid values for the Device Pool field, you can click the drop-down arrow and choose a device. The device pool has the CCM whose Cisco TCD service will service this pilot point. When selecting the device pool, consider the primary CCM, call processing, and device load balancing.
Partition	Use the drop-down arrow to view the Partition field values, and choose **None**. CCM Attendant Console pilot points do not belong to partitions.
Calling Search Space	To designate which partitions the pilot point searches when attempting to route a call, you can use the drop-down arrow to view the Calling Search Space field values and then choose a calling search space.
Pilot Number (DirN)	Enter a directory number into this field to designate a directory number for this pilot point. Verify that this number is unique throughout the system; it cannot be a shared-line appearance.
Route Calls To	Use the drop-down arrow to view the Route Calls To field values. You will choose one of the following options, based on the type of hunt group member: ■ Choose the **First Available Hunt Group Member** option to route incoming calls to the first available member of a hunt group. ■ Choose the **Longest Idle Hunt Group Member** option to order members based on the length of time that each directory number or line remains idle. If the voice-mail number is the longest idle member of the group, Cisco TCD will route the call to voice mail without first checking the other members of the group.

Note If the pilot point is not the main or general telephone number, the main number can go to a translation pattern that is transformed to the pilot number.



After you configure the pilot point, you must configure the hunt group. A hunt group consists of a list of destinations (either directory numbers, or CCM Attendant Console user or line numbers) that determine the call redirection order.

In Cisco CallManager Administration, access **Service>Cisco CM Attendant Console.** The Pilot Point Configuration pane will display. Click the link to **Hunt Group Configuration** in the upper-right corner of the Pilot Point Configuration pane. The Hunt Group Configuration page will display. Choose the pilot point for which you want to add hunt group members.

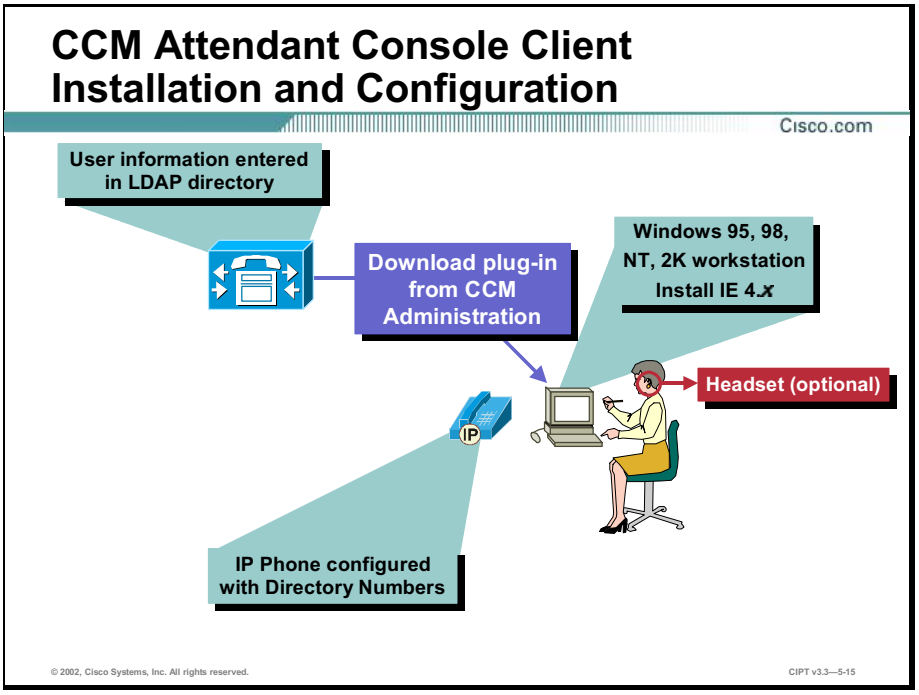
The Hunt Group Configuration Fields table defines the settings on the Hunt Group Configuration page shown in the figure.

Table: Hunt Group Configuration Fields

Field	Description
Partition	If a hunt group member is a directory number, you can use the drop-down arrow to view the values for the Partition field, and then choose the appropriate option. Enter the directory number in the **Directory Number** field in the Device Member Information section. The partition designates the route partition to which the directory number belongs. If the directory number for this hunt group member is in a partition, you must choose a partition. If the directory number is not in a partition, choose **None**. Always Route Member is an optional check box that applies to directory numbers only. If this check box is checked, Cisco TCD always routes the call to this hunt group member, whether it is busy or not. To manage overflow conditions, you can check this check box for voice-mail or auto-attendant numbers that handle multiple, simultaneous calls. For linked hunt groups, only check the **Always Route Member** check box when you are configuring the final member of each hunt group.
Directory Number	Enter the directory number of the hunt group member device in this field. When the directory number is not in the specified partition, an error dialog box displays.
User Name	If the hunt group member is a user and line number, fill in only the **CCM Attendant Console User Name** and **Line Number** fields in the User Member Information section. Use the drop-down arrow to view the values for the User Name field, and choose the CCM Attendant Console users that will serve as hunt group members. Only CCM Attendant Console usernames, added using CCM Attendant Console User Configuration, appear in this list.
Line Number	Use the drop-down arrow to view the values for the Line Number field, and choose the appropriate line numbers for the hunt group.

Client Installation

This topic describes the installation and configuration of the CCM Attendant Console on the client machine.



From the CCM Attendant Console client, perform the following tasks to install the CCM Attendant Console application:

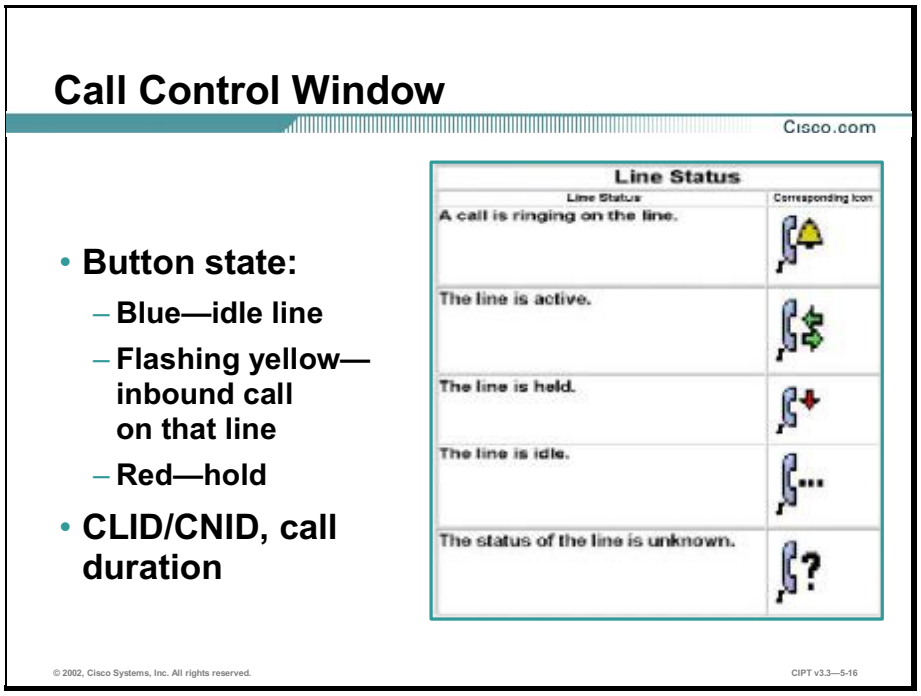
Step 1 Download the CCM Attendant Console plug-in by accessing **Application>Install Plugins** on the Cisco CallManager Administration page. Save the CiscoAttendantConsoleClient.exe file to the local machine.

Step 2 Launch the CiscoAttendantConsoleClient.exe file.

Step 3 Specify the IP address of CCM TCD server and the directory number of the associated IP Phone, and click **Save**.

Step 4 Provide the user ID and password.

After you install the CCM Attendant Console, the user is ready to start the application. After opening the CCM Attendant Console application, the user will have to log in and then go online. The user is then ready to answer calls.



The Call Control window has the following two components:

- **Call Details pane:** This component includes the line status, the directory number of the incoming call, the name of the person (if available), the operator directory number, and the elapsed time display.

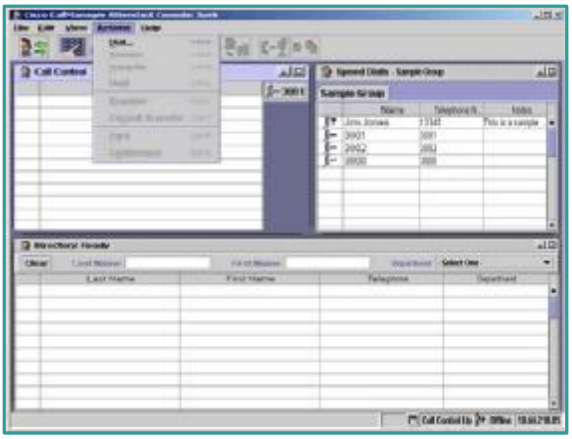
- **Operator Line buttons:** This component includes the line status and the directory number of the attendant Cisco IP Phone, displayed in the upper-right corner of the window.

The Call Details pane displays the lines on the Cisco IP Phone that the CCM Attendant Console controls. The number of lines configured depends on the type of configuration. For example, if you have a Cisco IP Phone Model 7960 with two attachments of the Cisco IP Phone Expansion Module 7914, a total of 34 lines can display if you associated a directory number with each line.

Client Menu Options

Cisco.com

- **Log on/off—CCM Attendant Console user not available as hunt group member**
- **Invoke features—drag and drop**
- **Keyboard shortcuts**



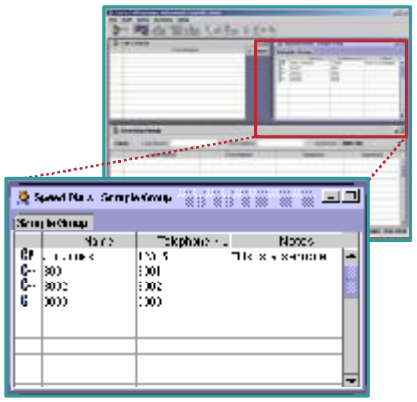
The features of the CCM Attendant Console are menu-driven. You can use the associated shortcut keys to access all of the menu functions.

- **File menu:** From the File menu, you can go online or offline, log out, and exit the program.
- **Edit menu:** From the Edit menu, you can create your own keyboard shortcuts. You can also add, modify, and delete speed-dial entries or groups, and view or revise settings, which is an optional task.
- **View menu:** From the View menu, you can change the size of the text in the windows or the color on the console.
- **Actions menu:** You perform call-control tasks through the Actions menu. This menu includes many feature options such as answering calls, transferring calls, parking calls, and enabling other features on the system.
- **Help menu:** CCM Attendant Console provides on-line help and easy access to the latest CCM Attendant Console plug-in for an upgrade.

CCM Attendant Console Client GUI: Customized Speed Dials

Cisco.com

- 26 button/indicators
- Dual function:
  - Speed dial with user label
  - Line state monitor
- Configured by dragging user entry from 'Directory' section
- Invoke features—drag and drop



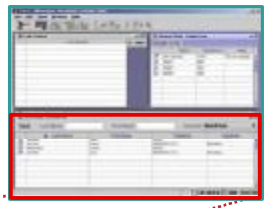
CIPT v3.3—5-18

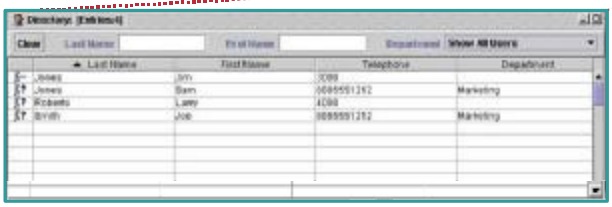
The Speed Dial pane is located in the upper-right corner of the screen. The speed dials contain directory numbers and labels. By clicking any speed-dial button, you place a call from the currently selected attendant line to the associated directory number. You can also drag and drop the directory number or speed-dial number to the attendant line from which you are making calls.

CCM Attendant Console Client GUI: Directory Lookup

Cisco.com

- **Line state**
- **Invoke features through drag and drop or keyboard shortcut**
- **Access to all users in LDAP directory**
- **Sortable columns; column header character string entry queries LDAP/local directory**



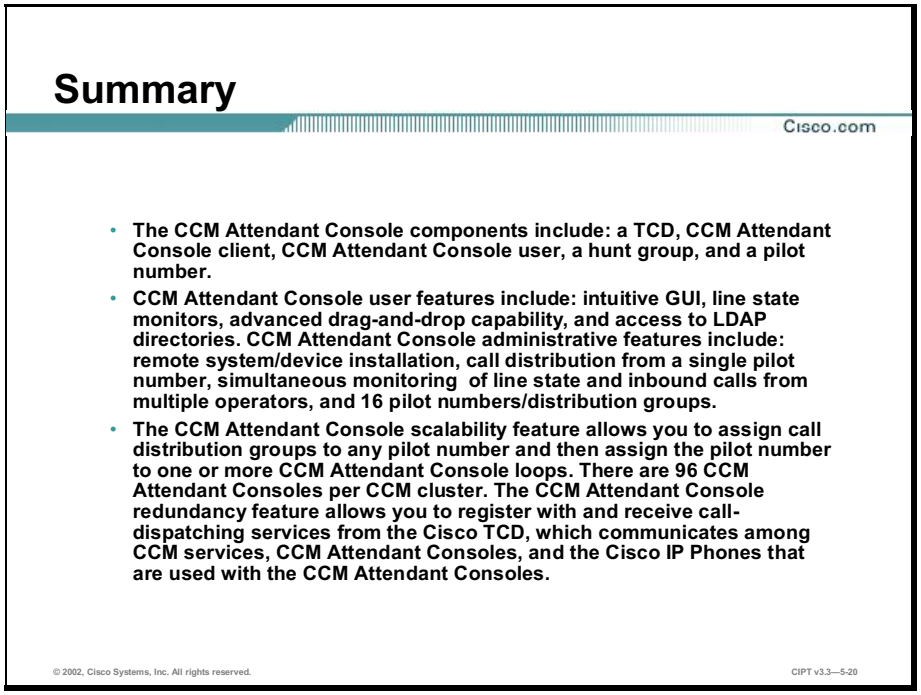


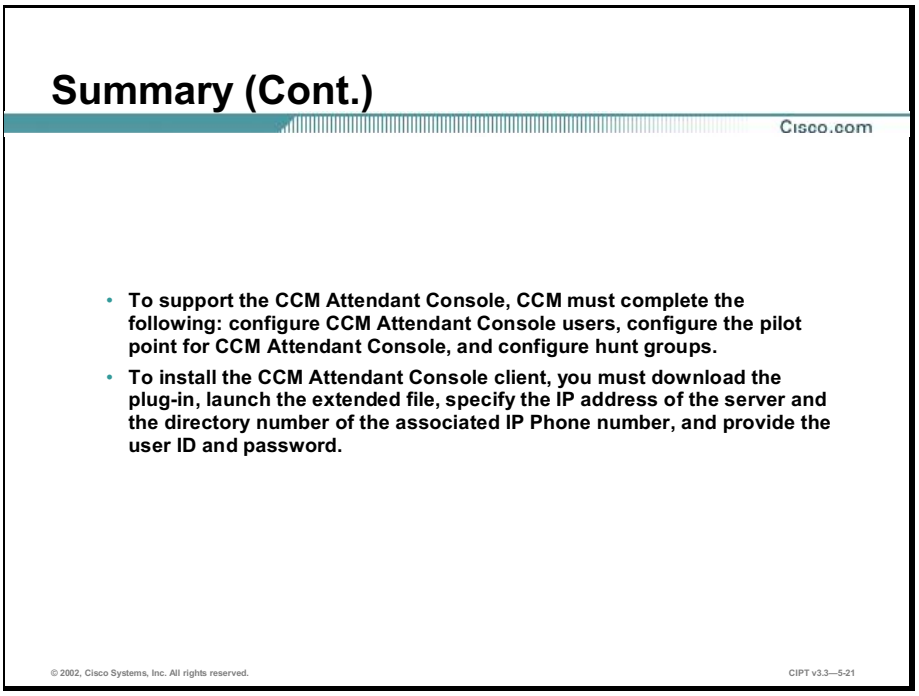
The bottom grid is the Directory pane. This pane shows a system directory telephone listing. You will find a Status column that displays whether the line is idle, ringing, active, or unknown. You will also see the directory number, first name, last name, and department information if you have configured all of this information to be displayed in the CCM Attendant Console configuration window.

The directory headers display the current order (ascending or descending) of the directory entries. You sort the directory by clicking the up or down arrow in any header in the Directory window.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Cisco IP SoftPhone lesson

References

For additional information, refer to this resource:

- *Cisco Attendant Console Installation and Administration Guide*: http://www.cisco.com/univercd/cc/td/doc/product/voice/attendnt/call_att/ccmac111.htm

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of these terms best describes the number that users would dial to reach a receptionist?

A) hunt group

B) pilot number

C) CCM Attendant Console DN

D) all of the above

Q2) Which of these are valid line states in the CCM Attendant Console client? (Choose all that apply.)

A) idle

B) active

C) ringing

D) unknown

Q3) The CCM Attendant Console client software interfaces directly with which of these CCM components?

A) CiscoAC.dll

B) hunt group

C) pilot point

D) TCD

Q4) To function correctly, what user must you create for the CCM Attendant Console?

A) ac

B) proxy

C) transparent

D) CAC

Q5) To run the CCM Attendant Console, what must a client workstation have?

A) a recent Microsoft operating system

B) a Cisco IP Phone in close proximity

C) the LDAP CCM Attendant Console user information

D) all of the above

Cisco IP SoftPhone

Overview

The Cisco IP SoftPhone is a communications application for your PC desktop. Because Cisco IP SoftPhone is an integral part of the Cisco Architecture for Voice, Video and Integrated Data (AVVID), you can use it with any application that supports a Cisco IP Phone, as it is fully integrated with the Cisco line of IP Phones.

This lesson describes the configuration of the Cisco IP SoftPhone and Extension Mobility features. A Cisco CallManager (CCM) cluster that includes the Customer Response Solution (CRS) server provides these features. This lesson also examines the configuration of CRS.

Importance

The Cisco IP SoftPhone is an application that provides flexibility and increases productivity for users. It allows the users within a company to have one device that supports data and voice technologies. With Cisco IP SoftPhone, users can collaborate with a simple click.

The Extension Mobility feature allows users to log in to an IP Phone device and have their extension and preferences placed on that IP Phone device. This lesson benefits those students who work in an office environment where multiple users share the same IP Phone device, such as a sales office or a 24-hour service office.

Objectives

Upon completing this lesson, you will be able to:

- Identify and define the Cisco IP SoftPhone features and components
- List and describe the considerations that need to be taken into account when deploying the Cisco IP SoftPhone
- Configure CCM for Cisco IP SoftPhone use
- Install, configure, and use the Cisco IP SoftPhone application
- Describe the Extension Mobility feature

- Configure the Extension Mobility feature

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Basic familiarity with the Cisco CallManager Administration page
- General Microsoft Windows knowledge (installation of programs, control panel settings, and other processes)

Outline

This lesson includes these topics:

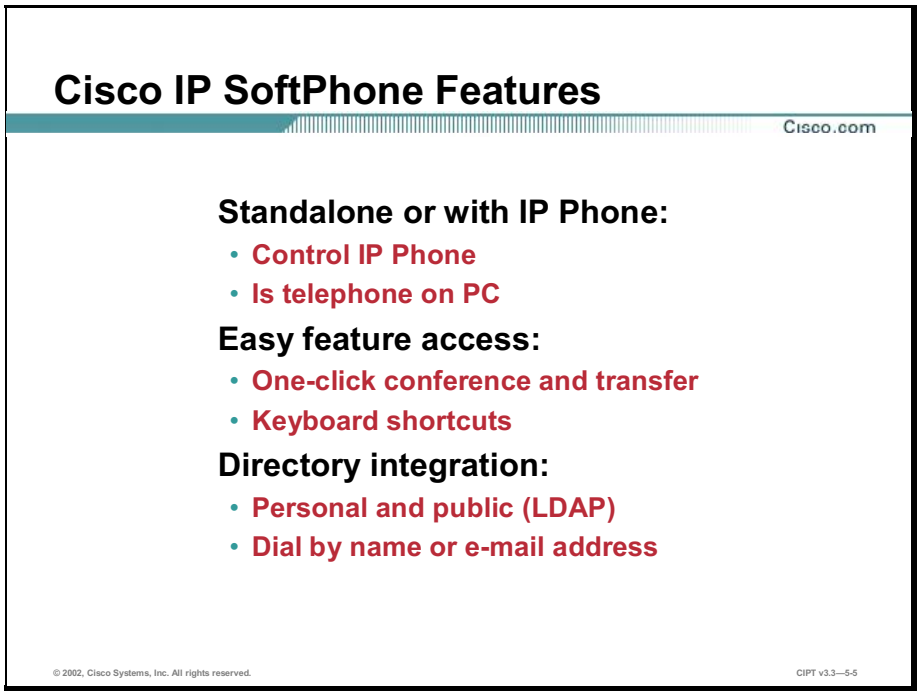
- Overview
- Cisco IP SoftPhone Features and Components
- Deployment Considerations
- CCM Cisco IP SoftPhone Configuration
- Client Cisco IP SoftPhone Installation and Configuration
- Extension Mobility
- Extension Mobility Configuration
- Summary
- Lesson Review

Cisco IP SoftPhone Features and Components

This topic examines the features and components of the Cisco IP SoftPhone.

Cisco IP SoftPhone takes advantage of PC usability, controls IP Phone hardware, and functions as a standalone software IP Phone. The intuitive user interface and context-sensitive controls replace the archaic keystroke combinations of legacy telephones. In addition, Cisco IP SoftPhone integrates with Microsoft NetMeeting, providing advanced multimedia collaboration tools with a single click.

Cisco IP SoftPhone also implements Lightweight Directory Access Protocol (LDAP) services that are integrated into Cisco Architecture for Voice, Video and Integrated Data (AVVID). Calling users is as simple as looking up names in a directory, and dragging and dropping the information into the Cisco IP SoftPhone. With a personal directory or telephone book, users can locate contact list and connection information *without* being connected to a main directory server.



Cisco IP SoftPhone is a Windows-based application for the PC. Used alone or in conjunction with the Cisco IP Phone, Cisco IP SoftPhone provides the following features:

- **Mobility:** With Cisco IP SoftPhone running on a laptop, users can receive calls when connected to the corporate network. When traveling, users can use the dial-up connection to check voice mail and place calls.

- **Directory integration:** Integration with LDAP directories allows users to quickly place or transfer calls by looking up individual names or e-mail addresses. This integration also supports corporate and public directories and a personal address book.

- **Intuitive user interface:** The Cisco IP SoftPhone intuitive user interface and context-sensitive controls replace the nonintuitive buttons of legacy telephones. Extensive use of drag-and-drop allows users to quickly place calls from most Windows programs, using virtual business cards (VCards), directory entries, and text fields.

- **Virtual conference room:** Setting up conference calls is quick and intuitive. Users can invite participants by dragging and dropping directory entries onto the user interface to create a virtual conference room. During a voice conference, you can share desktop applications with all of the participants by choosing them from a list or dragging the associated documents into the virtual conference room.

- **Telephony Application Programming Interface (TAPI) architecture:** The TAPI architecture is an abstraction layer between the TAPI application (Cisco IP SoftPhone) and the underlying hardware and transport protocols of Cisco CallManager (CCM). The Cisco IP SoftPhone application accesses the device-specific controls for communication and call processing through a dynamic link library (DLL). Each TAPI application is a separate

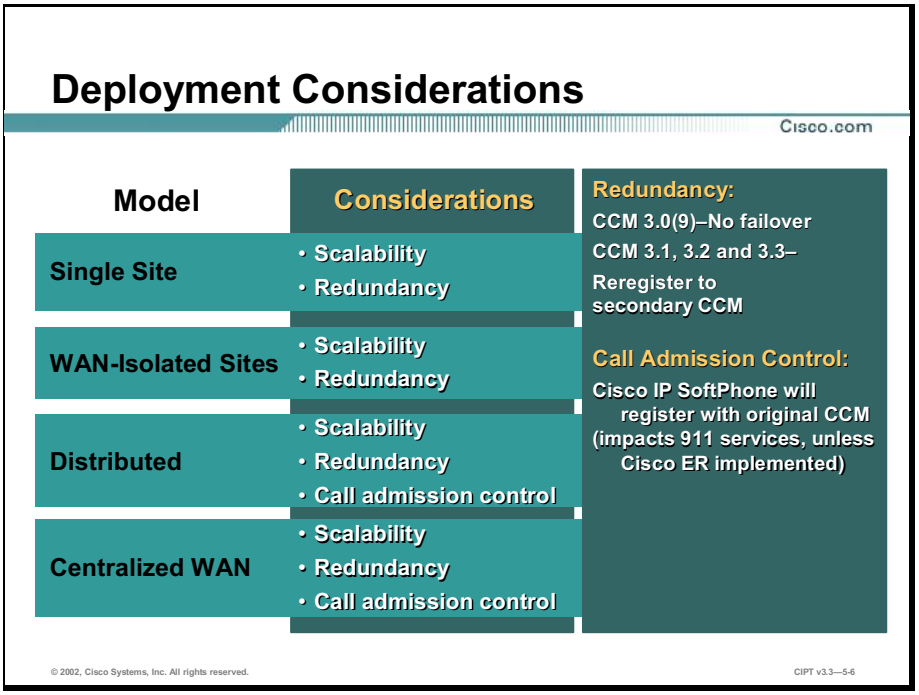
process that communicates using TAPI with the Tapi32.dll or Tapi3.dll, provided by Microsoft.

- **Other features include:** Users can turn on the auto-answer feature so that Cisco IP SoftPhone answers a call after a configurable number of rings.
  - Users can also record a .WAV file on a PC using any sound recording application and specifying the location of the .WAV file in the Cisco IP SoftPhone. They can use this .WAV file as a custom greeting that automatically plays when a call is answered.Function keys in Cisco IP SoftPhone are context sensitive and are only available to the user in the correct call state. For example, a user can place a call on hold only after the call has reached the connected state.
  - Cisco IP SoftPhone uses DirectX 6 to implement media termination. DirectX 6 ensures the highest level of sound-card compatibility, because the media player for Microsoft also uses it.
  - The media termination components handle all compression rates supported by Cisco AVVID, such as G.711, G.723, and G.729. In theory, using G.729 transcoding will only require about 30 kbps of bandwidth. G.711 may be used, however, to match internal voice encoding and provide better quality. G.711 requires at least 80 kbps of bandwidth. For this reason, Cisco recommends 128 kbps as the minimum bandwidth requirement for Cisco IP SoftPhone users. This bandwidth requirement will ensure that G.711 audio and overhead packets from the user station are transmitted back into the corporate network where the CCM is located.
  - The media-terminating component of Cisco IP SoftPhone performs voice activity detection (VAD) to reduce bandwidth usage.
  - When Cisco IP SoftPhone has keyboard focus, all letters are translated to numbers, based on the mapping of a telephone keypad. This process allows you to easily dial vanity numbers, such as 222-FILM, and makes it easy to specify names when using the dial-by-name feature for automated telephone attendant systems.
  - In addition to the keyboard, you can use the Cisco IP SoftPhone graphical user interface (GUI) keypad to enter numbers. This keypad also translates letters to digits and allows the user to paste numbers from the clipboard for dialing. You can use this process when entering account numbers during an interaction with an interactive voice response (IVR)-based checking system.
  - An enterprise can distribute Cisco IP SoftPhone on a CD-ROM, or configure and download it to the client machines over the network or Internet. Administrators can configure settings including the server address, LDAP preferences, and dial plans.
  - Cisco IP SoftPhone users can specify their own dial plans to translate strings (which the user enters into the Destination field) into numbers that CCM can route. These strings may come from several sources, including VCards, text from a document, and web-based yellow pages, and can have different formats for each user.
  - When a line has the call-waiting feature and a user is already on a call, an incoming call appears as a second call block with its own caller ID field.

- Organizations can choose either a Windows NT logon or Cisco AVVID directory-based security when deploying Cisco IP SoftPhone.

Deployment Considerations

This topic describes the deployment options and considerations for Cisco IP SoftPhone.



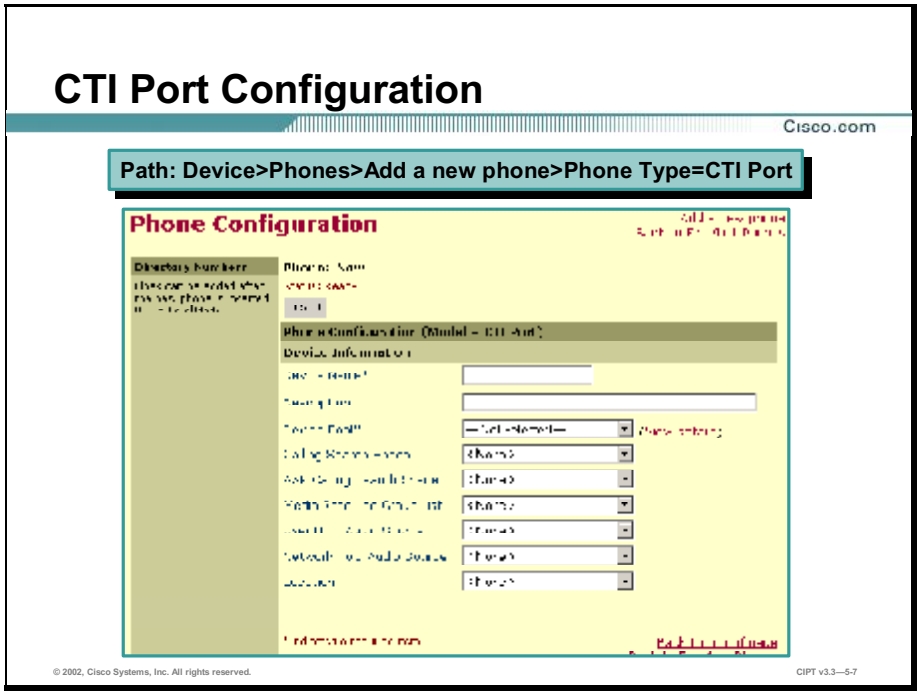
A Cisco IP SoftPhone is a “heavier” device within CCM. The Cisco IP SoftPhone consumes a considerable amount of device weight units (20 units) compared to a standard IP Phone (1 unit).

When deploying the Cisco IP SoftPhone, you must consider the increased device weight. For example, if the CCM server is a Cisco Media Convergence Server (MCS) 7835 with a maximum of 5000 device weight units, the server will support 2500 IP Phones, but only 250 Cisco IP SoftPhones.

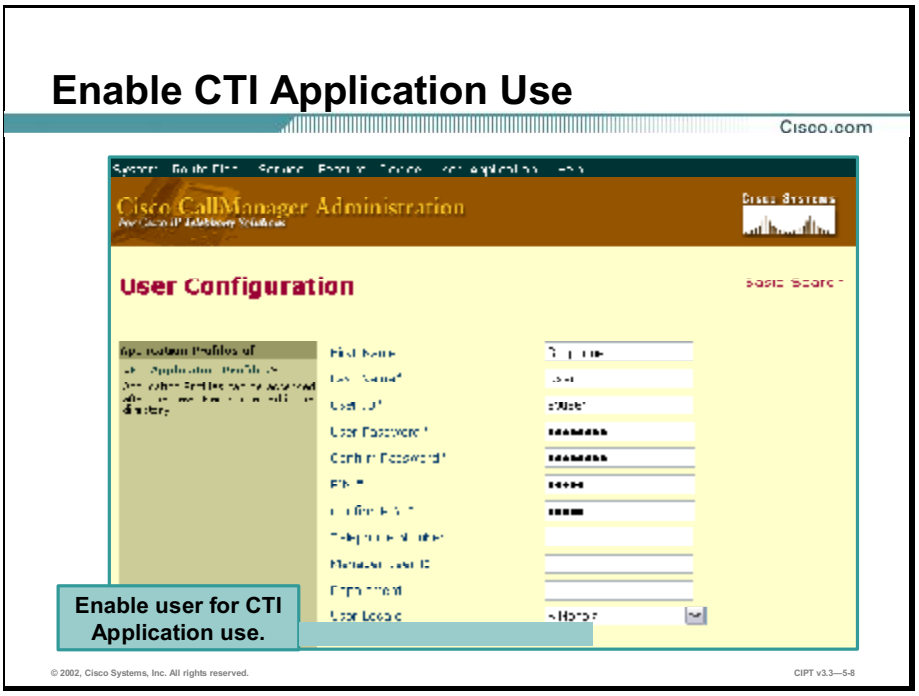
Call Admission Control (CAC) directly affects 911 services. Cisco IP SoftPhones will register with their original CCM. When Cisco IP SoftPhone initiates calls, they route out of original CCM, regardless of where Cisco IP SoftPhone is located in the network. Cisco Emergency Responder (ER) alleviates this issue.

CCM Cisco IP SoftPhone Configuration

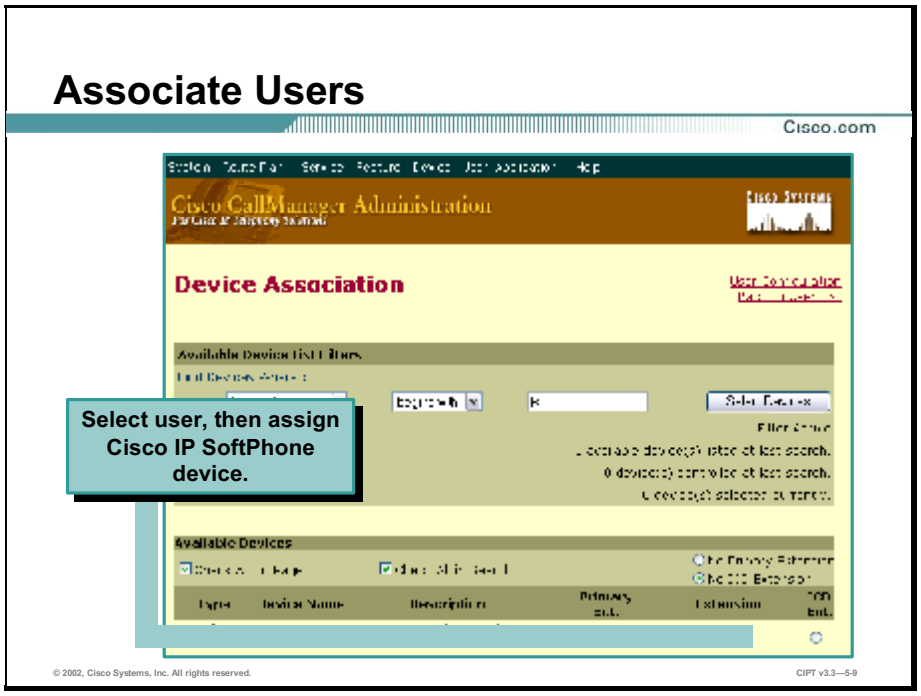
This topic describes the required CCM configuration to enable Cisco IP SoftPhone use.



To enable Cisco IP SoftPhone use, you must first configure a Computer Telephony Integration (CTI) port, which is a device in Cisco CallManager Administration. Because the CTI port is a telephone type, to access this page you must go to **Device>Phone>Add New Phone** and choose **CTI Port** as the telephone type.



For a Cisco IP SoftPhone to use first-party control, you must enable Cisco IP SoftPhone CTI application use. When adding a user or updating the personal profile for a user, check the **Enable CTI Application Use** check box. Checking this box also enables the Auto Attendant (AA) application to search for the user.

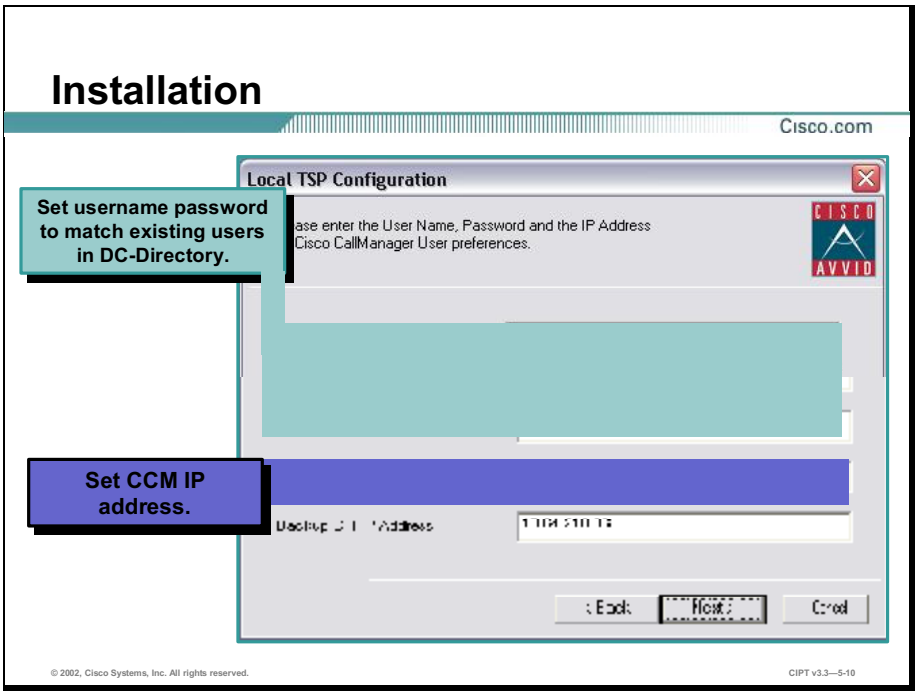


After enabling users to use a CTI application, you must associate users with their configured CTI port device.

Note	Creating a CTI port is similar to configuring a telephone device. After you associate users to this CTI port device, they are ready to install Cisco IP SoftPhone on their desktop or laptop.

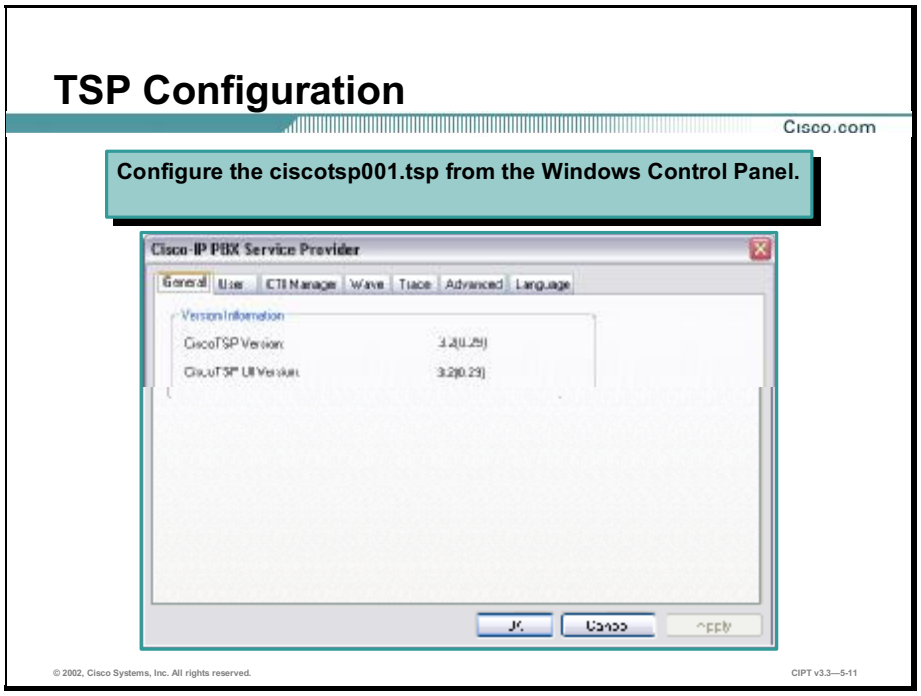
Client Cisco IP SoftPhone Installation and Configuration

This topic examines the Cisco IP SoftPhone installation and configuration.



The majority of the installation process is intuitive; however, users must have some information readily available.

When installing the Cisco IP SoftPhone, users will use their user IDs and passwords to log on to the CCM User Options page. Cisco IP SoftPhone 1.2 and above support CCM redundancy, and the user must know the IP addresses of their primary and secondary CCMs. In most cases, you must provide your users with this information.



In some instances (such as troubleshooting why users do not have any lines listed in their Cisco IP SoftPhone), you must verify that you have configured the Cisco TAPI Service Provider (TSP) service in Windows to communicate with the CCM. This procedure describes how to verify the configuration:

Step 1 From the Windows control panel, choose **Telephony** (Windows 95/98/Me/NT) or **Phone and Modem Options** (Windows 2000/XP).

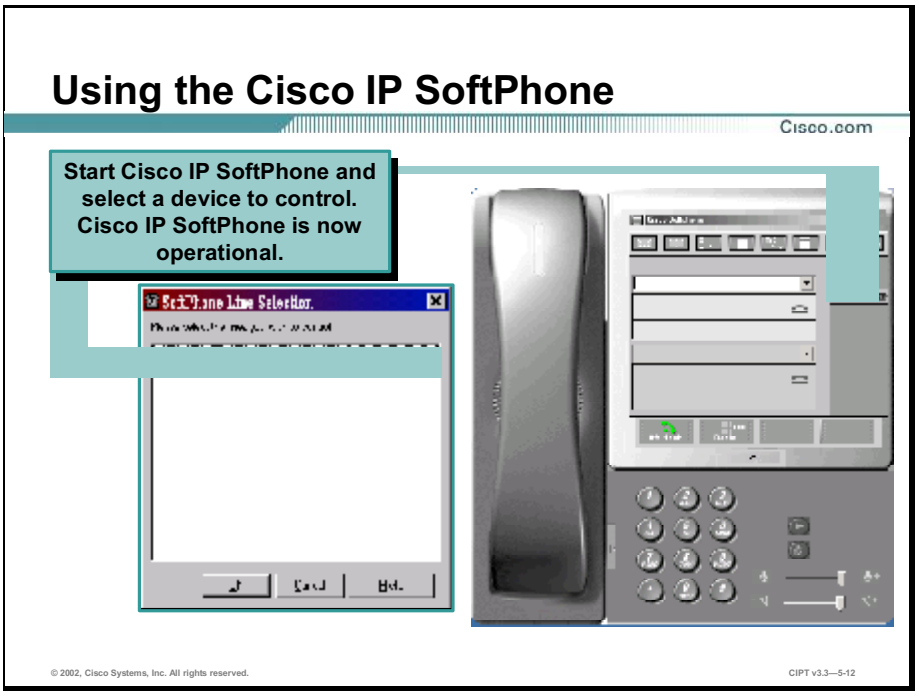
Step 2 Click the **Telephony Drivers** tab (Windows 95/98/Me/NT) or **Advanced** tab (Windows 2000/XP).

Step 3 Choose **ciscotsp001.tsp** in the Selection menu, and click **Configure…**.
If you do not see the **Cisco IP PBX Service Provider** Telephony driver option in the list box, or if you see a **ciscotsp.tsp** option, uninstall Cisco IP SoftPhone and run the install program again.

Step 4 Configure (or verify) the following settings in the Cisco IP PBX Service Provider window: click the **User** tab and re-enter the username and password assigned to this user on the CCM; click the **CTI Manager** tab, and verify that the CCM IP Address radio button is enabled and that the window displays the correct IP address for the CCMs.
If the wrong IP address is displayed, enter the correct address; click the **Advanced** tab; enter **15** in the Synchronous Message Timeout field; click **OK**.

Step 5 Restart the telephony service.

Step 6 Launch Cisco IP SoftPhone.
If you still do not see any lines, verify that you have network connectivity to CCM.

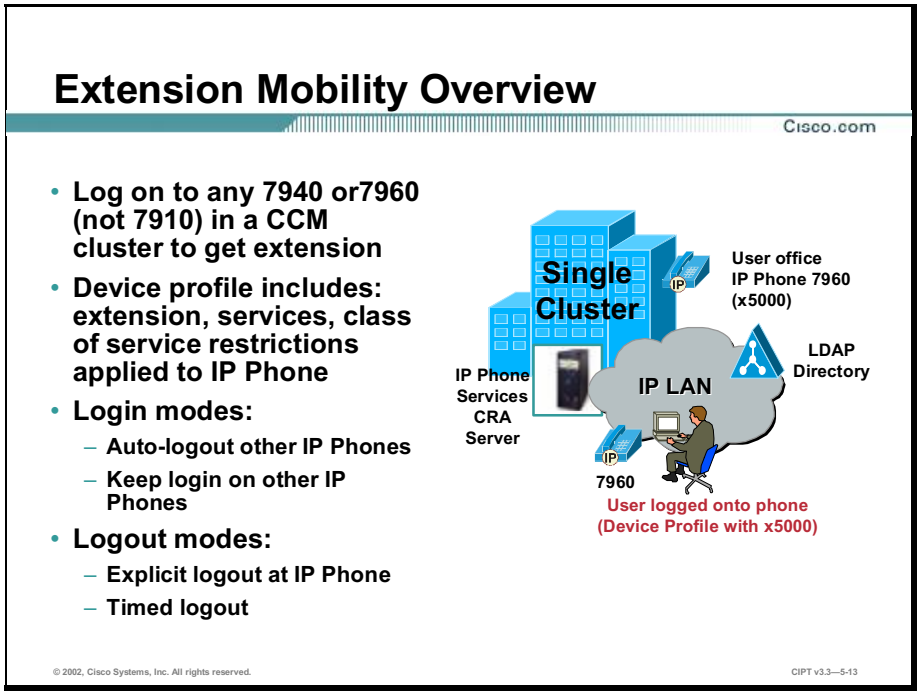


After installing the Cisco IP Phone application and rebooting the PC, a user can launch Cisco IP SoftPhone. Because Cisco IP SoftPhone can operate by either first-party or third-party control, a dialog box appears and prompts the user to choose a line to control. The lines that appear are generated based on the devices associated with the user. The user can then determine how to use Cisco IP SoftPhone by choosing a line. If no lines appear, the user must verify that the TSP configuration in Windows is correct.

Reference This URL provides more information about using the Cisco IP SoftPhone: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/ip_7960/softphon/ver_1_2/eng/user/sp_chap3.htm

Extension Mobility

This topic provides an overview of the Extension Mobility feature.

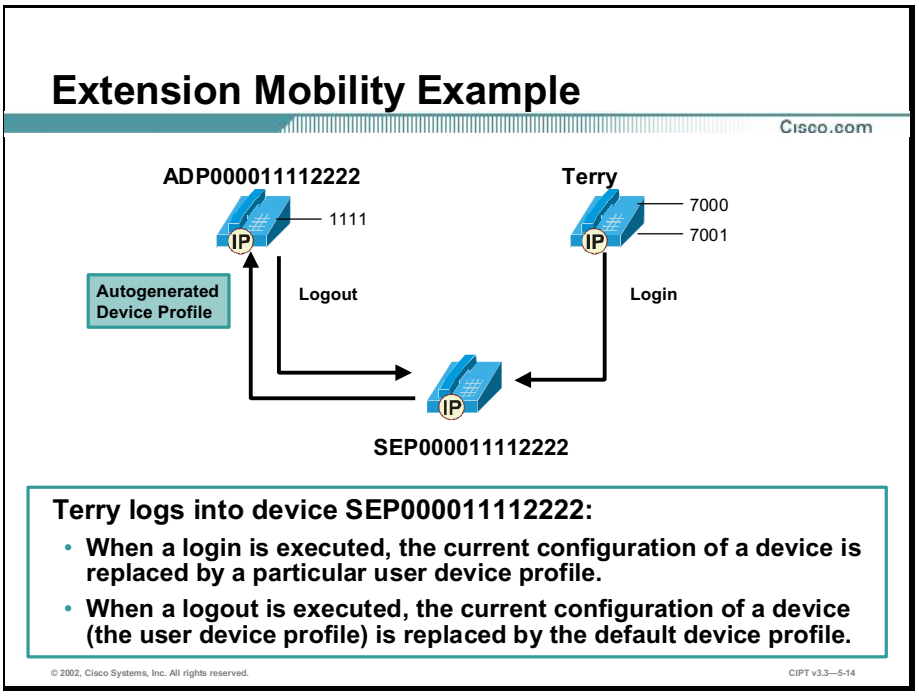


Extension Mobility is an approach to organizing work environments so that workspaces—including offices, cubes, and desks—are not permanently assigned to individuals. Instead, employees "check into" an office space by performing a login process at the IP Phone where they wish to receive their calls. Then, their assigned direct telephone number with all of its characteristics (ring type, speed dial, and other characteristics) associates with that IP Phone. Environments where employees do not routinely conduct business in the same office space every day, such as sales offices, commonly use Extension Mobility.

CCM 3.1 and higher provide a standard login service. Using a set of extensible markup language (XML) over HTTP requests can expand the login service. Third parties (including customers and integrators) can replace the login user interface with one of their own design. For example, third parties can add capabilities to the standard login service such as authenticating via smart card readers or automating the login process according to a "desk sharing" web application.

The multilogin behavior variables define how the system behaves when a user tries to log in to two devices at the same time. For example, the system may allow the second login, the system may not allow the second login, or the system may allow the second login after the first login is automatically logged out.

Because XML-based services support Extension Mobility, it is only available on Cisco IP Phone 7940 and 7960.



Example

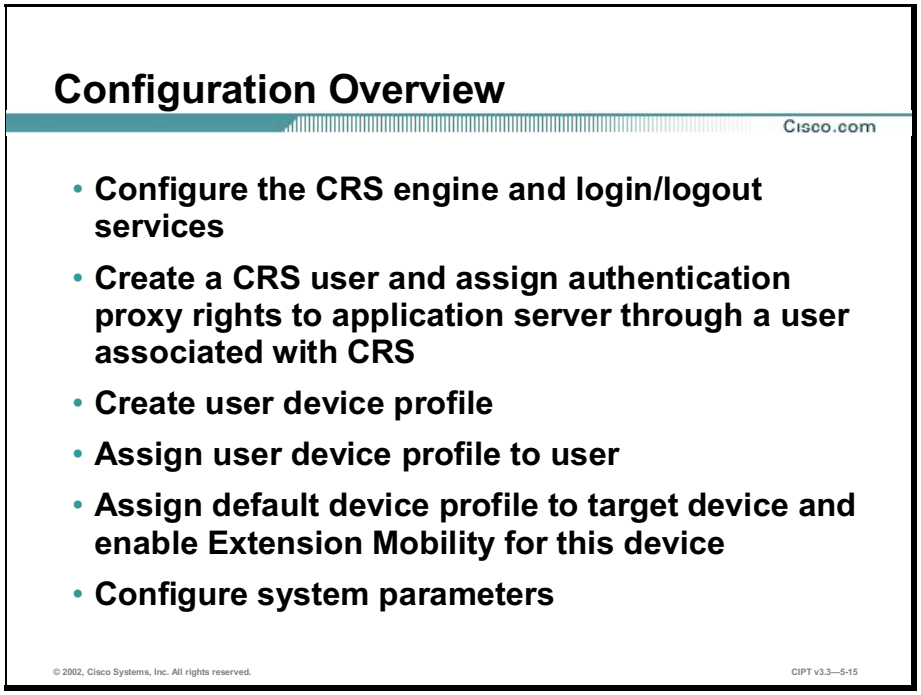
Terry has configured a user device profile called Terry. This profile has a line appearance with a directory number (DN) of 7000 and another with 7001. Terry is logging into device SEP000011112222, which has an autogenerated device profile, ADP000011112222, as its default device profile. The default device profile is configured with a single-line appearance with the DN of 1111.

When Terry logs in, the device restarts and displays lines 7000 and 7001. It no longer has line 1111 assigned to it. All of the speed dials and services configured on Terry replace those that are normally on SEP000011112222.

When Terry logs out, the device restarts and loads the autogenerated device profile.

Extension Mobility Configuration

This topic examines the configuration of the Extension Mobility feature.



To use the Extension Mobility feature, you must configure two applications, CRS and CCM.

In CRS, configure the following elements:

- LDAP directory services
- Login and logout scripts
- HTTP triggers for the login and logout scripts
- CRS user that has authentication proxy rights

In CCM, configure the following elements:

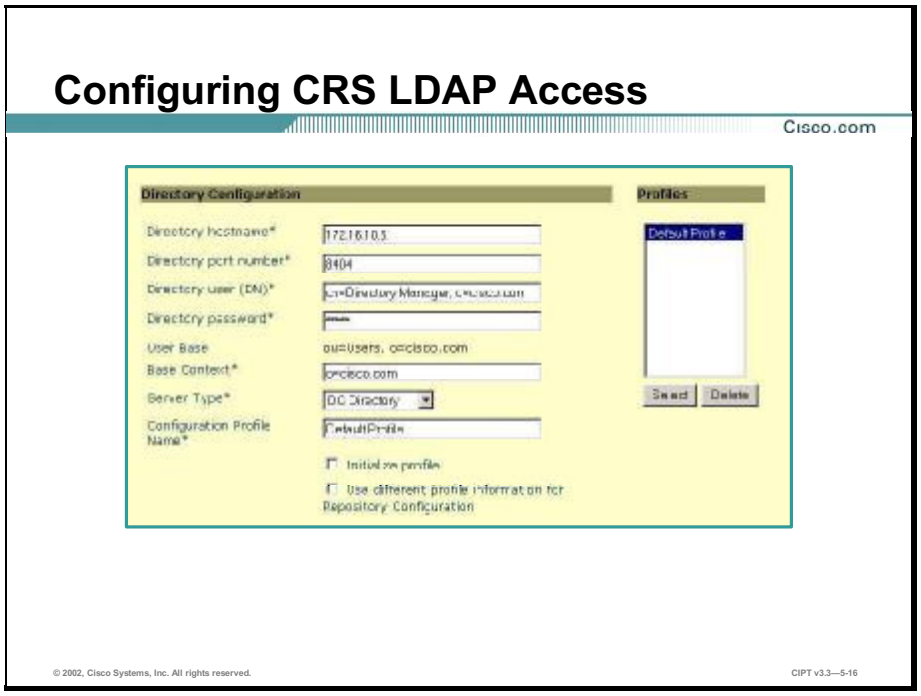
- CCM username that is the same as the CRS username that has authentication proxy rights
- Device profile associated to users that will use the Extension Mobility feature

The Cisco CRS engine provides the underlying services for enabling IP-based telephony applications, such as IP IVR, IP Integrated Contact Distribution (ICD), and extended services (such as Extension Mobility). These applications are scripts written to run on top of the engine, and Cisco packages and sells them individually. For example, when you purchase the Cisco IP IVR, you receive the Application Engine and the scripts for the IVR application.

Extension Mobility in CCM 3.3 uses the hotel.aef script. You receive this script when you purchase and install the Extended Services application. The Extended Services product consists of the Application Engine and the hotel.aef and hotelOut.aef scripts, which allow you to run the login and logout services for IP Phones. These scripts are necessary for logging in and out of Extension Mobility.

If you install (and provide the appropriate license key for) the Extended Services application, these scripts install during the CRS engine installation. You can find these scripts listed in the CRS Application Administration pages under Generic Applications.

Reference The Application Administration pages are available at:
http://<servername>/appadmin.
The <servername> is the hostname or IP address of the CRS server.

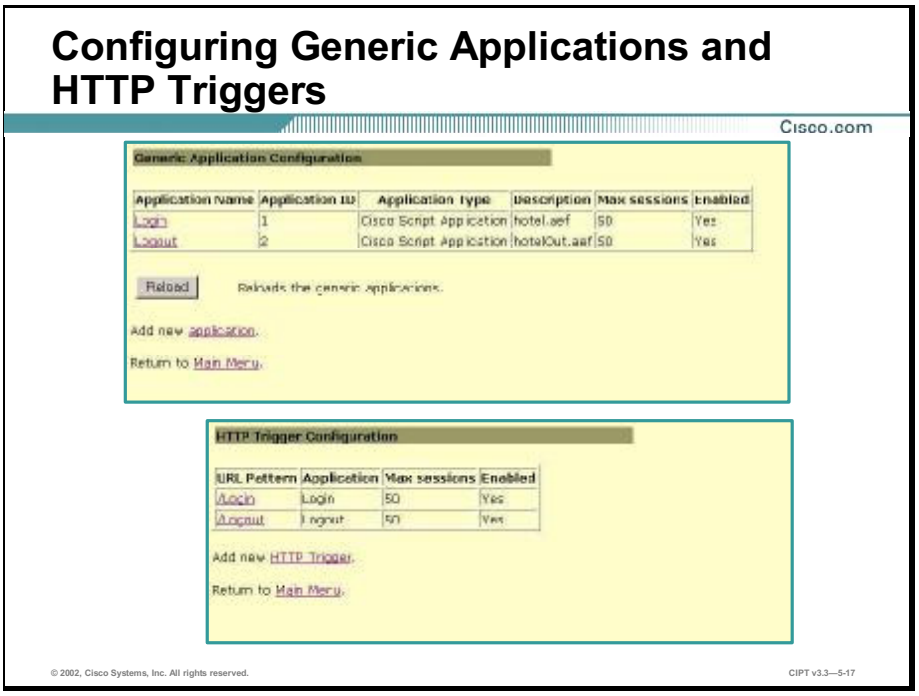


Configure the hostname or the IP address of the server where the LDAP directory exists. The simplest configuration is when the Application Engine resides on the same Cisco MCS server as CCM, and you are using the embedded DC-directory that comes with CCM. In this case, you can specify the "localhost," the hostname of the computer, or the IP address of the server where these three components are running.

With a more advanced configuration, DNS services exist in the network, the Application Engine is installed on a different Cisco MCS server than CCM, and you are using the enterprise LDAP directory for the computer.

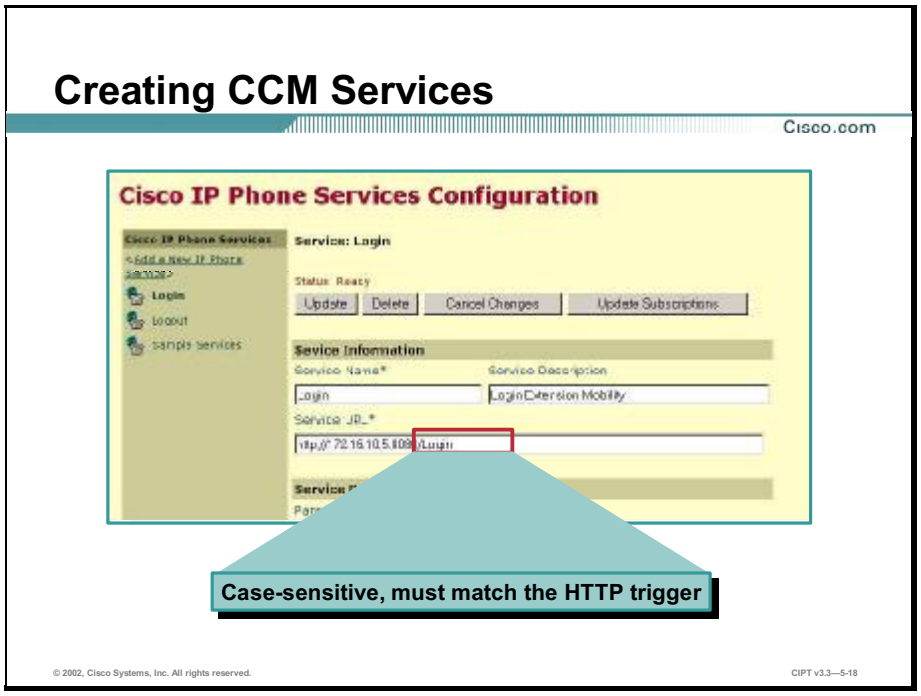
In any case, you must configure the Application Engine to know the location of the directory, the type of directory (Netscape, active directory, DC-Directory, or other directory), the TCP port number for connecting to the directory, the user base information, and the administrator username and password for accessing the directory.

Reference To access the Directory Configuration page, open Application Administration page at: http://<servername>/appadmin.
The <servername> is the hostname or IP address of the CRS server.



You must configure the generic login and logout applications and the HTTP triggers, because you will use them when configuring other services. For example, you use the HTTP triggers in the Cisco CallManager Administration page when configuring the Cisco IP Phone services, and you use the generic login and logout applications to access the hotel.aef and hotelOut.aef application scripts.

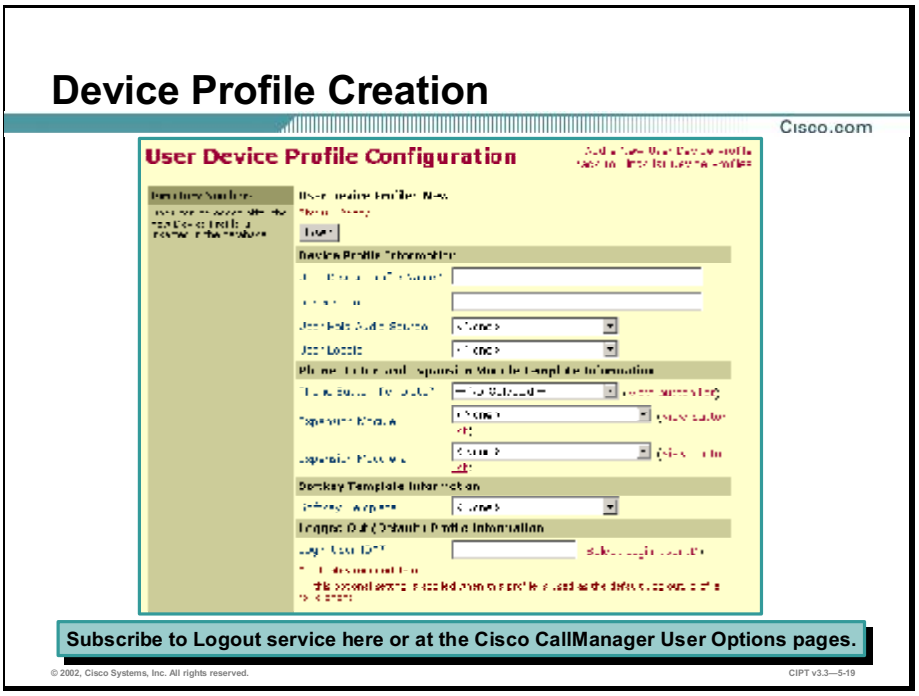
Note	The names of the .AEF scripts are case sensitive.



After configuring CRS, configure CCM. Start with configuring the Cisco IP Phone login and logout services.

Reference The service URL is:
http://<server_name>:8080/Login or http://<server_name>:8080/Logout.
Verify that the end of the URL matches the HTTP triggers configured on the CRS server.

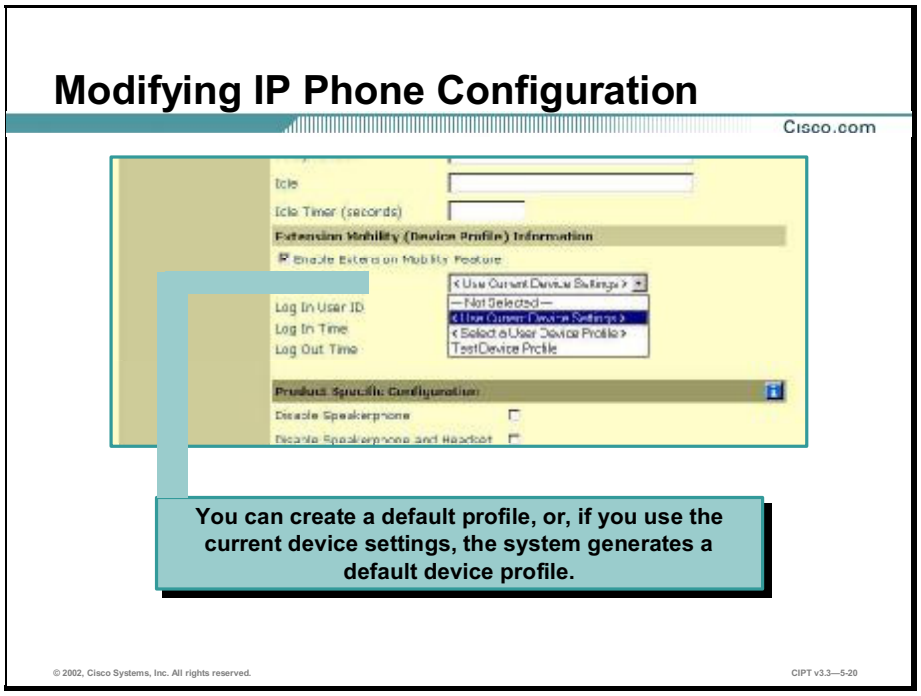
Ensure that every IP Phone that will allow Extension Mobility subscribes to the login service. Also, ensure that every device profile that can use Extension Mobility subscribes to the logout service.



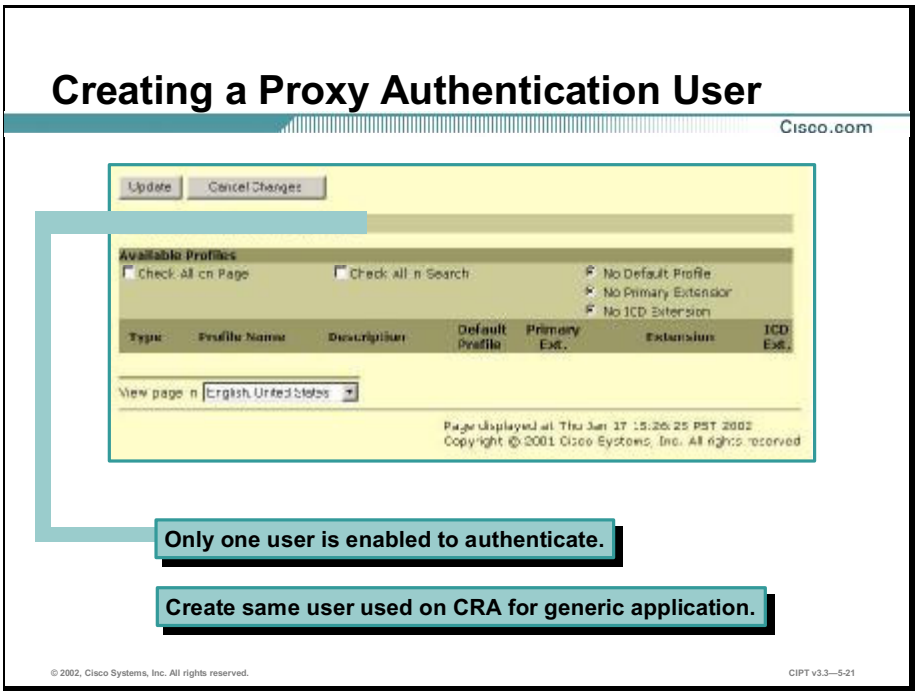
Configure a device profile for the user to log in to an IP Phone device. You can subscribe to the logout service, or you can leave it up to your users to subscribe to the logout service.

If the device profile does not subscribe to the logout service, the IP Phone device must wait for an automatic timed logout or another means of logging out.

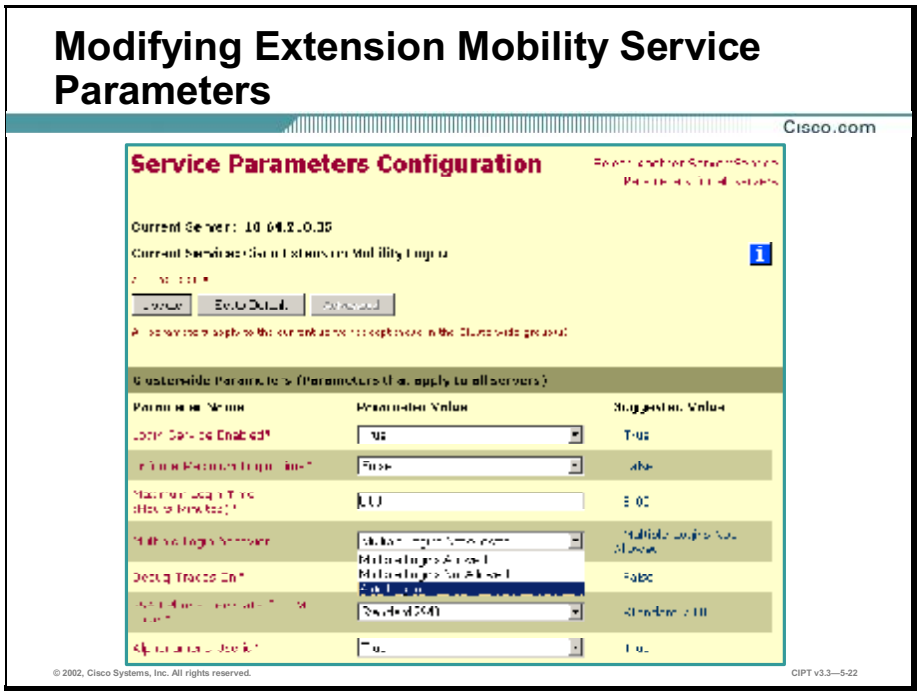
A device profile configuration is very similar to a telephone configuration in CCM. Once you configure the device profile, you must associate it to a user. The personal identification number (PIN) that you assign to the user is part of the information with which the user logs in.



The IP Phone device must have a logged-out profile to use as its default profile when no one is logged in to it. The logged-out profile can use the current device settings or a user device profile. Either way, verify that you have subscribed the logged-out profile for the IP Phone device to the login Cisco IP Phone service.



In CCM, you must configure and enable a user to authenticate with proxy rights for the users that will use the Extension Mobility feature. The username must match the user configured on the CRS server that you created when configuring the generic application.



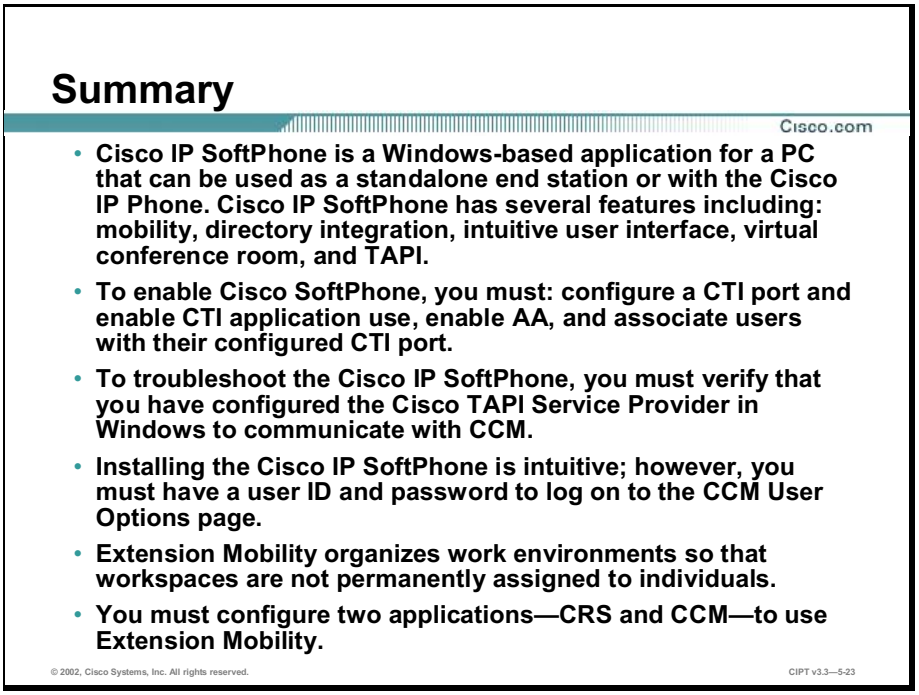
The figure shows the service parameters for the Extension Mobility service. The table defines the settings on the Service Parameters Configuration page.

Table: Service Parameters

Parameter	Description
Login Service Enabled	Choose **True** to enable the Extension Mobility system or **False** to disable the system.
Enforce Maximum Login Time	When True, this parameter will enforce a maximum login time. If False, no time limit is set on logins.
Maximum Login Time (Hours:Minutes)	This parameter is the maximum amount of time a user is allowed to log into a device. The maximum allowable value is 168:00, entered as HHH:MM. Note that :MM is also an acceptable format for durations under 1 hour. This parameter is ignored if the Maximum Login Time parameter is not enforced.
Multi Login Behavior	This parameter specifies the behavior for multiple attempted logins by the same user on different devices. The choices are to allow, not allow, and cause a previous login to automatically log out.
Debug Traces On	Forces Cisco CallManager Serviceability to record debug information for Extension Mobility functions.
7940 Telephone Template for EM Login	Allows you to specify the template used by the 7940 IP Phones for the Extension Mobility login.
Alphanumeric Userid	Choose **True** to allow CCM to accept alphanumeric Extension Mobility logins or **False** to force numeric logins only.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Cisco Voice over IP Integrated Applications lesson

References

For additional information, refer to these resources:

- *Cisco IP SoftPhone Administration and User Guides*: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/ip_7960/softphon
- *Configuring Cisco CallManager Extension Mobility*: http://www.cisco.com/univercd/cc/td/doc/product/voice/serv_fea/ext_serv/esgd03.htm

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which three of these are not features of the Cisco IP SoftPhone? (Choose three.)

A) It can function as a standalone IP Phone.

B) It can control hardware IP Phones.

C) It can integrate with LDAPv3 directories.

D) It has built-in VPN capabilities.

E) It automatically marks voice traffic with type of service (ToS) or class of service (CoS) of 5.

Q2) How many device weight units does Cisco IP SoftPhone consume?

A) 1

B) 3

C) 5

D) 20

E) 25

Q3) On the user configuration page, what is the check box that you must check to allow that user to use Cisco IP SoftPhone?

A) enable Cisco IP SoftPhone use

B) enable CTI port use

C) enable CTI application use

D) enable TAPI application use

Q4) Which of the following is NOT required when installing Cisco IP SoftPhone?

A) CTI port name

B) user ID

C) password

D) CCM IP addresses

Q5) When a user logs in to an IP Phone using the Extension Mobility feature, what is pushed to the IP Phone?

A) the IP Phone configuration that the user uses at the desk

B) an automatically generated device setting

C) an automatically generated device profile

D) the device profile associated with the user

Q6) To allow for extension mobility functionality, you must configure a user in CRS for the generic application. Which of the following functions should you configure the user for in CCM?

A) default device profile

B) default user for device profiles

C) authenticate proxy rights

D) authenticate device profile rights

Cisco Voice over IP Integrated Applications

Overview

This lesson provides a high-level overview of the Cisco Voice over IP (VoIP) applications that can be integrated into a Cisco IP telephony solution.

Importance

You can use many add-on applications within a Cisco IP telephony solution to provide value-added services and enhance the IP telephony experience of end users. Knowing how these applications fit into the Cisco IP telephony solution can provide insight into deployment considerations and foresight into addressing the legacy application concerns of customers.

Objectives

Upon completing this lesson, you will be able to:

- Define the Cisco Personal Assistant application
- Describe the Cisco Customer Response Solution 3.0
- Identify the Cisco IP Interactive Voice Response application
- Define the Cisco IP Auto Attendant application
- Describe the Cisco IP Integrated Contact Distribution system
- Identify the Cisco IP Contact Center application
- Describe the Cisco Conference Connection application
- Define the Cisco Unity application

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Basic knowledge of Internet applications, such as e-mail, fax, and Web browsers
- Basic knowledge of Cisco CallManager

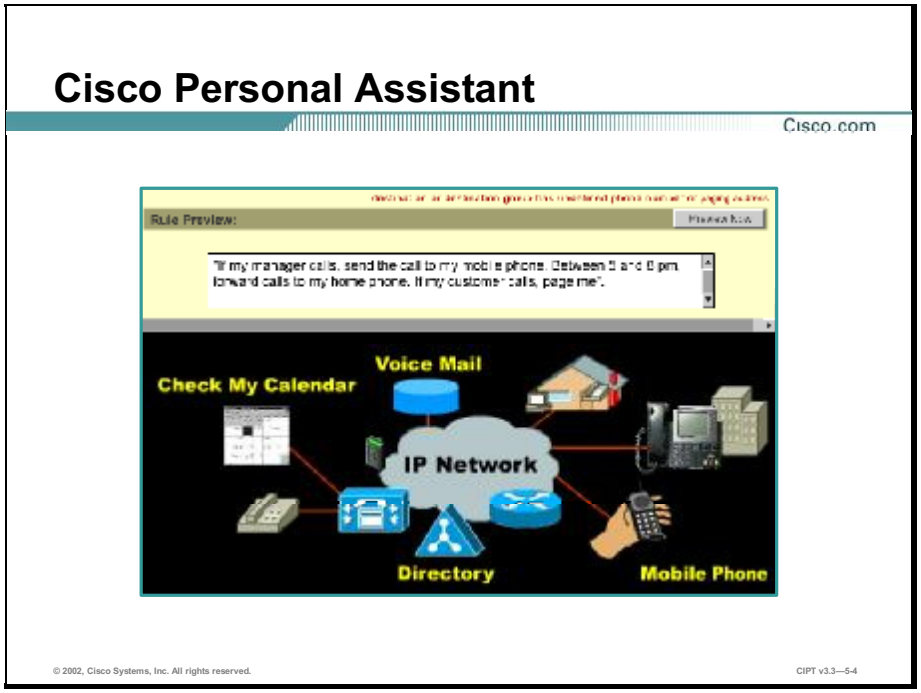
Outline

This lesson includes these topics:

- Overview
- Cisco Personal Assistant
- Cisco Customer Response Solution
- Cisco IP Interactive Voice Response
- Cisco IP Auto Attendant
- Cisco IP Integrated Contact Distribution
- Cisco IP Contact Center
- Cisco Conference Connection
- Cisco Unity
- Summary
- Lesson Review

Cisco Personal Assistant

This topic describes how Cisco Personal Assistant helps mobile workers manage communications and maximize productivity with personal call rules, speech recognition, and productivity services for IP Phones.



Personal Assistant can selectively handle incoming calls and assist individuals in placing outgoing calls. Personal Assistant interacts with Cisco CallManager (CCM) to intercept incoming calls to individual extensions. By intercepting these calls, Personal Assistant can redirect the calls based on user-defined rules. For example, you can configure a rule that instructs Personal Assistant to send all incoming calls straight to voice mail. Users will set up these rules through a web-based interface, and activate different sets of rules through the web interface. Users can also set up the rules by talking to Personal Assistant over the telephone.

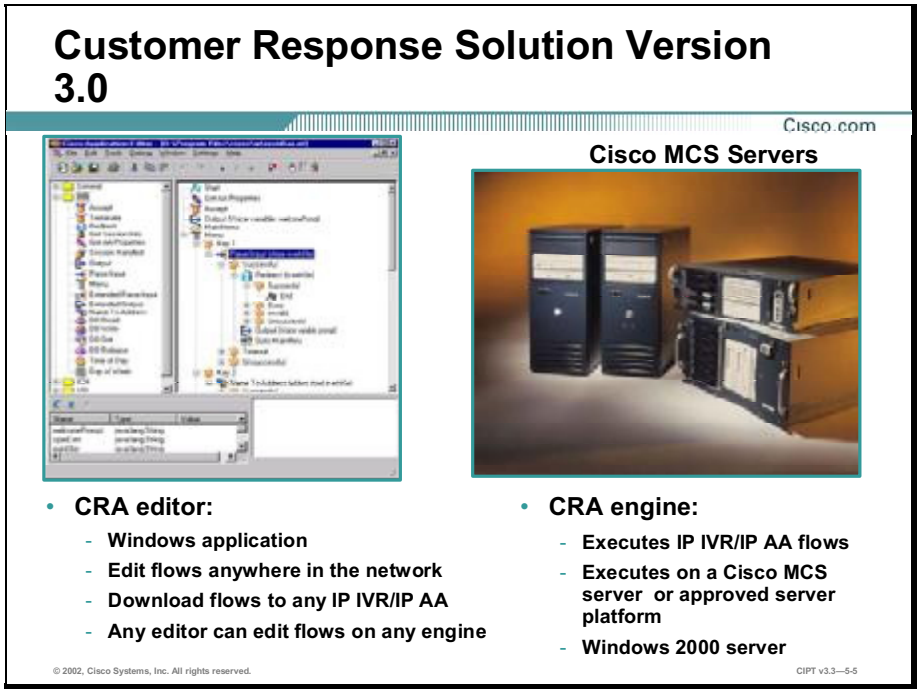
Although CCM does not require that you set up partitions, you must create partitions if you want to enable rule-based call routing and allow Personal Assistant to intercept user calls. Personal Assistant cannot intercept user calls if you do not configure partitions and calling search spaces. You can still use the speech features provided by Personal Assistant, such as dial-by-name and speech-enabled voice-mail access, to assist a user in placing calls. The table lists some of the features that Personal Assistant offers.

Table: Personal Assistant Features

Personal Assistant Features	Description
Rule-Based Call Routing	Personal Assistant can forward and screen incoming calls based on user-defined rules. Incoming calls can be handled according to caller ID, date and time of day, and the office hours, meeting schedules, vacations, and holidays of the user. Personal Assistant can also selectively route calls to other telephone numbers. Therefore, an incoming call to a desk telephone can be routed to a cell telephone or home telephone, based on the call routing rules that your users create.
Speech-Enabled Directory Dialing	Users can dial telephone numbers by speaking the name of the person to Personal Assistant. Personal Assistant obtains the telephone number from the corporate directory or personal address book. To use any speech-enabled feature, you must add a sufficient number of speech and license servers to your Personal Assistant installation.
Speech-Enabled Voice-Mail Browsing	Users can use voice commands to browse, listen to, and delete voice-mail messages.
Speech-Enabled Simple Ad Hoc Conferencing	Users can initiate conference calls by telling Personal Assistant to set up a conference call with the desired participants or groups.
Follow-Me Call Transferring	Users can tell Personal Assistant to use an alternate telephone number as their primary location for a specific time. Personal Assistant routes calls to the follow-me telephone. For example, a user could route calls to a hotel room telephone during a business trip.
Simple Automated Attendant for Dial by Name	You can set up a simple automated attendant to allow callers to reach people by saying their name rather than having to know their telephone number.
Support for Multiple Locales	You can support users or outside callers that speak different languages. Personal Assistant uses the language they select through the user web interface. If you create a Personal Assistant automated attendant, callers can switch between supported locales.

Cisco Customer Response Solution

This topic discusses the Cisco Customer Response Solution (CRS) 3.0, which provides Cisco IP Interactive Voice Response (IVR), Cisco IP Auto Attendant (AA), and Cisco IP Integrated Contact Distribution (ICD) functionality in a Cisco IP telephony environment.

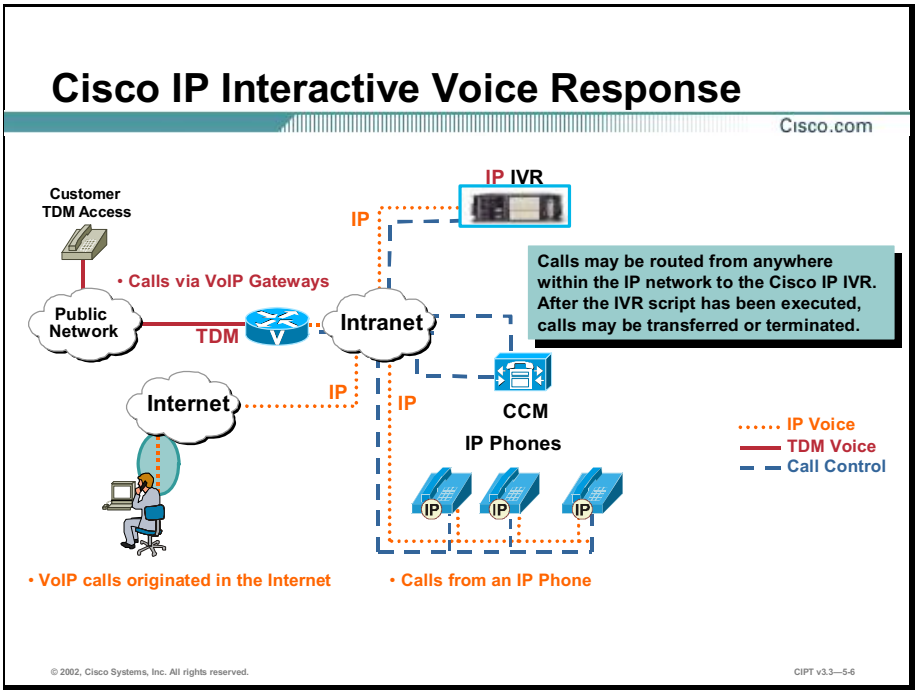


Cisco CRS 3.0 is designed to help you to enhance the efficiency of any contact center organization by simplifying business application integration, easing agent administration, increasing agent flexibility, and providing efficiency gains in network hosting. These features reduce business costs and improve customer response for the contact center. This single-server integrated platform includes the following applications: IVR, ICD, and Cisco IP Queue Manager (QM). Cisco IP QM is an option for an IP Contact Center (IPCC) that provides call treatment to calls in a queue.

CRS provides agent location independence, improves agent scalability, and enhances the features of an automatic call distributor (ACD), such as skills-based routing and priority queuing. The CRS solution is tightly integrated with CCM, and is a natural addition to any voice deployment that you will make across IP.

Cisco IP Interactive Voice Response

This topic discusses the Cisco IP IVR application, which provides interactive voice prompts and call automation.

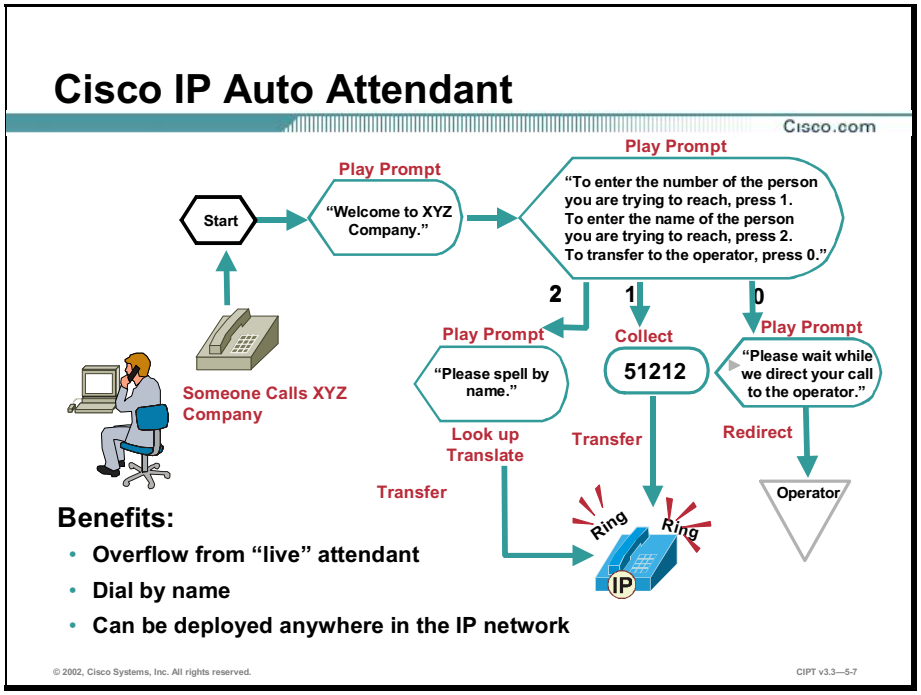


Cisco IP IVR is an IP-powered IVR solution that provides you with an open, extensible, and feature-rich foundation for the creation and delivery of IVR solutions via Internet technology. Cisco IP IVR helps you automate the handling of calls by independently interacting with users. The IP IVR processes user commands to facilitate command response features, such as access to checking account information or user-directed call routing. The IP IVR also performs "prompt and collect" functions to obtain user data, such as passwords or account identification. Additionally, you can use the Cisco IP IVR to extract and parse web-based content and present this data to customers via a telephony interface, thus facilitating the delivery of web-maintained information to a voice media user. When you deploy Cisco architecture, the Cisco IP IVR product is constructed specifically to exploit the power of your IP-based communications.

An IP IVR flow is similar in concept to legacy IVR scripts. However, flows are more powerful because they facilitate the concepts of binding and managing multiple media types in a single customer interaction solution. The Cisco IP IVR feature set is accomplished by processing Voice over IP (VoIP) streams routed to the IP IVR by CCM, and thus requires no Digital Signal Processor (DSP) cards in the IP IVR itself. To connect the IP IVR, CCM, and the Public Switched Telephone Network (PSTN), only one time-division multiplexing (TDM) interface is required—the VoIP gateway interface to the PSTN. The IP-originated calls require no TDM infrastructure; thus, the Cisco IP IVR can terminate Internet- or intranet-generated VoIP calls directly.

Cisco IP Auto Attendant

This topic discusses the Cisco IP AA that comes with the Cisco IP IVR.



Cisco IP AA is an automated attendant flow included with the IP IVR that provides you with simple call-answering and call-forwarding services. Cisco IP AA provides you with both dial-by-extension and telephone keypad mapping for dial-by-name.

The Cisco IP AA includes the following functionality:

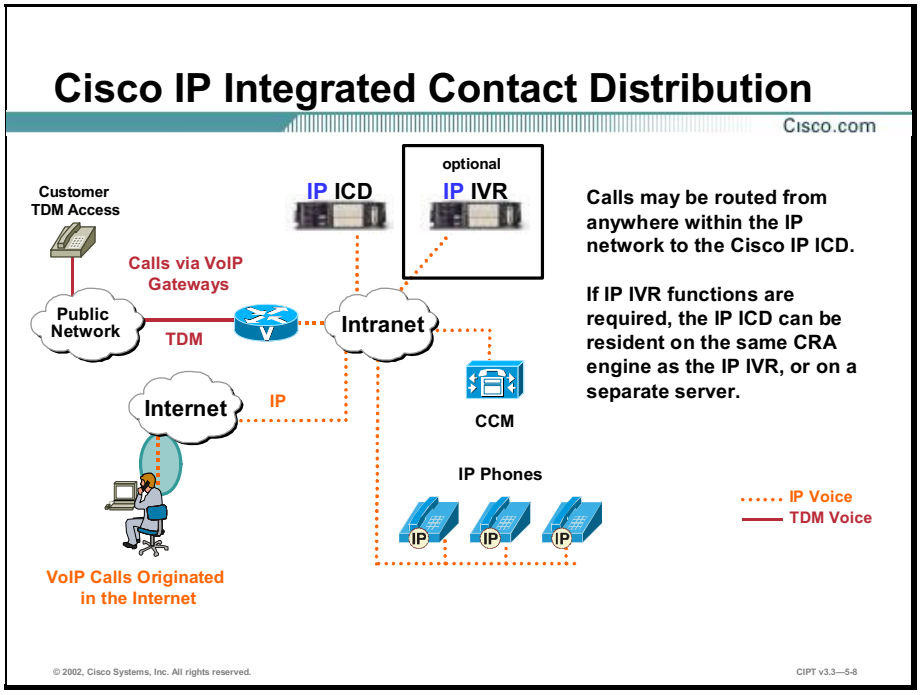
- Answers a call.
- Plays a user-configurable Welcome prompt.
- Plays a Main menu prompt asking the user to perform one of three actions:
  - Press "0" for the operator.
  - Press "1" to enter an extension number.
  - Press "2" to spell by name.

When your caller chooses to enter letters (option 2), the system compares the letters entered with the available extensions. If one matches, the system prompts the user for confirmation of the name, and transfers the call to the primary extension of that user. With more than one match, the system prompts the user to select the correct extension. When there are too many matches, the system prompts the user to enter more characters. After your caller has specified

the destination, the system transfers the call. When the line is busy or not in service, the system informs the user accordingly and replays the Main menu prompt.

Cisco IP Integrated Contact Distribution

This topic discusses Cisco IP Integrated Contact Distribution (ICD), an inexpensive, easy-to-install, and easy-to-use ACD for enterprise organizations.



Cisco IP ICD is one in a series of solutions built on the Cisco CRS 3.0 platform, which is the Cisco Systems open platform for customer response applications. You can use Cisco IP ICD to seamlessly integrate with all other customer response applications, including Cisco IP IVR and Cisco IP AA.

The key benefits of the Cisco IP ICD include:

- A low-cost, entry-level ACD that is easy to install, administer, and use
- Multimedia (voice, data, and web) access when used with Cisco IP IVR
- Complete customization tools for call flow scripts
- Supports seamless integration with any current or future Cisco customer response application

This table shows the key features of the Cisco IP ICD.

Table: Key Features

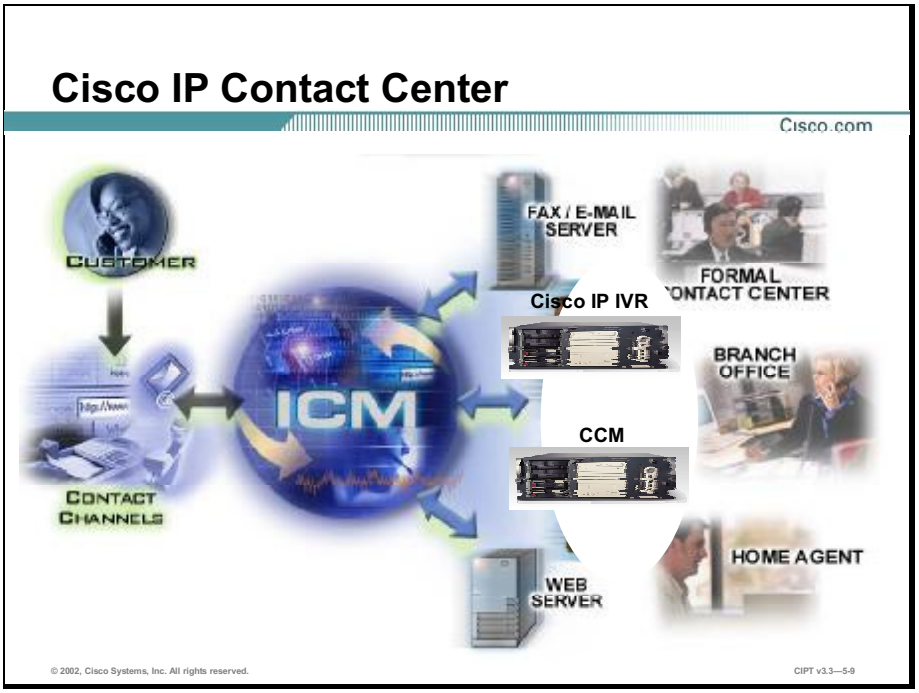
Features	Definition
Performance and Capacity	Cisco IP ICD supports up to 48 agents in as many as 48 groups. IP ICD simultaneously supports 48 calls in progress and 48 calls in the queue.
Incoming Call Queuing	When one or more agents are available, Cisco IP ICD immediately connects the caller to an agent. When an agent is not available, Cisco IP ICD queues the call in a *first in first out* queue. Up to 48 calls can be queued at one time.
Incoming Call Routing	Cisco IP ICD can service multiple groups from a single CCM route point. In addition, you can create multiple CCM route points (for example, one route point per group for group-specific handling).
ACD	The following ACD distribution algorithms are available: ■ Weighted linear (hunt group) ■ Circular (distribution group) ■ Longest available (the agent who has been available the longest)
Welcome Messages	You can create your own welcome messages or use a predefined Cisco message.
Queue Messages and Behavior	You can create your own queuing messages and in-queue behavior or use a predefined Cisco message and behavior.
Groups and Agents	You can create up to 48 groups with as many as 48 agents per group. Cisco IP ICD supports a maximum of 48 agents across all defined groups.
Agent Desktop	Agents use a simple Java application to log on or off, to announce their availability for call distribution, and to display their current status (for example, "in-session").
Cisco IP Phones	Cisco IP ICD supports the use of the Cisco 7900 Series IP Phones and the Cisco IP SoftPhone as an agent telephone. Agent functions and status are accessed and displayed separately on the PC agent desktop application.
Real-Time Reports	On-demand and automatically cycling real-time reports for system, group, and agent status are available.
Historical Reports	Historical reporting packages are available from partners at an additional cost.
Deployment	You can deploy Cisco IP ICD with any supported Cisco deployment model, including centralized call processing with remote agents.
Integrated Installation and Operations, Administration, and Maintenance	Cisco CRAs [1] feature one-click installation and common operations, administration, and maintenance.

Custom Call Flow Creation	You can use any CRA editor to create custom call flows. CRA Engine—Runtime environment that executes Cisco IP ICD flows. CRA Editor Step Folders—Collections of call processing steps used to create flows for a particular function (for example, perform call processing and communicate with databases. These are libraries of JavaBeans that provide the programming constructs, called "steps," for the Cisco IP ICD flows. Flow repository (LDAP[2] directory)—for storage of all flows and configuration data for a Cisco IP ICD. Reports—Provide real-time flow execution statistics. In addition, Cisco partners can provide historical reporting at an additional cost.

1. CRA = Customer Response Application
2. LDAP = Lightweight Directory Access Protocol

Cisco IP Contact Center

This topic describes how the Cisco IPCC delivers intelligent call routing, network-to-desktop computer telephony integration (CTI), and multimedia contact management to contact center agents over an IP network.



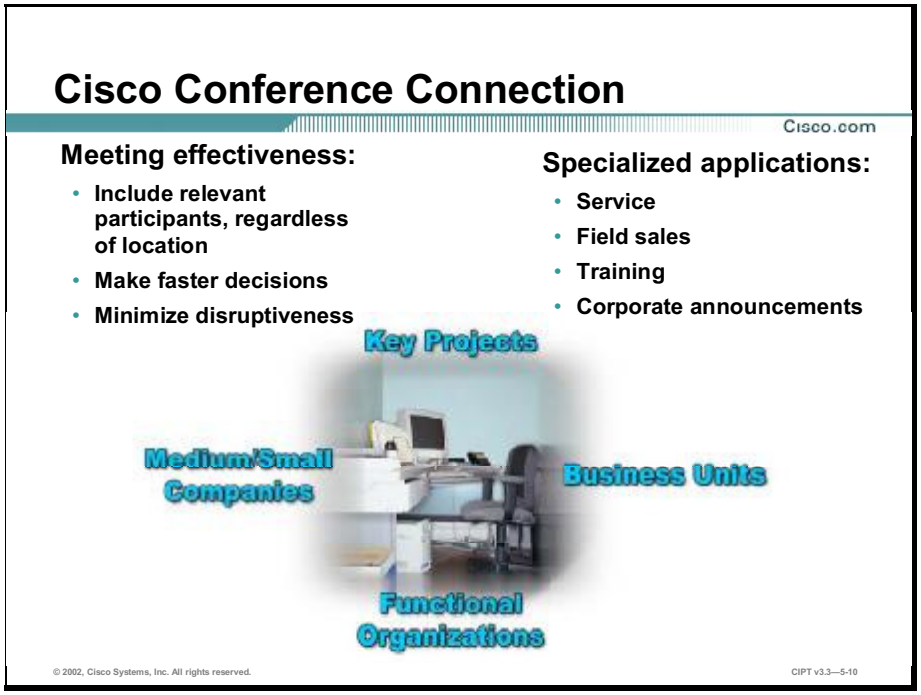
By combining Cisco IP telephony and contact-center solutions, the Cisco IPCC delivers an integrated suite of proven products that enables agents using Cisco IP Phones to receive both TDM and VoIP calls. This combination enables you to rapidly deploy a distributed contact center infrastructure to support your global e-sales and e-service initiatives. Because the IPCC was intended for integration with legacy call-center platforms and networks, it provides a migration path to IP-based customer contact while taking advantage of previous technology investments.

The Cisco IPCC enables you to have an integrated suite of proven products—including Cisco Intelligent Contact Manager (ICM), CCM, Cisco IP IVR, Cisco VoIP gateways and Cisco IP Phones—that combine Cisco IP telephony and contact center solutions. Specific capabilities that you will have include: intelligent call routing, multi-channel functionality for an ACD, IVR, call queuing, and consolidated reporting. The IPCC helps you integrate with legacy call center platforms and networks, enabling your organization to continue to leverage its investment in legacy systems while providing a smooth migration path to an IP infrastructure.

The Cisco IPCC is designed for implementation in both single-site and multisite contact centers. It utilizes the existing customer IP network, allowing customers to leverage their WAN infrastructure, lower administrative expenses, and extend the boundaries of their contact center enterprise to include branch offices, home agents, and knowledge workers.

Cisco Conference Connection

This topic discusses the Cisco Conference Connection application.



The Cisco Conference Connection is an audio conference server that you can use for scheduled conferences. The conference owner can use an intuitive web interface to schedule calls. The conference participants simply dial into a single number and enter a meeting ID; they are then connected into the conference. You may also configure Cisco IP Phone services so that users can enter a conference at the touch of a button from their IP Phone.

Cisco Conference Connection supports up to 100 ports. You may divide ports among any number of participants. You can assign all ports in one large conference call or multiple calls, or smaller conferences may be planned. Cisco Conference Connection is IP-based and allows you to integrate with CCM. Your conference participants need not be IP-based, because conference connectivity is universal.

You can synchronize Cisco Conference Connection user accounts from CCM, which uses LDAP directory profiles. Your user profile administration is through the CCM User Preferences interface. You may modify Guest, User, and Administrator settings through Cisco Conference Connection.

You can enable Cisco Conference Connection to operate on a Cisco Media Convergence Server (MCS), either the Cisco MCS 7825-800 or the Cisco MCS 7835-1000. The Cisco MCS 7825-800 supports up to 60 conference ports. The Cisco MCS 7835-1000 supports up to 100 conference ports. The Cisco MCS server is dedicated to the Cisco Conference Connection application. Neither CCM, nor any other applications may be coresident on the Cisco MCS server running Cisco Conference Connection.

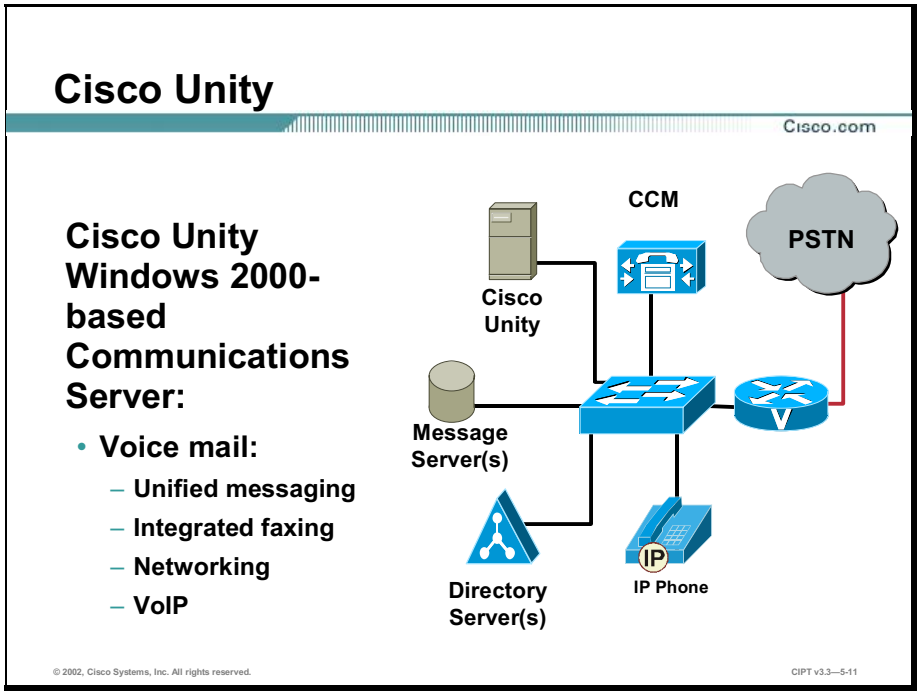
Capacity planning is important during the implementation design. The required capacity is very application-dependent. However, it is important that you plan for peak utilization periods. You must encourage your customers to look at their business environments to determine capacity requirements. Within Cisco, plans are based on a requirement of one conference port for every twenty telephones. This can include the telephones that are not assigned to individuals; such as lobby telephones, lab telephones, and conference room telephones.

When you use audio conferencing, it increases the effectiveness of meetings. Participants in a conference may reside in distant locations, or they may be traveling. Location is no longer a barrier to effective meetings in an organization. Cisco Conference Connection reduces travel time, costs, and provides for better, faster decisions. You can do this and still minimize the disruption to individual schedules. Even within a single corporate campus, participant efficiency increases by allowing them to frequently participate in meetings from their desk.

Historically, audio conference servers were found only in large organizations. Cisco Conference Connection builds on a new model, as audio conferencing becomes an easily available resource for your business units, functional organizations, key projects, and medium or small businesses.

Cisco Unity

This topic highlights Cisco Unity, which is the Cisco unified messaging application.



The Cisco Unity server is based on Microsoft Windows 2000 and uses Exchange 2000 as its message store. It offers unified messaging, integrated faxing (using a third-party faxing product), and networking which allows you to interconnect Cisco Unity servers in branch offices across the country. Cisco Unity allows you to seamlessly integrate with CCM. Cisco Unity will also support many other legacy PBX systems as well.

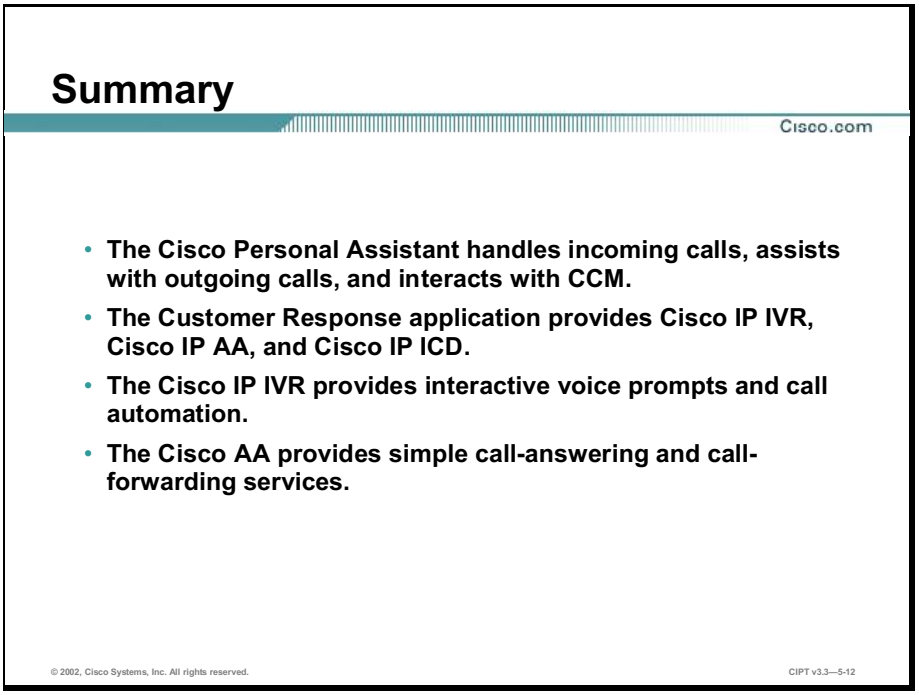
Each Cisco unified messaging solution consists of three main components: the Cisco Unity server, the directory server, and the message store. These three components can run on the same server, or you can distribute them across two or more servers. The Cisco open architecture provides maximum flexibility in the choice of components. In particular, the open architecture provides an integration platform that facilitates multivendor “best of class” solutions.

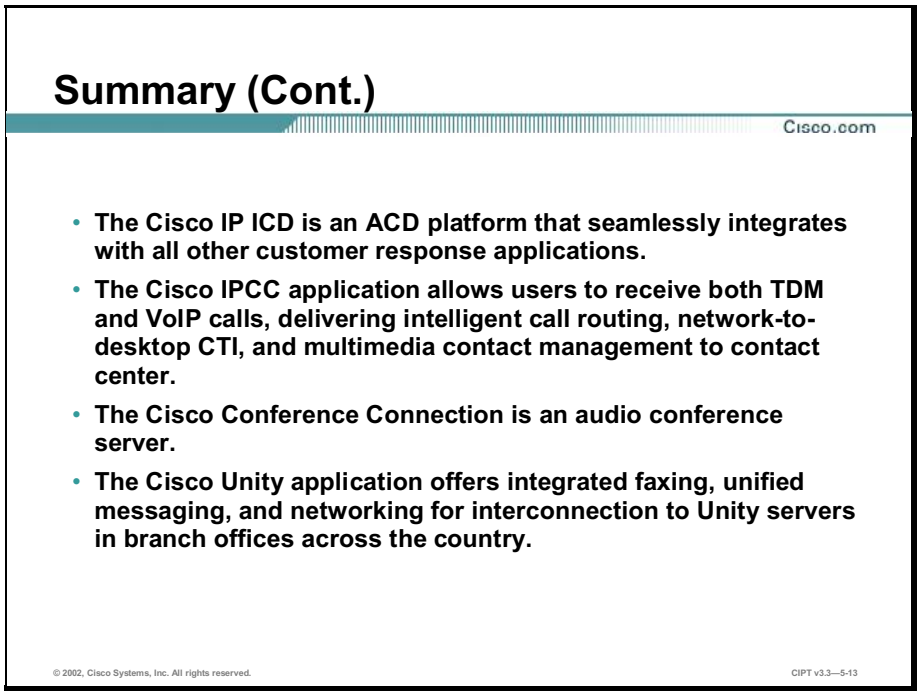
The Cisco unified messaging architecture is a three-tiered architecture where e-mail, voice mail, and fax mail is a single system supporting these different modes. In a unified messaging architecture, the user has a single inbox. All message types are delivered to that inbox. The user may access their inbox via an IP Phone, a handheld terminal, a full-featured PC, or a purpose-built interface (such as a pager-like device).

For example, the voice message left by a sender can either be listened to over the telephone, or the subscriber can go to an electronic media. This would include a Web browser or e-mail client. You could listen to the message over the multimedia device on a PC, laptop, or personal digital assistant (PDA). The user can listen to e-mail messages (once available via a graphical e-mail client interface only) via the telephone with text-to-speech translation.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Manageability and Monitoring Tools module

References

For additional information, refer to these resources:

- Personal Assistant: http://www.cisco.com/warp/public/cc/pd/undo/persasst/
- Contact Center: http://www.cisco.com/warp/public/779/largeent/avvid/products/callctr.html
- Integrated Contact Distribution: http://www.cisco.com/warp/public/cc/pd/unco/ipicd/

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) _____ must be configured if you want to enable rule-based call routing and allow Personal Assistant to intercept calls.

A) partitions

B) gateways

C) gatekeepers

D) all of the above

Q2) Which of the following is NOT part of CRS?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Q3) Which of these generates interactive voice prompts and provides call automation?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Q4) Which of these provides simple call-answering and call-forwarding services?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Q5) Which of these is an inexpensive, easy-to-install, and easy-to-use ACD?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Q6) In IPCC, which of these products provides the ACD functionality?

A) IP IVR

B) ICM

C) CCM

D) CRS

Q7) Which of these best describes the Cisco Conference Connection?

A) an audio conference server for scheduled conferences

B) an audio conference server to mix voice streams

C) an audio conference module for scheduled conferences

D) an audio conference module to mix voice streams

Q8) When using Cisco Unity for unified messaging, which three of these applications are part of the unified messaging solution? (Choose three.)

A) voice mail

B) e-mail

C) fax

D) paging

6

Manageability and Monitoring Tools

Overview

This module describes the Cisco CallManager (CCM) manageability and monitoring tools. Upon completing this module, you will be able to:

- Install and use the Cisco Bulk Administration Tool
- Use the internal server monitoring tools

Outline

The module contains these lessons:

- Cisco Bulk Administration Tool
- Internal Server Tools

Cisco Bulk Administration Tool

Overview

The Cisco Bulk Administration Tool (BAT) is a plug-in application for Cisco CallManager (CCM). It allows you to add, update, or delete a large number of telephones, users, Cisco VG200 gateways and ports, and Cisco Catalyst 6000 24-port Foreign Exchange Station (FXS) analog interface modules in the Cisco CCM database. BAT automates the process to increase the speed of these operations.

Importance

This lesson provides information about efficiently configuring and updating the CCM database in large systems.

Objectives

Upon completing this lesson, you will be able to:

- Identify the features of the BAT application
- Install the BAT application
- Create an IP Phone template to use with BAT
- Create CSV files
- Update the IP Phone and line settings with BAT
- Configure and install the Tool for Auto Registered Phone Support

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Configuration of a single Cisco IP Phone device
- Cisco CallManager Administration basics

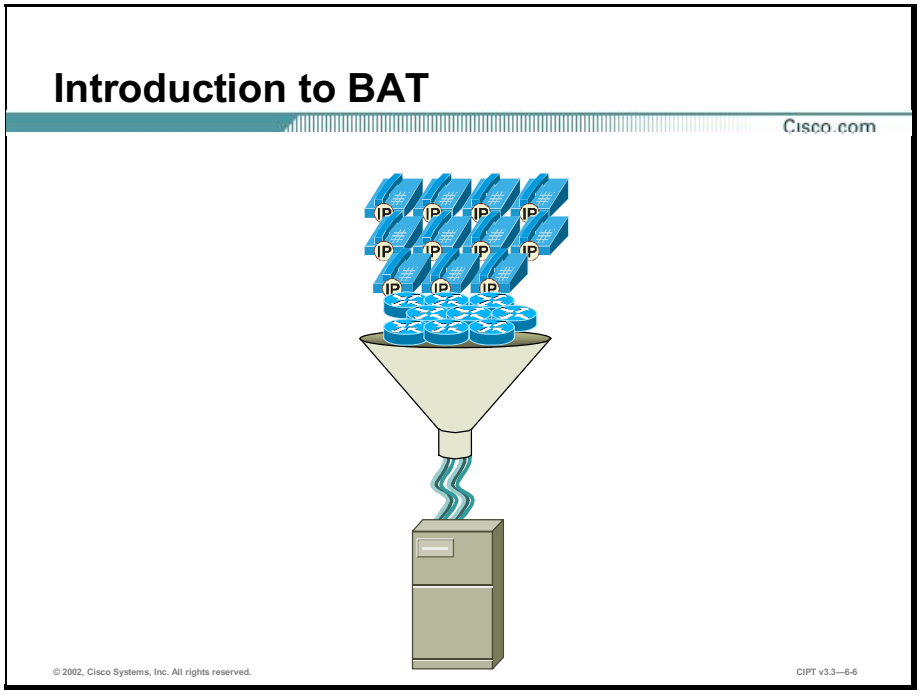
Outline

This lesson includes these topics:

- Overview
- Introduction to the Cisco Bulk Administration Tool
- BAT Installation
- Configuring BAT Templates
- Creating CSV Files
- Adding and Updating with BAT
- Tool for Auto Registered Phone Support
- Summary
- Lesson Review

Introduction to the Cisco Bulk Administration Tool

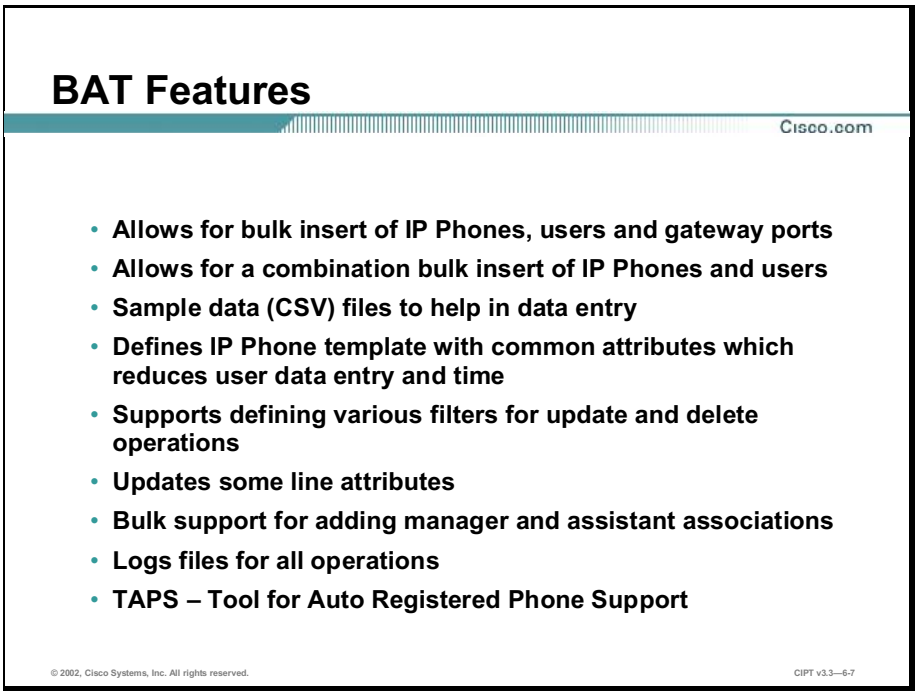
This topic examines the Cisco Bulk Administration Tool (BAT), a product that enables the Cisco CallManager (CCM) administrator to complete the bulk adds, updates, and deletions for IP Phones.



BAT includes the devices, lines, associated users, and the bulk administration for gateways, including the Cisco VG200 gateways and Cisco Catalyst 6000 Foreign Exchange Station (FXS) ports configuration.

BAT provides an optional application, the Tool for Auto Registered Phone Support (TAPS), which retrieves the predefined configuration for auto-registered telephones.

Reference For additional information on BAT or TAPS, search for BAT from the main Search menu at: http://www.cisco.com.



BAT and TAPS use approximately 16 MB of disk space for the applications and online documentation. This figure displays other BAT and TAPS features.

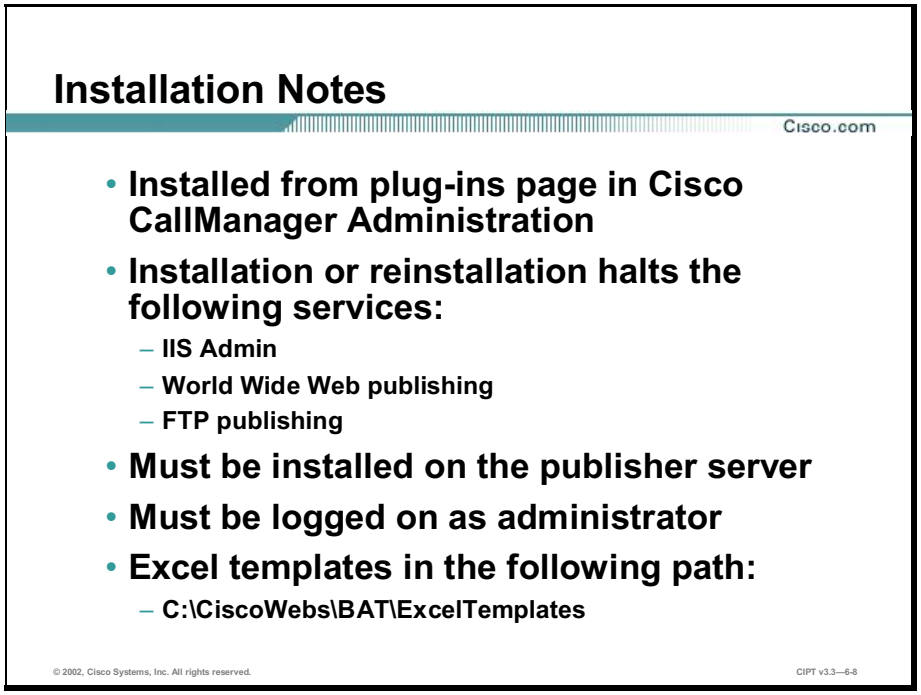
Only CCM system administrators require access to BAT, but end users can use TAPS with permission from a system administrator to register new IP Phones.

Cisco Systems based the BAT utility, which is a web-based application, on the Cisco CallManager Administration interface. You can access BAT from Cisco CallManager Administration or the Application menu.

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

BAT Installation

This topic examines the BAT installation steps.



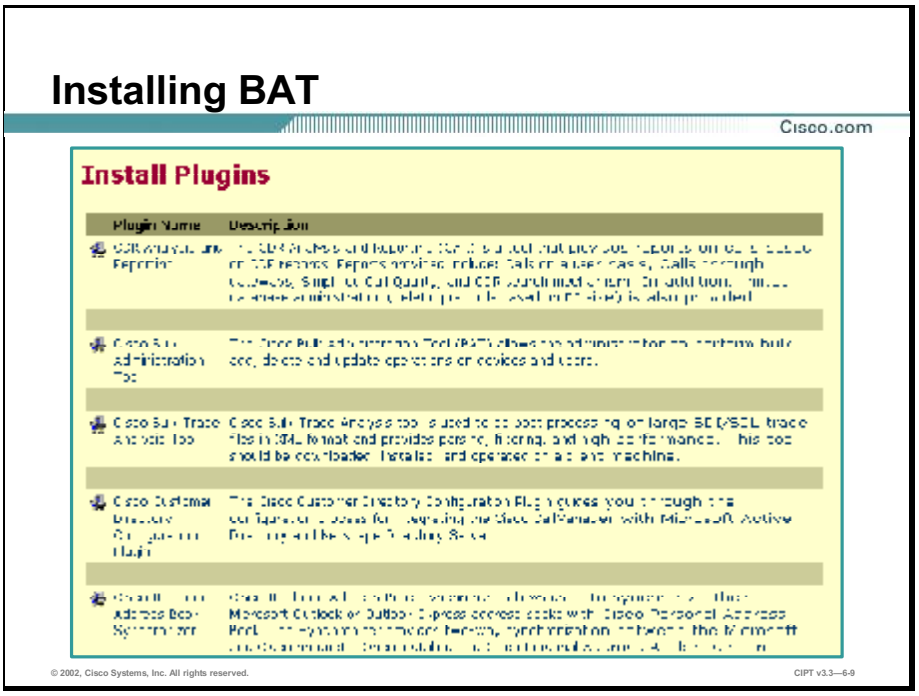
BAT must be installed on the same server as the publisher database for CCM. During BAT installation, the setup program stops the following services:

- Internet Information Server (IIS) Admin
- World Wide Web publishing
- File Transfer Protocol (FTP) publishing

These services automatically restart when the installation is complete.

The BAT installation process includes BAT Excel template files, located in the BAT\Excel template folder. Copy these templates to the Microsoft Excel template folder and access them from that location.

Installing BAT



These steps describe the BAT installation process:

Step 1 Using the administrator privileges, log on to the system running the publisher database for CCM.

Step 2 Choose **Applications**>**Install Plugins**.
The Install Plugins window displays, as shown here.

Step 3 Locate BAT, and double-click the **Setup** icon.
A standard Windows dialog box appears.

Step 4 Determine whether to copy the BAT install executable to the system or run it from the current location.

Caution Upgrading to BAT 4.4 from 4.0 through 4.3 migrates templates, while upgrading from BAT 3.0(3) does not.

Step 5 Choose **Next** when the Welcome window appears.
The Current Settings: window displays.

Step 6 Choose **Next** to install to the default location, C:\CiscoWebs\BAT.

Note You cannot change this path.

The Start Copying Files window displays, and Setup begins copying files. Setup allows you to install TAPS. TAPS updates the MAC addresses for IP Phones that were bulk-added in BAT using dummy MAC addresses. When you dial into a TAPS directory number, the IP Phone configuration downloads to the IP Phone, and the MAC address updates in CCM.

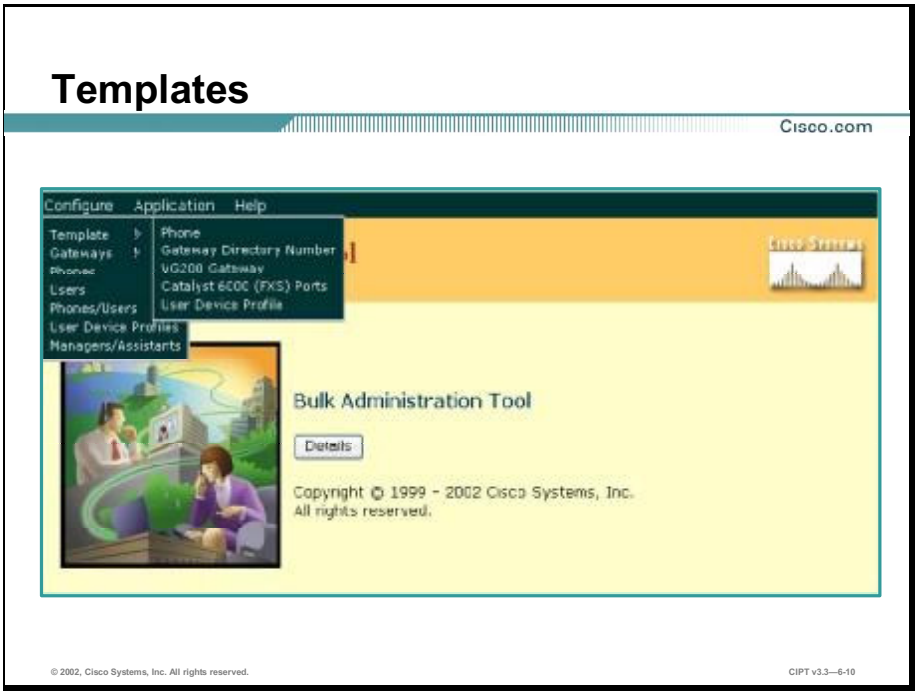
Step 7 To install TAPS, click **Yes**.
If you want to skip the TAPS installation, click **No**.

The Setup Complete window displays to show that you have successfully installed BAT. If you chose to install TAPS, you must complete that installation by installing and uploading TAPS to the Cisco CRS server.

Step 8 Click **Finish** to close Setup.

Configuring BAT Templates

This topic discusses inserting, updating, and deleting templates for BAT.



BAT has five templates that can be used to insert, update, or delete telephones, gateways, gateway directory numbers, Catalyst 6000 ports, and user device profiles, as shown here.

Note	The BAT templates are different than the Phone Button templates for Cisco CallManager Administration.

- **Phone template:** The IP Phone template and Comma Separated Value (CSV) files work together in bulk transactions. You can create a template that has all of the common features of an IP Phone group, such as model and device pool. The system stores these templates, so you can reuse them for future bulk transactions.

  The CSV file stores the details for each individual IP Phone, such as the MAC address and description. Because you customize CSV files for each bulk transaction, you are less likely to reuse them.

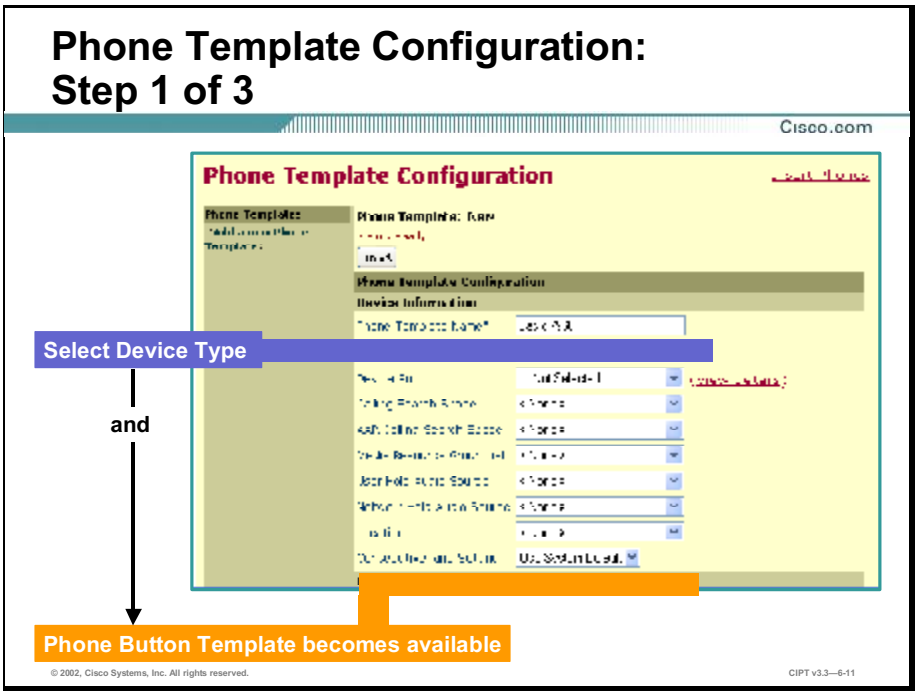
  Because you cannot create new configuration settings in BAT, verify that the IP Phone options, such as Device Pool, Location, Calling Search Space, and Button Template have already been configured in Cisco CallManager Administration before creating the template. To create an IP Phone template, enter the required telephone settings, and add the appropriate number of lines to each IP Phone.

- **Cisco VG200 Gateway template:** The gateway template and CSV file work together in bulk transactions. You can create a template that has the common settings for all of the gateways to be added in that batch, such as the module in slot and type of endpoint identifier. BAT stores these templates, so that they are reusable for other batches. The CSV file stores the details for each individual port, such as directory number, description of port, and partition.

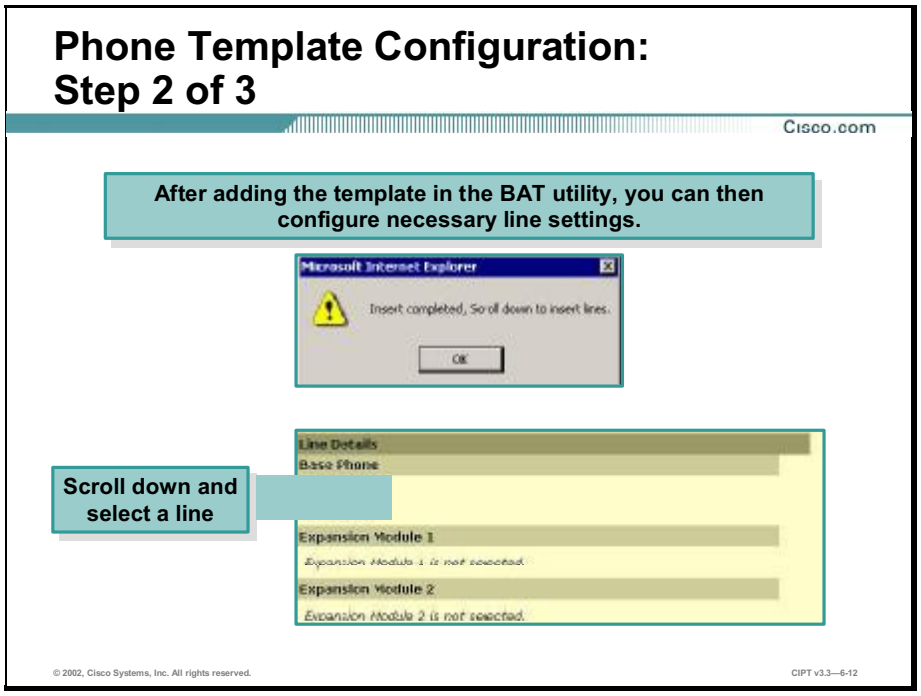
- **Cisco Catalyst 6000 (FXS) Ports template:** The port template and CSV files work together in bulk transactions. You can create a template with common analog details for all of the ports in that batch, such as the port direction and port level. The system stores these templates, so they are reusable for other batches. The CSV file stores the details for each individual port, such as the gateway, MAC address, port number, directory number for this port, and partition.

- **Gateway Directory Number template:** The template and CSV files work together in bulk transactions. You can create a template that has common directory number details, such as partition and calling search space. The system stores these templates, so that they are reusable for other batches. The CSV file stores the details for each individual port, such as the gateway, MAC address, port number, directory number for this port, and the partition. BAT has four templates for inserting, updating, or deleting IP Phones, gateways, and gateway directory numbers.

- **User Device Profile:** A device profile comprises the set of services or features associated with a particular device. A user device profile contains device information for a user logging into a device. The BAT utility allows the administrator to associate the softkey templates with the necessary devices and the line configuration for the user device profile.



The first step in configuring an IP Phone template is to choose an IP Phone (device) type from the Phone Template Configuration page, 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. After you have configured the initial template information, click **Insert** to add the template to the BAT utility.



After configuring the initial template settings, you can modify specific line configurations. Choose a line to configure, and a new configuration page 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 Excel spreadsheet.

Phone Template Configuration: Step 3 of 3

Cisco.com

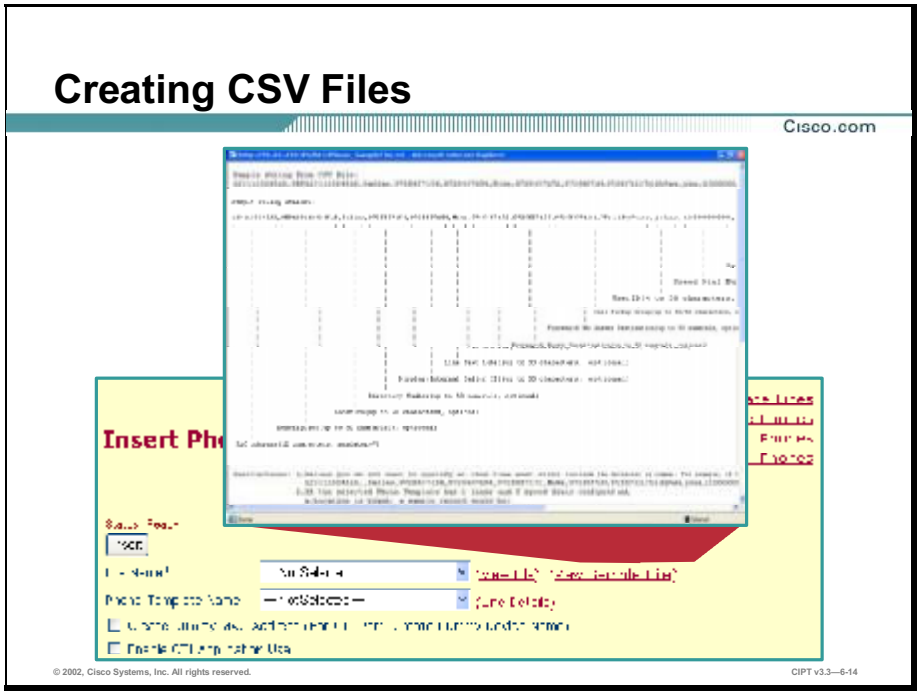
Configure Line Settings for template

CIPT v3.3—6-13

Configure the line settings by choosing options from the menus and then clicking **Insert and Close**, as shown here.

Creating CSV Files

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

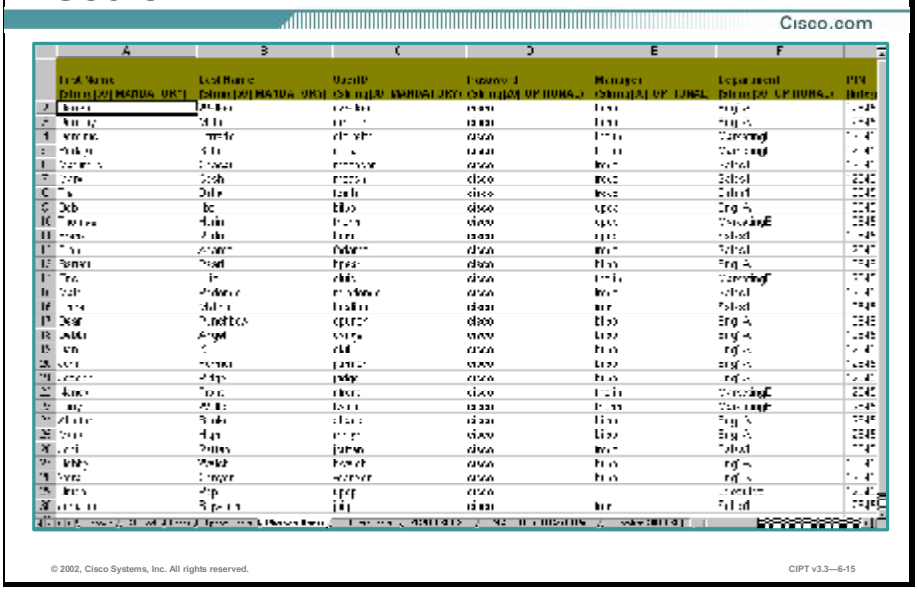


Before adding IP Phones using BAT, you must create an IP Phone template and a CSV file. A CSV file contains the values in a table as a series of ASCII text lines organized so that a comma separates the column values, and each row starts a new line.

Before configuring an IP Phone template, you must have the following values as defined in Cisco CallManager Administration:

- Device pool
- Location
- Calling search space
- Phone Button template

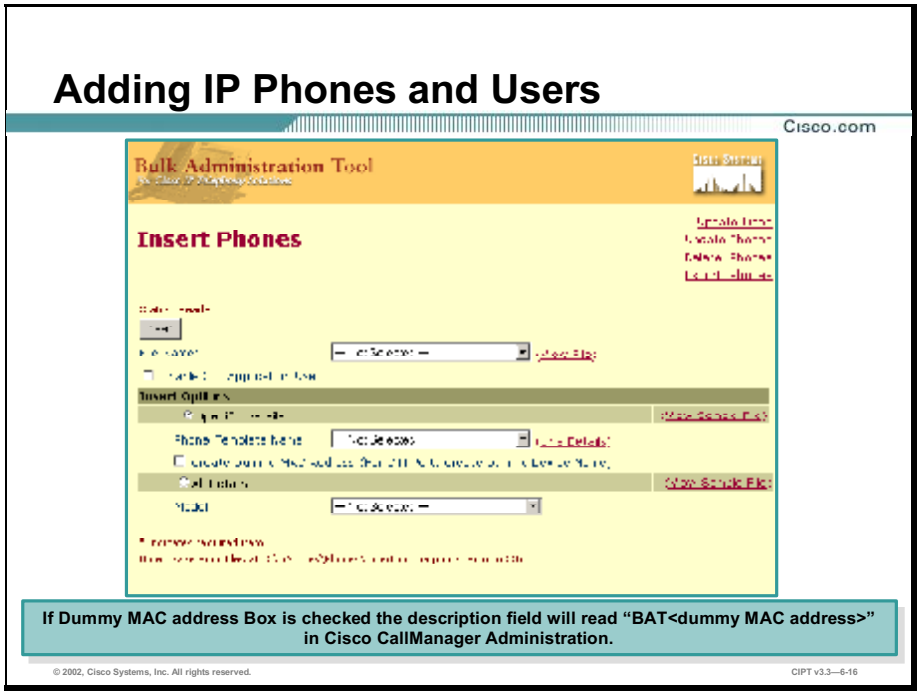
BAT Excel Template: IP Phone and Users



This figure shows the BAT.xlt Microsoft Excel template. You can find this template in the directory C:\CiscoWebs\BAT\ExcelTemplate\ on the publisher database server. Double-click **BAT.xlt**. When prompted, click **Enable Macros**. After entering the data into the Excel template, click **Export To BAT Format** to create the CSV file.

Adding and Updating with BAT

This topic describes how to use the BAT tool to add and update telephones and users.



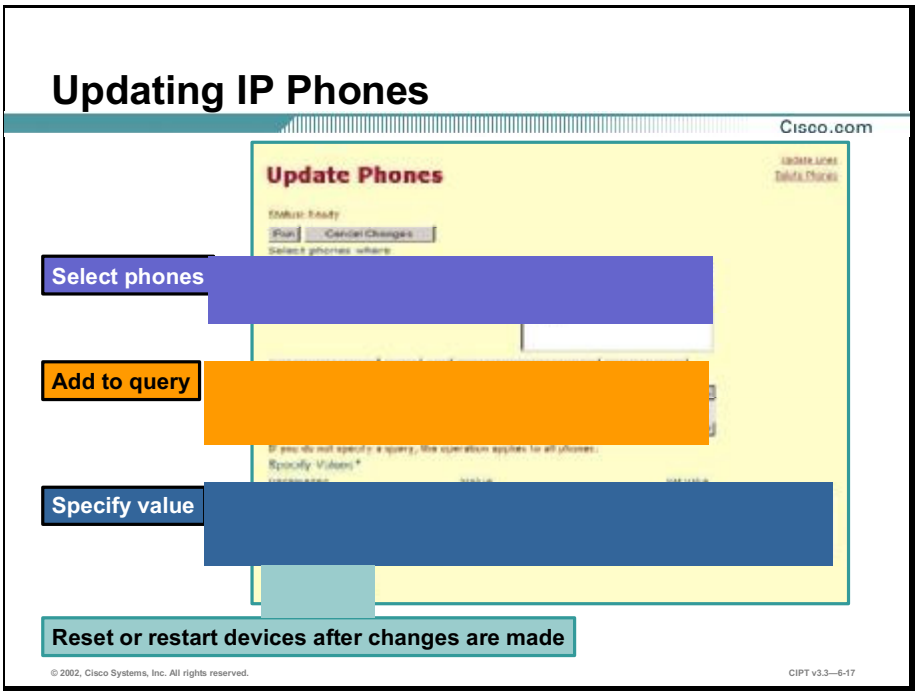
This figure shows the BAT input window for IP Phones and users, using a single CSV file. Use this procedure to insert IP Phones or users to the CCM database in bulk:

Step 1 Create a BAT IP Phone template to define common values for a set of IP telephony devices.

Step 2 Create a CSV file to define individual values for each device that you want to add.

Note	Cisco recommends that you create the CSV file using the Excel file, BAT.xlt.

Step 3 Insert the BAT template and CSV file to add the IP Phones, devices, or user combination to the CCM database.



This figure shows the Update Phones input window. To update the IP Phones, use this procedure:

Step 1 Select the IP Phones you wish to update.

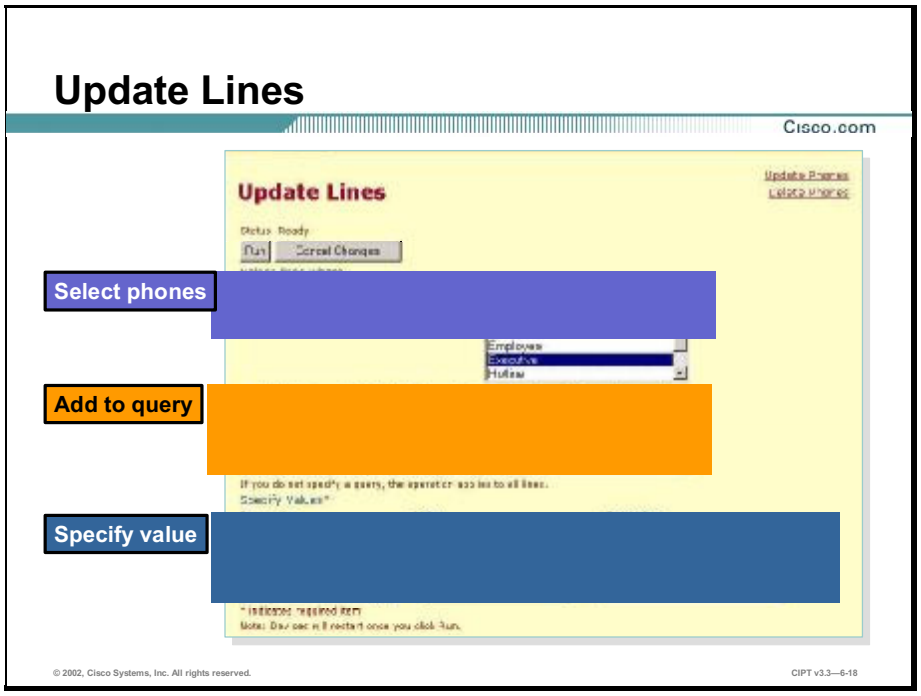
Step 2 Add the IP Phones to the query box.

Step 3 Specify the values to be updated within CCM.

Step 4 Reset the IP Phones through CCM, or plug them in and apply power.

Note	If you created dummy MAC addresses in the CSV file, you can update the IP Phones using the TAPS utility, which is discussed later in this lesson.

Step 5 To check the status of your insertion, read the status line, located above the Insert button.
If the status bar indicates that you inserted User Datagram Protocol (UDP) successfully, you are finished. If the status bar indicates a failure, click **View Latest Log File** to display a window that will help you to determine where the operation failed.



You can use BAT to update line attributes for user device profiles in bulk, as shown here. You can access the Update Lines window from the Insert User Device Profiles window. The following information will guide you through accessing updating lines:

Step 1 Launch BAT.

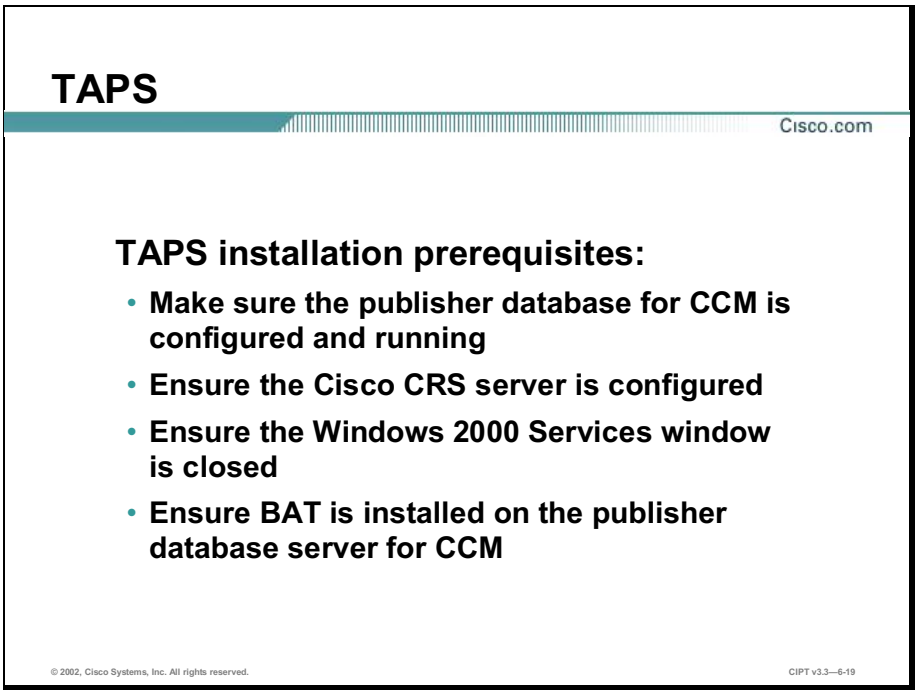
Step 2 Select **Configure** > **User Device Profile**.

Step 3 Click the **Update Lines** link.
The Update Lines window appears.

Step 4 Select the IP Phones that you wish to update the lines on, define the query, and specify the values to change.

Tool for Auto Registered Phone Support

This topic describes how to install and configure Tool for Auto Registered Phone Support (TAPS).



TAPS requires a two-part installation. The first part is the BAT installation, where you have the choice of installing TAPS with BAT on the publisher server. The second part is to install the Cisco Customer Response Solution (CRS) server and upload TAPS to this server.

These prerequisites apply to the TAPS installation for BAT:

- Ensure that the publisher database for CCM is configured and running.
  The publisher database can reside on its own server or on the same server as CCM.
- Ensure that the Cisco CRS server is configured.
- Ensure that the Windows 2000 Services window is closed.
- Ensure that BAT is installed on the publisher database server for CCM.

The following procedure lists the TAPS installation steps:

Step 1 Follow the steps for installing BAT; choose **Yes** to install TAPS.
The system copies all TAPS files onto the server running the publisher database.

Step 2 Log on, with administrator privileges, to the system running the publisher database for CCM.

Step 3 Choose **Applications**>**Install Plugins**.
The Install Plugins window displays.

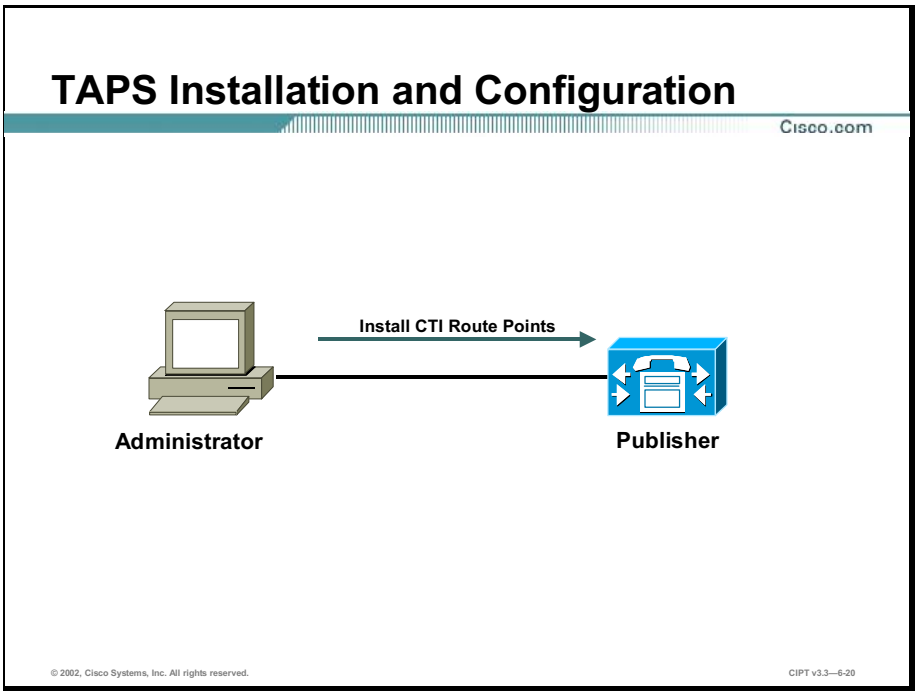
Step 4 Locate TAPS, and double-click the **Setup** icon.
A standard Windows dialog box appears.

Step 5 Determine whether you want to copy the TAPS install executable to your system or run it from the current location.

Step 6 Enter the primary CCM server IP address on the machine where BAT is installed, and click **Next** to continue.

Step 7 Follow the window prompts to complete the installation.
The final configuration is to upload TAPS to the Cisco CRS server.

Note The CCM Help files provide additional information on uploading TAPS to the Cisco CRS.



You must configure TAPS by adding a computer telphony integration (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 decribes how to configure TAPS in Cisco CallManager Administration:

Note	To use TAPS, verify that auto-registration is enabled in CCM.

Step 1 Create a CTI route point and assign it a unique directory number.

Step 2 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 3 Create one or more CTI ports with consecutive directory numbers.

Note	You can create CTI ports in BAT or Cisco CallManager Administration.

Step 4 Create a user.
The TAPS route point and ports should be in the users control devices list.

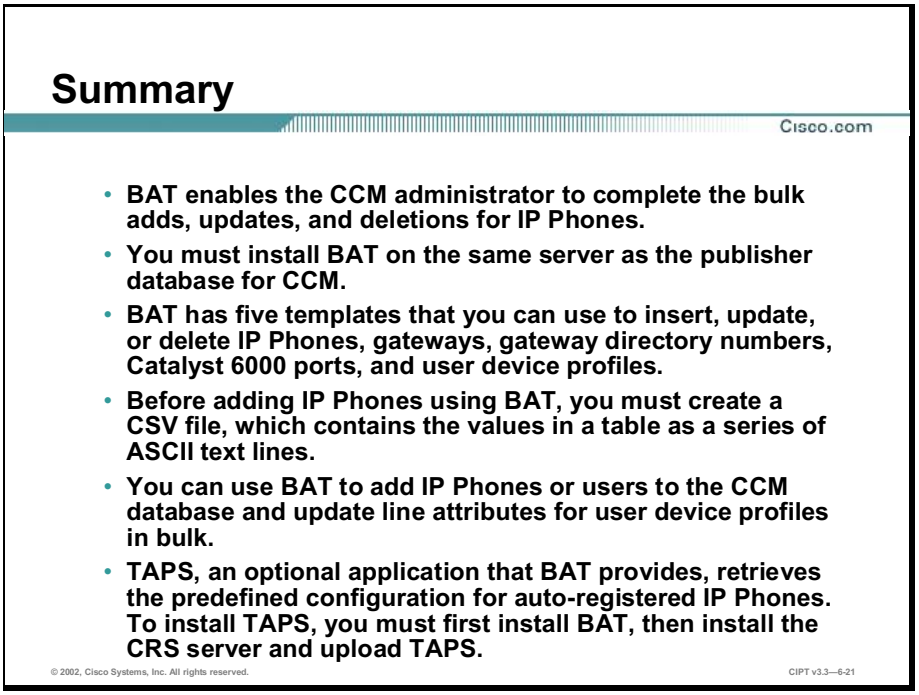
Note	TAPS supports a maximum number of sessions equal to the number of CTI ports configured for TAPS.

Step 5 Create an auto-registration partition and/or calling search space to prevent IP Phones that have auto-registered from dialing any directory number other than the number that is assigned to the TAPS CTI route point.

Restricting access to this directory number ensures that users download the proper configuration information for their IP Phones.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Internal Server Tools lesson

References

For additional information, refer to these resources:

- Cisco website:
  http://www.cisco.com
- *Configuring the BAT*:
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_configuration_guide09186a00800b7587.html

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of these tools allows you to complete bulk adds, updates, and deletions?

A) TAPS

B) BAT

C) CRA

D) CDR

Q2) Which server must have BAT installed on it?

A) publisher server

B) subscriber server

C) primary server

D) secondary server

Q3) What must you do before you are able to select the IP Phone Button template for the IP Phone template configuration?

A) select the number of lines to configure

B) select the line number to configures

C) select the device type to configure

D) select the device pool of the IP Phone

Q4) Which of these files is necessary to create BAT templates in Excel?

A) BAT.xlt

B) BAT.xls

C) BAT.csv

D) BAT.avr

Q5) Which of these items should you use to check the status of your insertion process?

A) view latest log file

B) status line

C) Event Viewer

D) CDR Records

Q6) Which two items must be installed for TAPS to function properly? (Choose two.)

A) CRS

B) BAT on the publisher server

C) plug-ins

D) Extension Mobility

Internal Server Tools

Overview

You must maintain the Cisco CallManager (CCM) operation to monitor the network for problems. This lesson will teach you the basic tools that identify problems with the CCM operation. You will learn about Data Connection Directory (DC-Directory) as well as the Cisco embedded directory and local Lightweight Directory Access Protocol (LDAP) directory containers. You will also learn about several command-line tools and monitoring devices that Cisco Systems provides for troubleshooting voice and data networks.

Importance

It is often possible to use the tools inherent in the Windows 2000 system to identify and isolate problems on the server, dealing with either configuration or operation. Because you can access the CCM server through Telnet on a limited basis, command-line tools are very useful. When web access is possible, the Cisco Admin Serviceability Tool (AST) provides web-page access to real-time monitoring functions, allowing you to remotely troubleshoot or monitor an existing environment.

Objectives

Upon completing this lesson, you will be able to:

- Describe how the Microsoft Event Viewer and Performance monitor tools for Windows 2000 aid in identifying problems with CCM operation
- Describe the tools inherent in Microsoft Structured Query Language for solving problems with database replication and monitoring
- Use component version information for customer support
- Use the various command-line tools available for troubleshooting
- Use the Cisco CallManager Serviceability tool to troubleshoot system problems
- Describe and list the characteristics of the Cisco Real-Time Monitoring Tool

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- Basic configuration of CCM
- Windows 2000 server

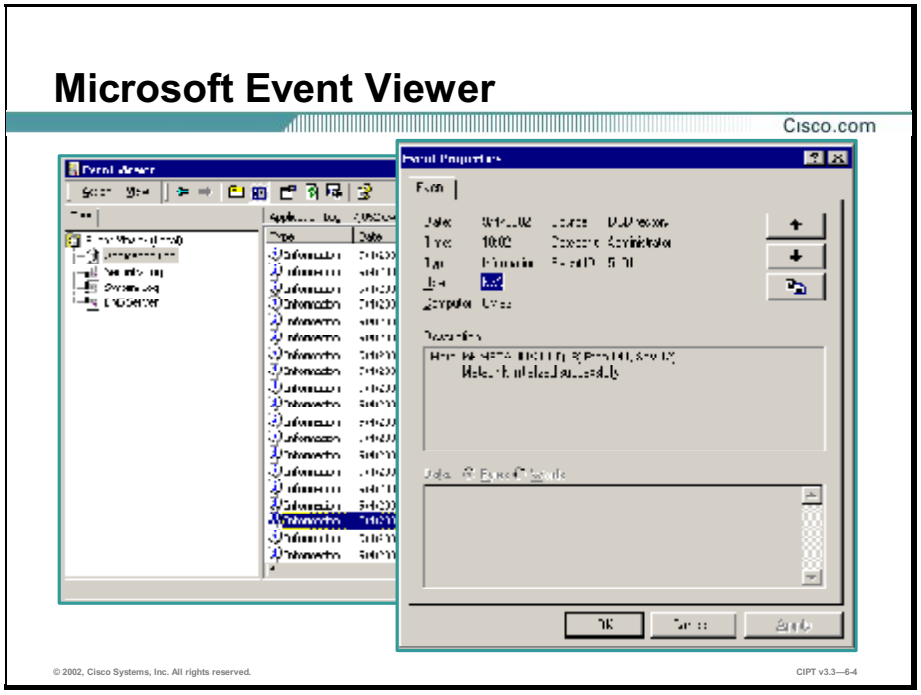
Outline

This lesson includes these topics:

- Overview
- Windows 2000 Tools and Accounts
- Database Services
- CCM Component Versions
- Command-Line Tools
- Cisco CallManager Serviceability
- Real-Time Monitoring Tool
- Summary
- Lesson Review

Windows 2000 Tools and Accounts

This topic describes the Microsoft Event Viewer and Performance monitor tools, which enable you to identify problems with Cisco CallManager (CCM) operations.



Microsoft Event Viewer can help you identify problems at the system level. Use Event Viewer to look for events regarding a specific gateway, such as registration or unregistration, to pinpoint the problem.

Log types

The Event Viewer log types include:

- **Application logs**: Contain events logged by applications or programs, such as CCM.
- **System logs:** Will report events logged by the Windows 2000 system components, such as the failure of an operating system component or driver.
- **Security logs:** Holds information records regarding security events. (CCM does not report events in this log.)

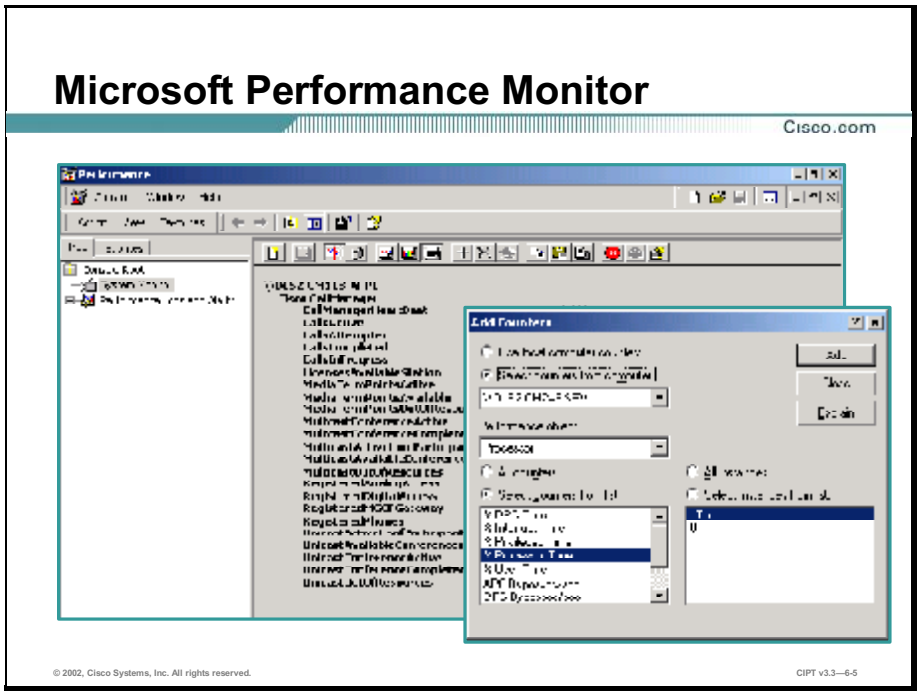
Event types

The Event Viewer event types include:

- **Error:** An indicator of a problem, such as the loss of data or failure to initialize properly.

- **Warning:** An event that might indicate a problem or a future problem, such as when a service is stopped or started, which is not necessarily an error.

- **Information:** System information messages, which may include host names, the version of the database in use, or startup success.



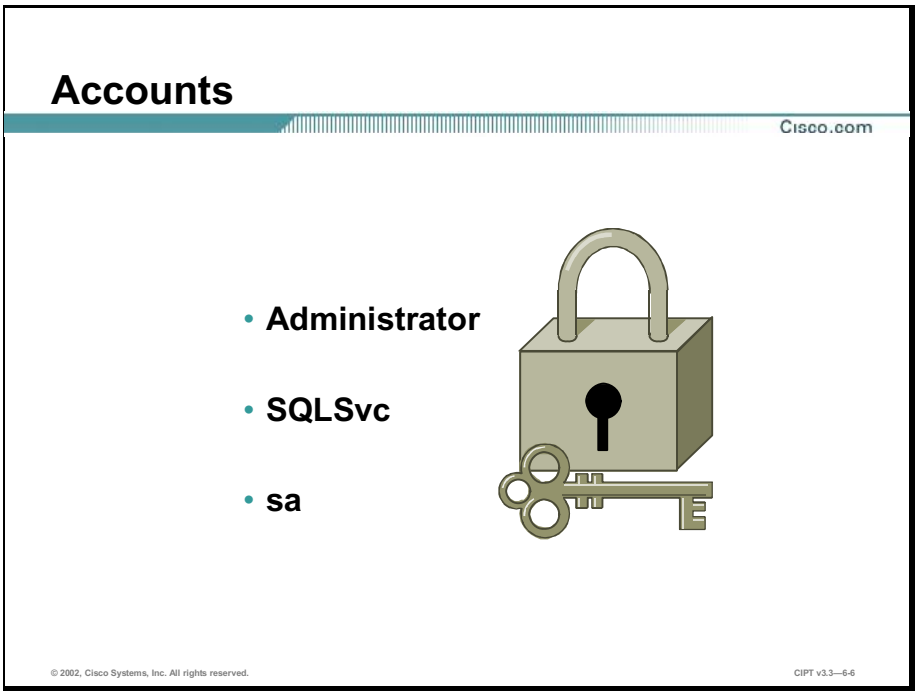
Microsoft Performance monitor is a Windows 2000 server application that displays the activities and status of a CCM system. Performance monitor reports both general and specific information in real time. You can use the Windows 2000 Performance monitor to collect and display system and device statistics for any CCM installation. This administrative tool allows you to gain a full understanding of a system without studying the operation of each component.

Microsoft Performance monitor, like the Cisco Admin Serviceability Tool (AST), monitors and logs resource counters from the CCM nodes in the network and displays the counters in real time. Performance monitor can collect data from multiple systems at once and store it in a single log file. The monitor can then export this logged file into a tab separated value (TSV), or into a Comma Separated Value (CSV) file, which you can view in most spreadsheet applications.

Note You must enable Statistics in CCM for the Performance monitor to collect data.

You must customize the Performance monitor to view the parameters related to CCM that you wish to monitor by choosing the objects, counters, and instances to include.

Within Performance monitor, you enable alarms to report certain value thresholds. For example, you can set the number of telephone devices active on the CCM to a particular level. If the number of devices exceeds that level, the monitor sends an alert to the administrator or the person in charge to inform them of the situation.



This list describes administration accounts and how to use the accounts in the CCM operation:

- **Administrator:** This is the default Windows NT administration account. CCM does not use this account for communication between servers. The password for this account can be different on all servers if you do not use it to access the Web Admin.

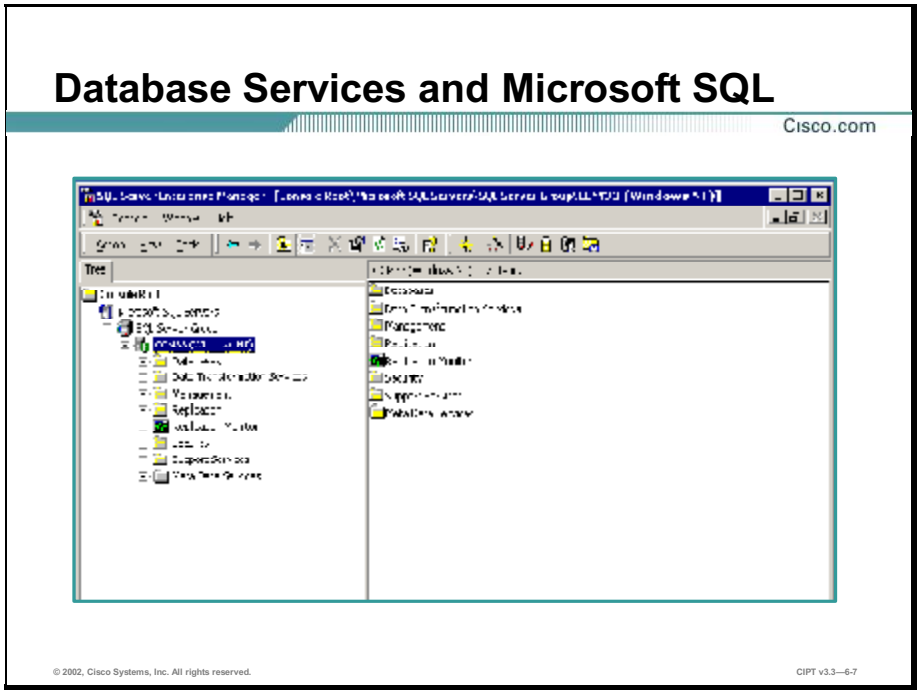
- **SQLSvc:** This account is the core account used for server-to-server interaction by the CCM system. To replicate this account, the account password must be the same on every machine in the cluster.

- **Sa:** This is the default Microsoft Structured Query Language (SQL) Server administration account. Most Microsoft SQL Server administrators use this account for system tasks only, such as installation and migration.

The account used to access the Web Admin should have an identical password and administrative privileges on each machine in the cluster. This condition supports the Control Center web page and allows the Internet Information Server (IIS) to impersonate the user to the other servers through a technique called Passive Authentication. Passive Authentication is also the authentication used for intracluster CCM replications.

Database Services

This topic describes the Microsoft SQL tools that are used to solve problems with database replication and monitoring.

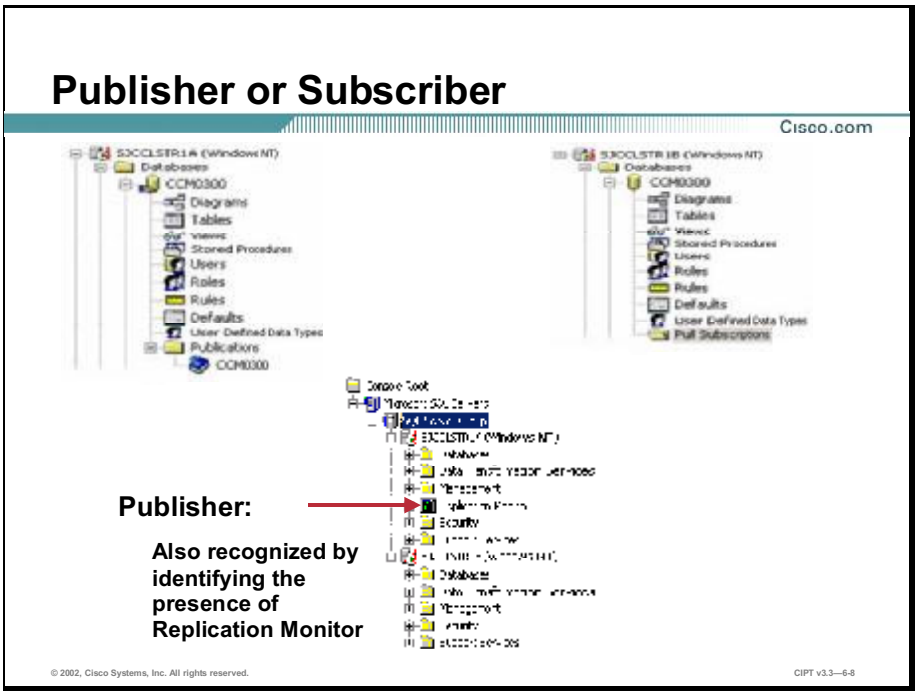


The database used is the Microsoft SQL Server 2000. To maintain data consistency throughout the cluster, the publisher database server uses one-way, or unidirectional, replication.

The database writes information to the publisher database only if you install CCM Web Components and perform Cisco CallManager Administration directly on the subscriber server. All entries that you make using the Cisco CallManager Administration page of the subscriber are written to the database on the publisher server. If the publisher is down, any updates made in the Cisco CallManager Administration page of the subscriber server are lost.

When building a publisher server, you may or may not choose to install CCM. If the publisher server does not have CCM installed, Cisco refers to the server as the glass house. The publisher occasionally acts as a backup, usually in smaller clusters.

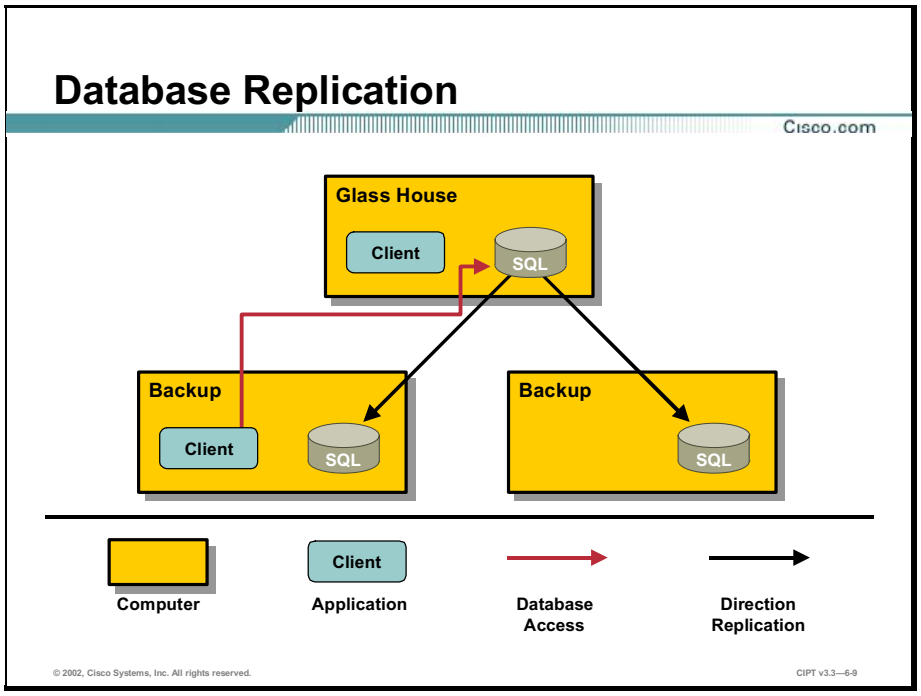
During the creation of the publisher server, the Microsoft SQL Server 2000 runs as a specified user, not as the interactive user or local system. The publisher is the glass house, the backup databases are subscribers, and all of the tables replicate, with the exception of the Call Detail Record (CDR) tables. The Microsoft SQL database name is CM03*xx*, where *xx* starts at 00 and increases incrementally with each migration. The Lightweight Directory Access Protocol (LDAP) directory sets up triggers.



In Microsoft SQL Server 2000 Enterprise Manager, you can determine if the server is the publisher or subscriber in two ways. One method is to expand the hierarchy down to the database:

- Microsoft SQL Servers\SQL Server Group\<Server_Name>\Databases\CCM0300
- For a publisher, you will see Publications in the Database Browse list
  - To see all of the subscribers, highlight CCM0300
- For a subscriber, you will see Pull Subscriptions in the Database Browse list

The second way to determine if the server is the publisher or subscriber is to check if the Replication Monitor is present. The Replication Monitor is only present on the publisher, and monitors the status of database replication between itself and the subscribers.



Database users should read from the same source to which they write. The glass house is the primary database with one-way replication. This replication is from the publisher to the subscribers.

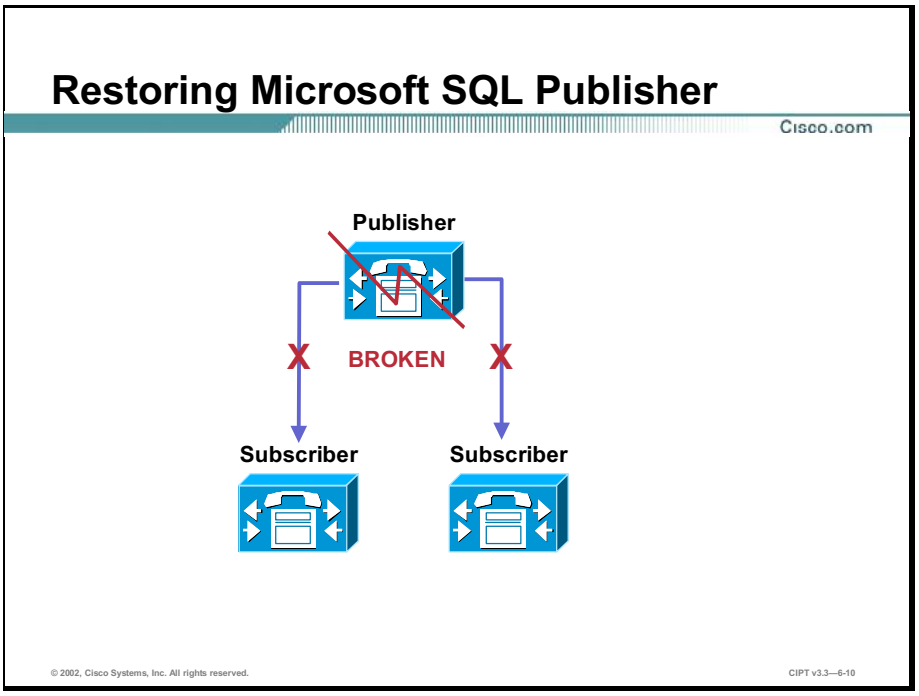
New entries to the database occur only at the glass house. After they are written to the glass house, these changes replicate to the backups.

The CCM writes all CDRs to the primary database (the glass house) for the cluster. If the primary database is not available, the CCM writes the CDRs to any of the other backup databases. When the glass house becomes available, the CCM begins to write new records to it and moves the locally written records to it on a catch-up basis.

The registry of each server stores the location of all databases. When you add more servers, they are written to the list of servers in the registry, but they are not available until the next boot.

The database layer first tries to use the glass house for reading and writing. If the glass house is not available, CCM uses a replicated database. If a replicated database exists on the local machine, Microsoft SQL database will access this database before any other.

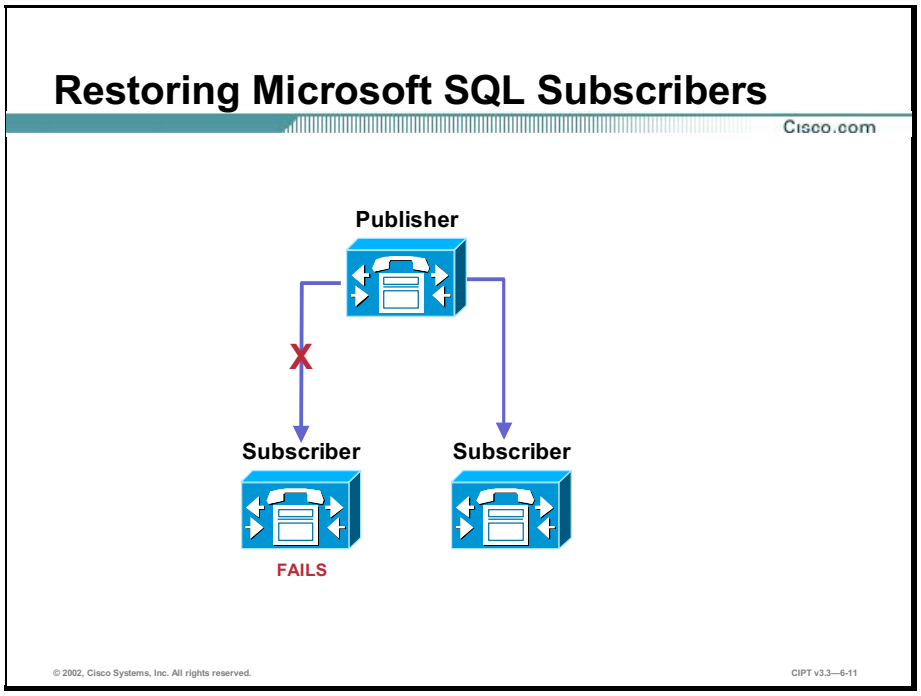
The Microsoft SQL Server uses Microsoft Transaction Server (MTS) to provide scalability via object pooling and transactional control. Greater speed is achieved with MTS, because Cisco TFTP does not pass through MTS at all, and CCM bypasses it during certain reads.



If the publisher fails, you must restore the publisher server from the last successful database backup. The symptoms of a publishing server failure will vary, but one sign of a failure is the inability to add devices to CCMs.

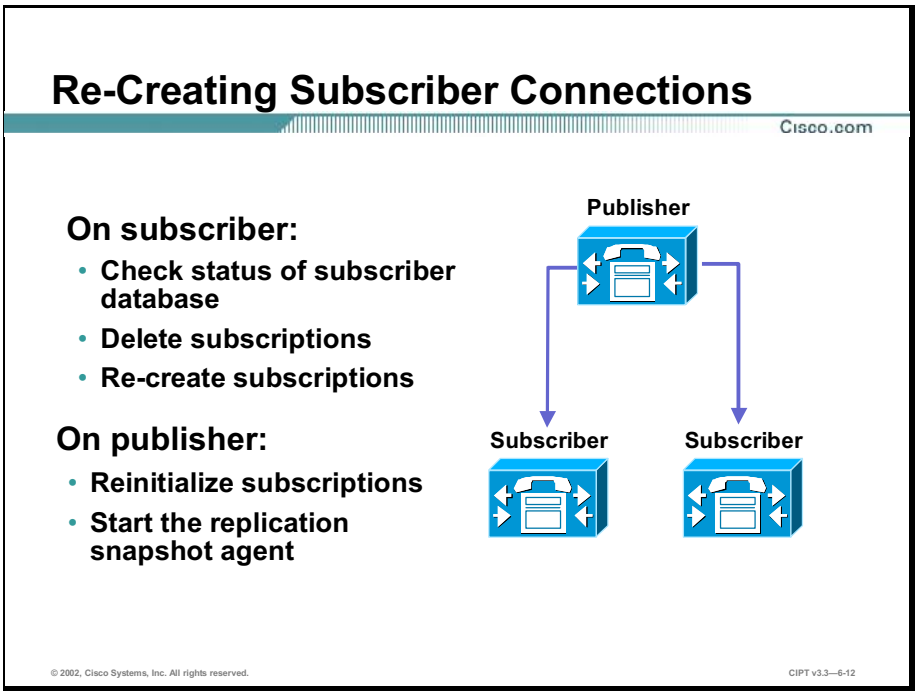
Cisco requires that you restore the server to the version of the last successful CCM database backup. As the server rebuilds, the system prompts you to select the upgrade and installation of the CCM publisher option. The Directory Server Configuration window opens and prompts you for the Directory Manager password. Enter the password in the Password field and in the Confirm Password field, and click Next to complete the configuration of CCM and the database server.

CCM and other included software are ready for installation. The Cisco IP telephony applications backup restores the database on the publisher server. The Cisco IP telephony applications restore utility prompts you to verify the location of the backup file (MCS.sti). The utility then automatically executes a restore operation to restore the CCM backup data from the specified tape or network directory.



If you have a subscriber failure, Cisco recommends that you restore the server to the original version of CCM. If the publisher functions properly, when the installation is complete, the Microsoft SQL Enterprise Manager can pull the database from the publisher in the cluster.

Note	The subscriber must have a valid subscription with the publisher for this function to work properly. The following page includes information on how to re-create the subscriber connections.



If you suspect a problem with subscriber connections, you should verify the status of the subscriptions or the jobs.

On the publisher server, perform these steps to verify the status of the subscribers and jobs:

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

Step 2 To see the status of subscriptions, choose the Pull Subscriptions folder located in the path: Microsoft SQL Servers/SQL Server Group/<this server's hostname>/Databases/<publication name>.

Step 3 To see the status of jobs, choose the Jobs folder located in the path: Microsoft SQL Servers/SQL Server Group/<this server's hostname>/Management/SQL Server Agent.

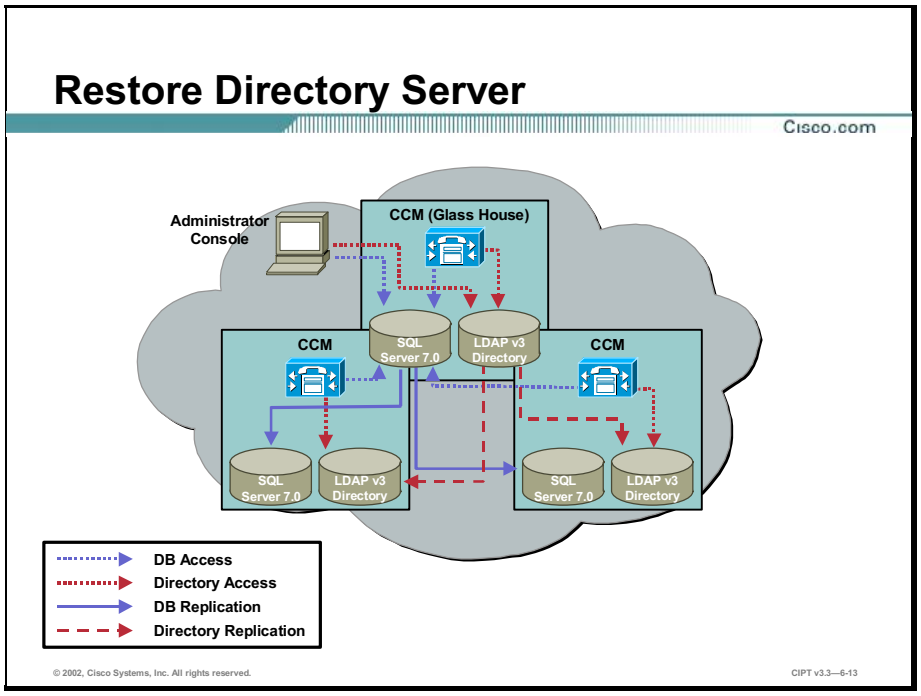
Step 4 The Expired Subscription Cleanup service may display a red x under normal operation. However, if a red x appears next to a subscriber name or a job name other than Expired Subscription Cleanup, assume that the subscriber connection is broken. You must reinitialize it.

Note The event log on the subscriber server lists Microsoft SQL Server Agent errors. To view the event log, choose Start>Programs>Administration tools>Event Viewer on the subscriber server.

If one or more subscription connections are broken, you must perform these actions:

Step 1 On each subscriber server, delete and then re-create the subscriptions.

Step 2 On the publisher server, reinitialize the subscriptions and start the replication snapshot agent.



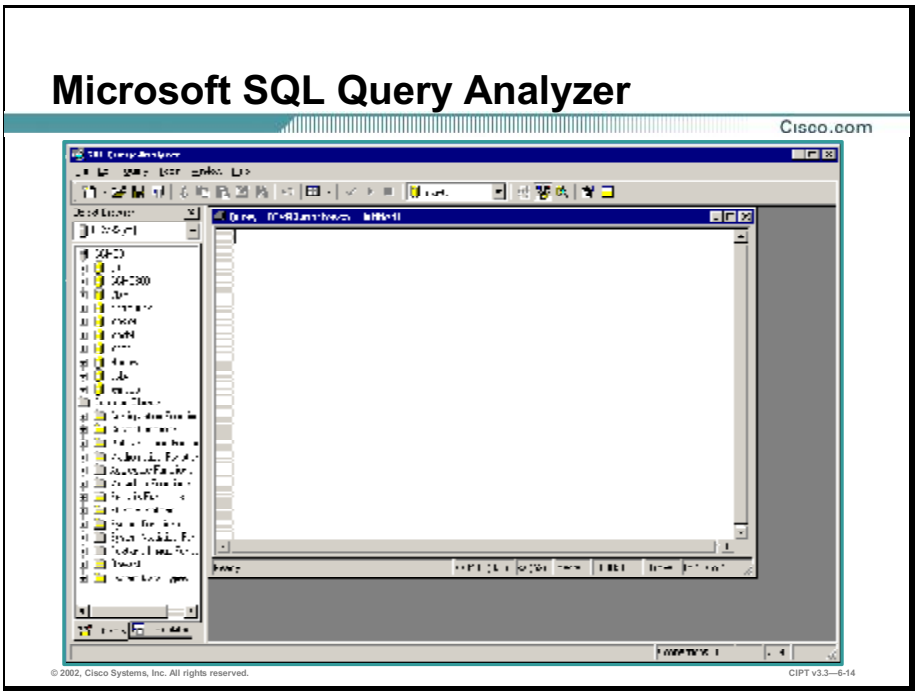
Data Connection Directory (DC-Directory) is the Cisco embedded directory and local LDAP directory container for all CCM user objects. If you are not using another LDAP directory, such as Microsoft Active Directory or Novell Directory Services, DC-Directory can provide a sufficient storage location for all CCM user information. In addition, the DC-Directory provides MetaLink functionality to synchronize information with external data sources.

You can restore the Directory Server if:

- A serious failure has caused data loss
- You must roll back a large update

Warning Restoring a backup destroys the current directory information base.

Caution Back up a corrupted directory server before restoring an old directory information base.

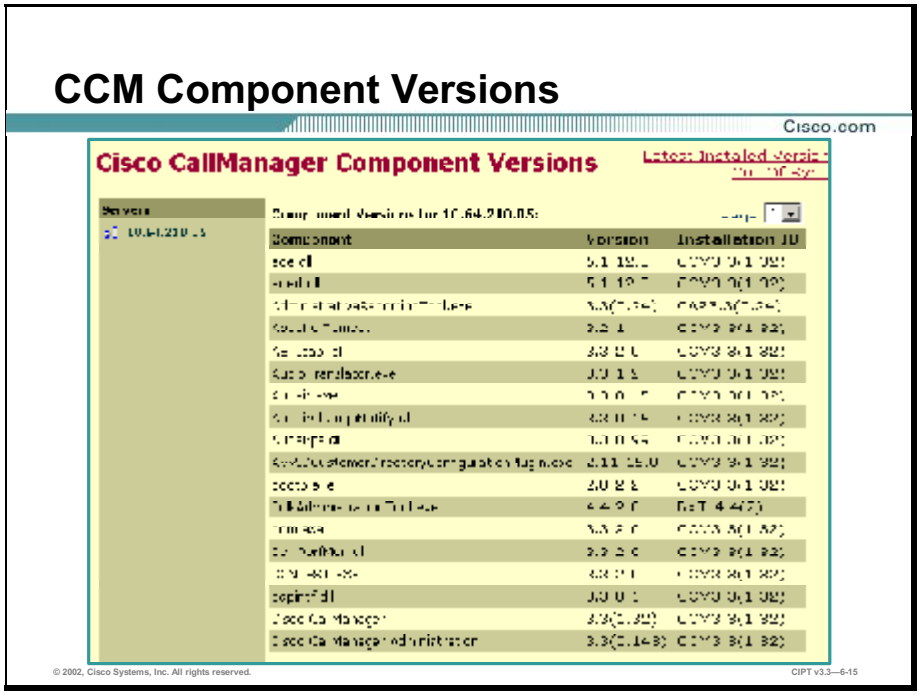


The Query Analyzer searches valid Microsoft SQL database tables for queried data. For example, you can request information about the devices assigned to the Locations parameter called test. The resulting display indicates the devices that are assigned to that parameter. The Select statement allows you to specify rows within the tables of the Microsoft SQL Database to retrieve and display information. The Select statement can be helpful to find information such as the number of devices in different locations.

Reference For more information on writing SQL Query Analyzer statements, refer to: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/architec/8_ar_sa_1a43.asp.

CCM Component Versions

This topic describes how administrators can view the component versions of CCM.

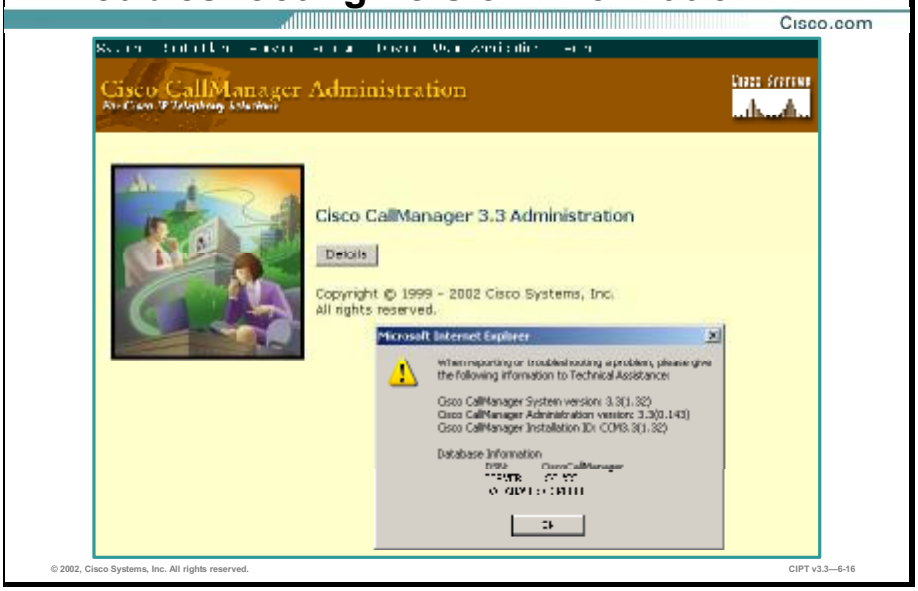


To find file versions associated with the current CCM, select **Help>Component Versions**, and then choose the specific server that you wish to monitor.

Note This example shows only one of several pages that contain information.

This listing helps determine if all of the servers within the cluster are up to date, as each server should show the same revision values.

Troubleshooting Version Information

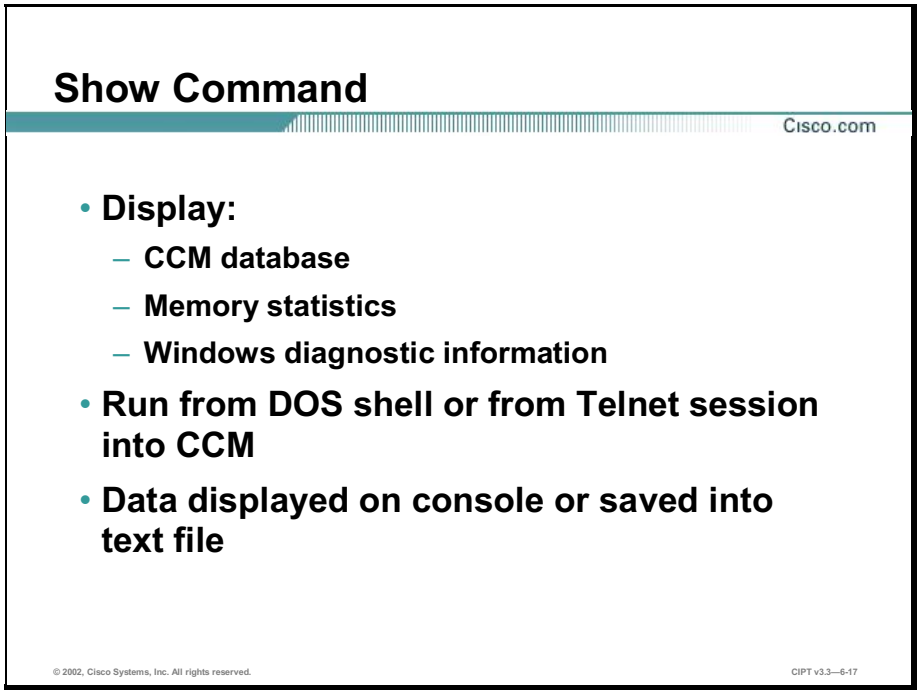


When supporting a customer, first check the information listed in the Cisco CallManager Administration Details. The detail information includes the system and Cisco CallManager Administration versions, database connection information, and Database Layer (DBL) versions. Encountering errors when displaying this information can indicate errors in the general system setup or configuration.

If an error occurs, try to refresh the page and check the database connection information again. If the information is still missing, a problem may exist in the connection to or the configuration of CCM(s) and Microsoft SQL server(s).

Command-Line Tools

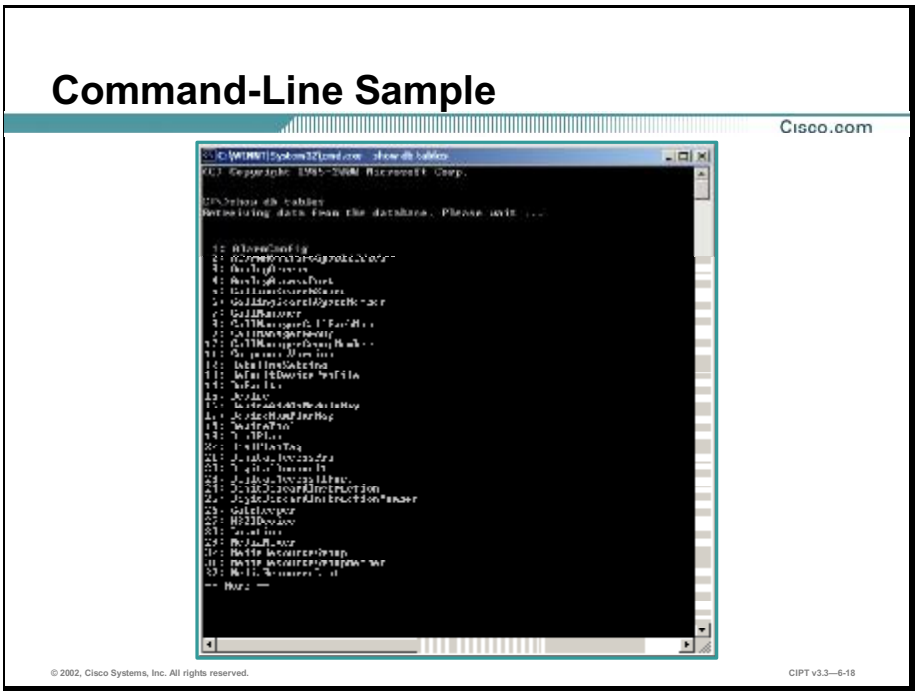
This topic examines the command-line tools that can effectively display useful information for identifying problems.



The **show** command-line tool displays the content of the CCM database, .ini config file, memory statistics, and Windows diagnostic information. If there is a problem with the Microsoft SQL database and you are unable to view the information by running the Microsoft SQL Query Analyzer, you can use the **show** command to display the information.

Run the **show** command from a DOS shell or a Telnet session into CCM. To accept Telnet sessions on the CCM, you must install separate Telnet server software. You can display the data on the command-line console or save it in a text file.

Note	The **show** command is a part of CCM that relies on CCM software. The **show** command is not available unless you install CCM. Cisco installs the show.exe executable file in the working directory \Program Files\Cisco\Bin



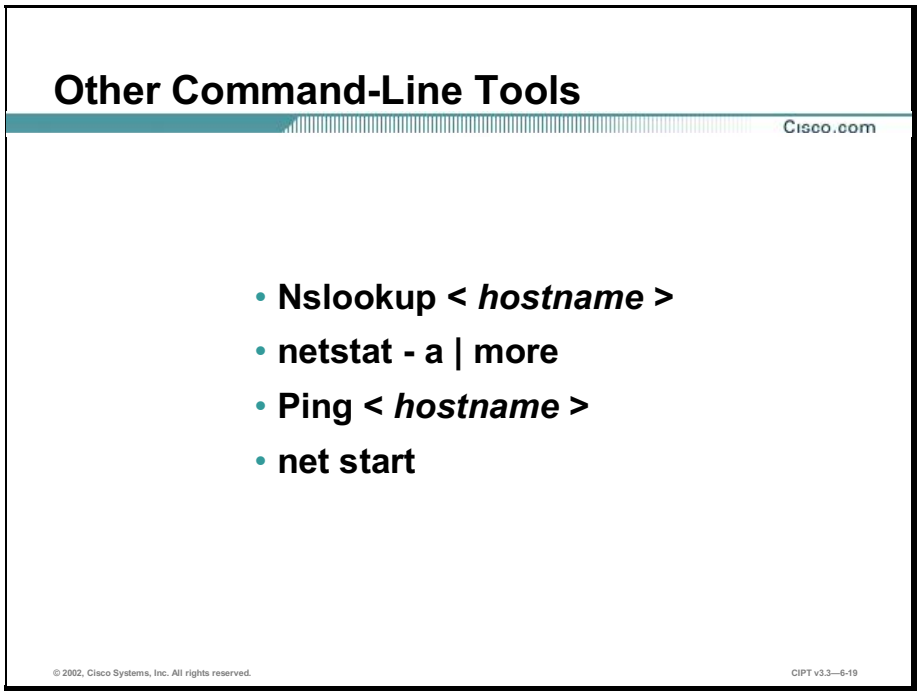
The **show db tables** command produces the sample output shown here. You can also gather this information from the Microsoft SQL Enterprise Manager under the Tables heading of the selected database, or by using command-line access from a Telnet connection.

Table: show Command Options

Command	Description
`-f <filename>`	Name of file where report is printed
`-c <col width>`	Width of each column in the database report (default 15)
`-w <con width>`	Width of the database report area (default 80)
`-v`	Verbose mode

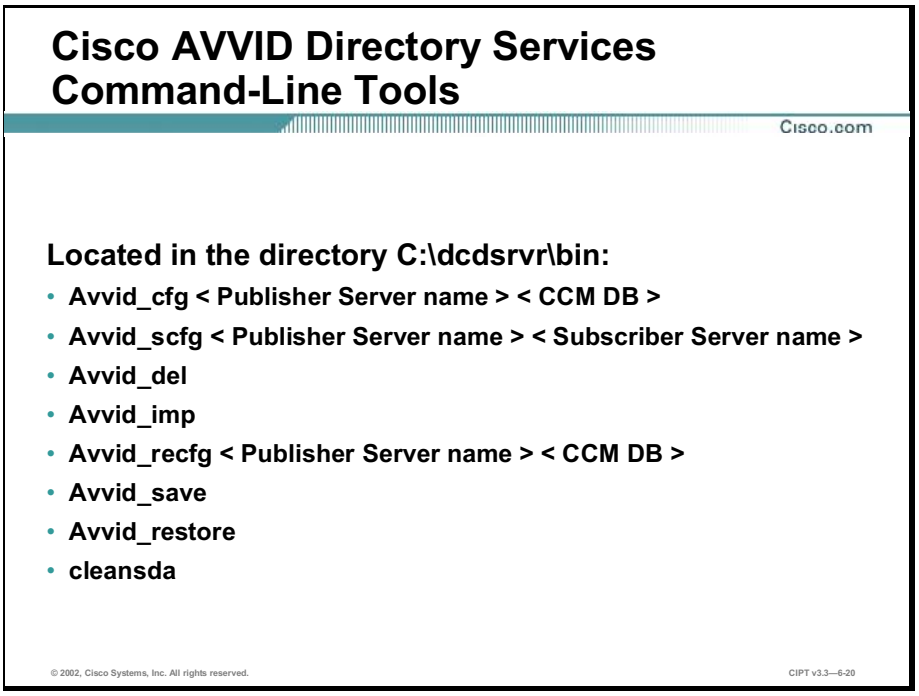
Table: show Command Parameters

Command	Description
`?`	Show help message
`db`	Show configuration database
`db tables`	Show database table names
`db t <tablename>`	Show content of database table
`win`	Report windows diagnostics



These standard Microsoft commands are useful troubleshooting command-line tools:

- **Nslookup < *hostname* >:** This command checks for hostname to IP address resolution.
- **netstat – a | more:** This command checks for socket listens, established sessions, and open port numbers.
- **Ping < *hostname* >:** This command checks that a machine is IP reachable.
- **net start:** This command checks to see if specific services are running on Windows NT.



If you cannot add a user or view to the Global Directory, there may be a problem regarding the DC-Directory. The DC-Directory service may have halted, or the DC-Directory services running on the subscriber and the publisher may not be synchronized. If you do not synchronize the subscriber and publisher, you cannot access the databases. These powerful command-line tools allow you to clear and reconnect the connections between the servers. After you restore the connections, replication can occur and the databases can synchronize again.

You run the commands shown from the command prompt of the CCM server after changing the directory to C:\dcdsrvr\bin. These commands restore a DC-Directory database MetaLink connection between server nodes:

- **Avvid_cfg** < publisher server name > < CCM database name >:
  - Invoked by Setup on primary (glass house) server
  - Initializes and configures DC-Directory
  - Configures MetaLink Open DataBase Connectivity (ODBC) Import Agreements
  - The primary server name can be substituted with the IP address of the server itself
- **Avvid_scfg** < publisher server name > < subscriber server name >:
  - Invoked by Setup on secondary server
  - Initializes and configures DC-Directory
  - Configures DC-Directory Replication Agreements

- As with the previous statement, IP addresses may be substituted for names where applicable

- **Avvid_del:**
  - Invoked on primary server
  - Deletes MetaLink ODBC Import Agreements and the imported information in the directory

- **Avvid_imp:**
  - Invoked on primary server
  - Creates MetaLink ODBC Import Agreements

- **Avvid_recfg** < primary Microsoft SQL Server name > < CCM database >:
  - Invoked on primary server
  - Deletes MetaLink ODBC Import Agreements and the imported information in the directory
  - Reconfigures MetaLink ODBC Import Agreements

- **Avvid_save:**
  - Invoked on primary server
  - Saves the current user and user profile information in text files

- **Avvid_restore:**
  - Invoked on primary server
  - Restores the user and user profile information (saved using avvid_save)

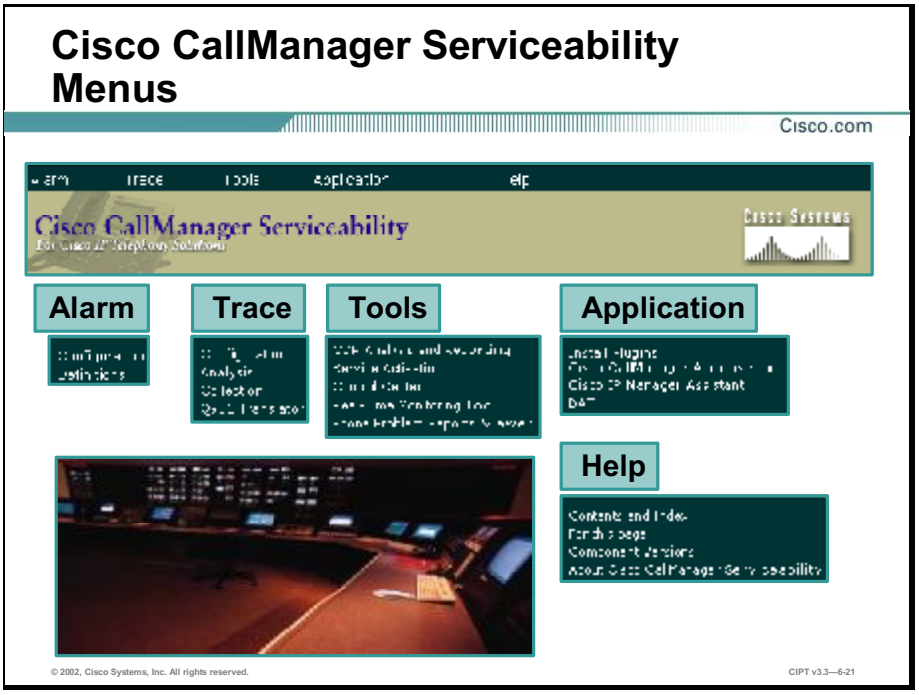
- **Cleansda:**
  - Clears out the existing Directory Information Database by deleting it and replacing it with a clean copy

---

Note Make sure that you can ping between the publisher and subscriber CCMs. Network connectivity is crucial. Anywhere the word “subscriber” or “publisher” appears in a command, replace it with the name of the appropriate subscriber or publisher server. You must be sitting at the console of the server to execute these commands. Do not execute them from a Terminal Services Window.

Cisco CallManager Serviceability

This topic describes how administrators can use the Cisco CallManager Serviceability tool to troubleshoot system problems.



The CCM AST provides you with these services:

- **Alarm:** Alarm saves information about CCM service events for troubleshooting and provides alarm message definitions. You can forward alarms to a trace file for further analysis.
  - The AST alarms allow you to configure the CCM to write an event to a trace file or the Windows 2000 Event Viewer when an incident occurs, such as the failure of a telephone to register. You can configure alarms for CCM servers in a cluster and for the services in each server.
  - The Definitions application stores alarm definitions and the recommended actions in a Microsoft SQL Server 2000 database. The system administrator can search the database for the definitions of all alarms. Definitions include the alarm name, description, recommended action, severity, parameters, and monitors.
- **Trace:** Trace allows you to save a detailed log of CCM events for troubleshooting system problems. You can configure, collect, and analyze trace data.

- Use the Configuration application to specify the trace parameters; for example, the CCM server within the cluster, the CCM service on the server, the debug level, and the specific trace fields.

- Use the Analysis application to provide greater trace detail on a Signal Distribution Layer (SDL) trace, system diagnostic interface (SDI) trace, a CCM service type, or the time and date of trace.

- Use the Collection application to collect the trace from a list of SDL or SDI log files. You can choose a specific log file from the list and request information from that log file, such as host address, IP address, trace type, and device name.

- The Q931 Translator application filters incoming data from CCM SDI logs and translates the data into Cisco IOS messages. The Translator application displays the message in the message translator interface.

- **Tools:** The Tools service offers three troubleshooting applications.

  - The Service Activation application can activate and deactivate all of the CCM services for all CCM servers.

  - The Control Center application allows you to start, stop, and view the status of CCM services.

  - The Real-Time Monitoring Tool application monitors the real-time behavior of all components in a CCM cluster and displays on-screen feedback through a Java-based application.

- **Application:** The Application service in the AST offers several troubleshooting applications.

  - The Install Plugins application can help you extend the functionality of CCM.

  - The CCM Administration application provides a convenient, direct link to the CCM Administration page.

  - The Bulk Administration Tool (BAT) application adds multiple telephones and users to CCM and performs bulk modifications to telephones.

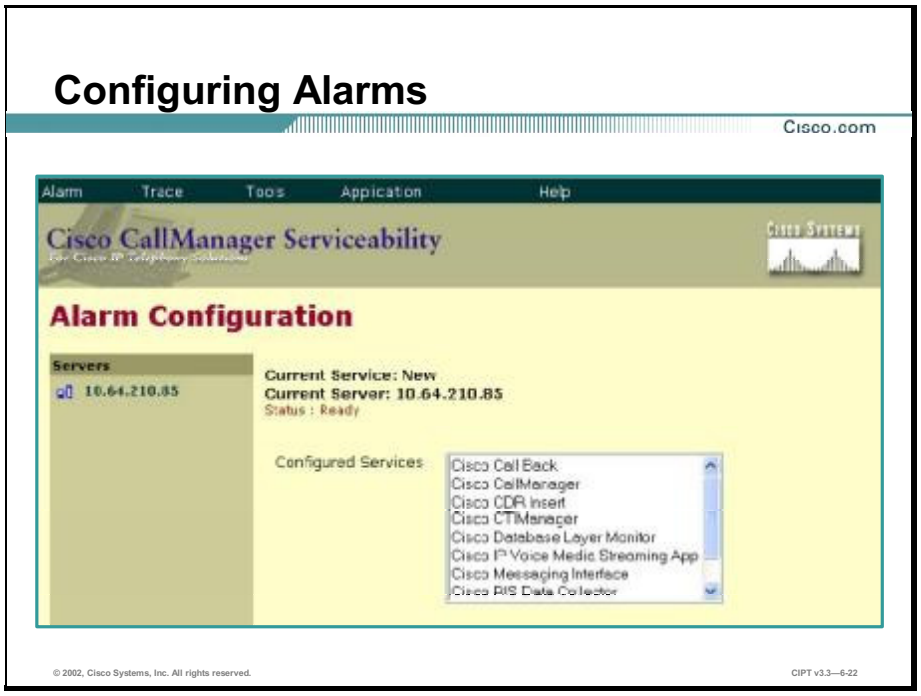
- **Help:** The Help service provides troubleshooting support.

  - The Contents and Index application provides you with online assistance.

  - The For this page application provides online help that corresponds to the page that you are viewing.

- The Component Versions application displays the latest installed component version information for all CCM servers in the cluster and lists servers in the cluster with out-of-sync system components.

- The About CCM Serviceability application provides a link that will take you directly to the main page of the CCM AST.



The Cisco CallManager Serviceability Alarms serves two main functions: configuring alarms and events, and providing alarm message definitions. Both functions assist the system administrator and support personnel in troubleshooting CCM problems.You can configure alarms for CCM servers in a cluster and services for each server, such as CCM, Cisco TFTP, and Cisco CTI Manager .

You use alarms to provide runtime status and the state of the system, and to take corrective action for problem resolution, such as determining whether IP Phones are registered and working. Alarms contain information including an explanation of the problem and recommended action. The alarm information includes application name, machine name, and cluster name to help you troubleshoot problems that are not on your local CCM.

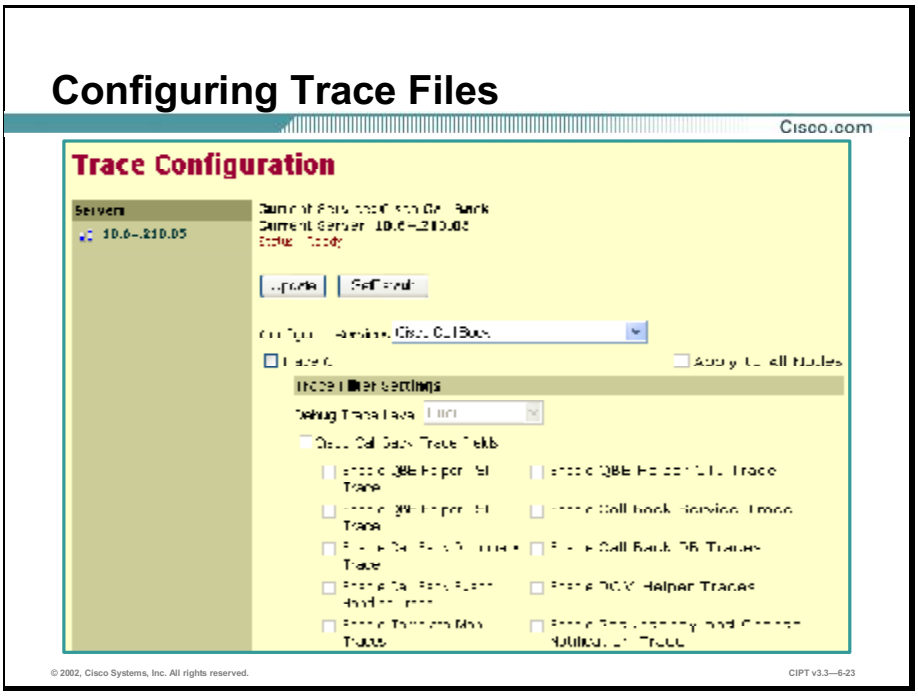
You can configure the alarm interface to send alarm information to multiple destinations, and each destination can have its own alarm event level, from debug to emergency.

You can forward alarms to a Serviceability Trace file. An administrator configures Alarms and Trace parameters and provides the information to a Cisco Technical Assistance Center (TAC) engineer. You can direct alarms to the Windows 2000 Event Log, syslog, an SDI trace log file, an SDL trace log file for CCM and CTI Manager only, or to all destinations. You can use the trace to collect and analyze the alarms.

When a service issues an alarm, the alarm interface sends the alarm to the chosen monitors, such as an SDI trace. The monitor either forwards the alarm or writes it to its final destination, such as a log file.

Note To log alarms in the SDI trace log file, check the Trace on and the Enable trace file log check boxes in Trace configuration, and the SDI alarm destination check box in Alarm configuration.

Configuring Trace Files



Cisco CallManager Serviceability provides a web-based trace tool to assist the system administrator and support personnel in troubleshooting CCM problems. Trace provides three main functions:

- Configure trace parameters
- Collect trace files
- Analyze trace data for troubleshooting problems

The Trace and Alarm tools work together. You can configure trace and alarm settings for CCM services, which primarily assist the Cisco TAC engineers. You can direct alarms to the Windows 2000 Event Viewer, CiscoWorks2000 syslog, SDI or SDL trace log files, or to all destinations. You can base traces for CCM services on debug levels, specific trace fields, and CCM devices such as IP Phones or gateways. You can perform a trace on the alarms that are sent to the SDI or SDL trace log files.

Use the Trace Configuration tool to specify the parameters that you want to trace for troubleshooting CCM problems. The Trace Configuration window provides two types of settings: trace filter and trace output.

You must specify the following trace parameters:

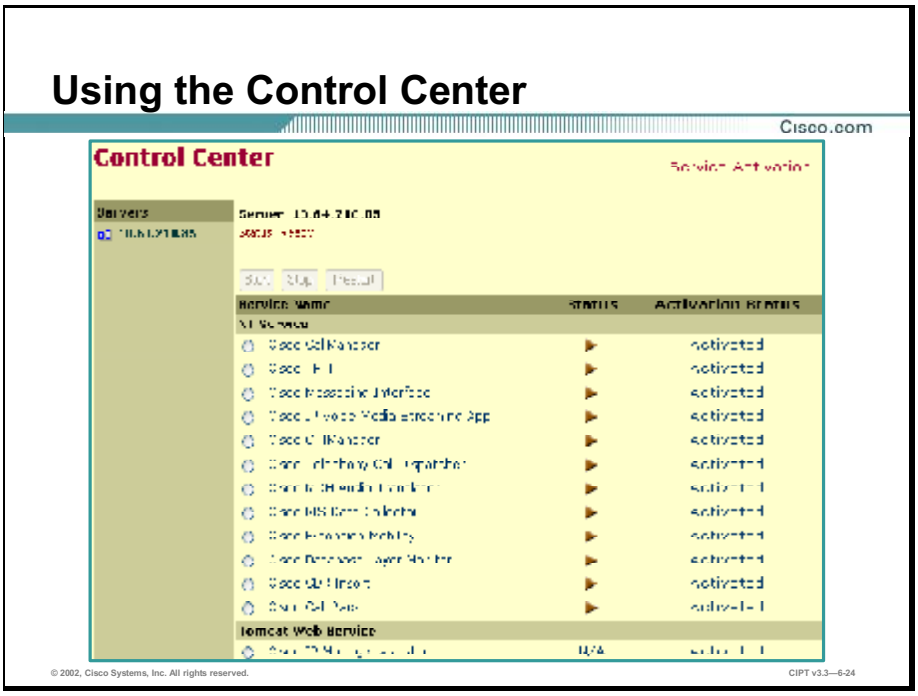
- CCM server (within the cluster)
- CCM service on the server
- Debug level

- Specific trace fields
- Output settings

If the service is a call-processing application, such as CCM or Cisco CTI Manager, you can configure a trace on devices such as IP Phones and gateways. For example, you can narrow the trace to all enabled IP Phones with a directory number beginning with 333.

Note Enabling Trace decreases system performance; therefore, enable Trace for troubleshooting purposes only. For assistance in using Trace, contact Cisco TAC.

Using the Control Center



You can use the Control Center tool to view the status of services and to start and stop CCM services for a particular server in a cluster.

By starting and stopping a CCM service, all of the Cisco IP Phones and gateways currently registered to that CCM service will fail over to their secondary CCM service. You will need to restart the devices and IP Phones if they cannot register with another CCM service. It is possible that starting and stopping a CCM service may cause other installed applications, such as Conference Bridge or Cisco Messaging Interface, to start and stop as well.

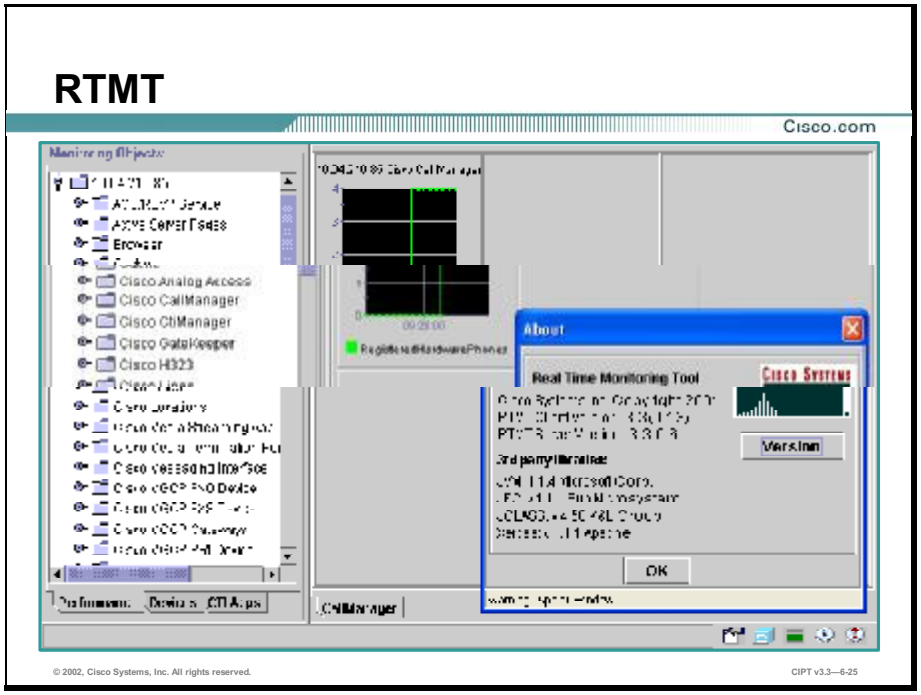
This list shows the symbols associated with the status of the service:

Icon Symbol	Description
Square	Service is stopped.
Arrow	Service is running.

Caution Stopping a CCM service also stops call processing for all devices controlled by that service. When you stop a CCM service, calls from an IP Phone to another IP Phone or to a Media Gateway Control Protocol (MGCP) gateway will stay up, but other types of calls will be dropped.

Real-Time Monitoring Tool

This topic explains how the Real-Time Monitoring Tool (RTMT) can assist administrators.



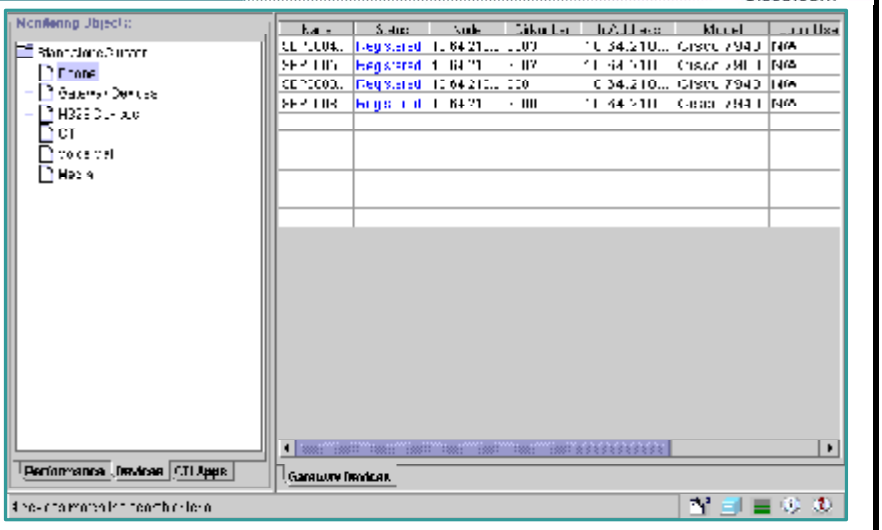
Administrators use the RTMT to view real-time status of the components in a CCM cluster by monitoring and displaying performance and device status information. The RTMT also provides an alert notification mechanism to ease system administrator troubleshooting tasks.

The RTMT monitors various aspects of the CCM performance by periodically polling Windows 2000 performance counter values. The tool discovers devices, regardless of their registration status in the cluster. RTMT searches according to the device name, IP address, or Domain Name (DN) and monitors the status of discovered devices. Device status monitoring provides an alert notification mechanism for gateway ports and channels.

You can view the properties by simply selecting them and dragging the value over to the monitor area.

Version information is useful in determining conflicts that might exist between clusters or when a known bug is linked to a specific release. You can display version information by clicking the icon in the bottom right corner tray of the window.

RTMT: Device Monitoring



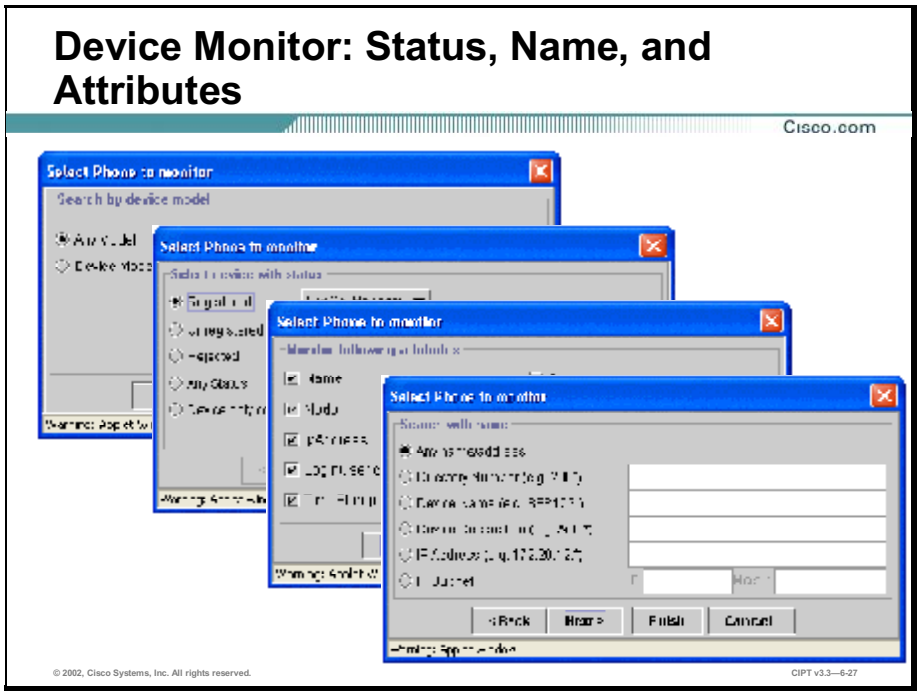
Device monitoring is useful in determining conflicts and the overall operation of clusters.

RTMT discovers devices regardless of their registration status, such as registered or failed, in the cluster. The tool searches by device name, device description, IP address, IP subnet, or DN, and monitors the status of discovered devices.

Device status monitoring supports these capabilities:

- Device selection and discovery for servers
- Cluster-wide device selection and discovery
- Discovery of configured devices that are not physically connected.
- Gateway port and channel status monitoring and alert notification

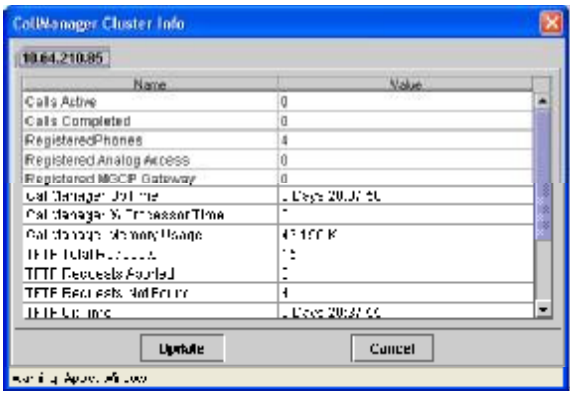
To access this area in the RTMT, select the device tab in the lower left-hand corner of the RTMT tool. Select the device that you wish to monitor, and select the appropriate parameters to display the information.



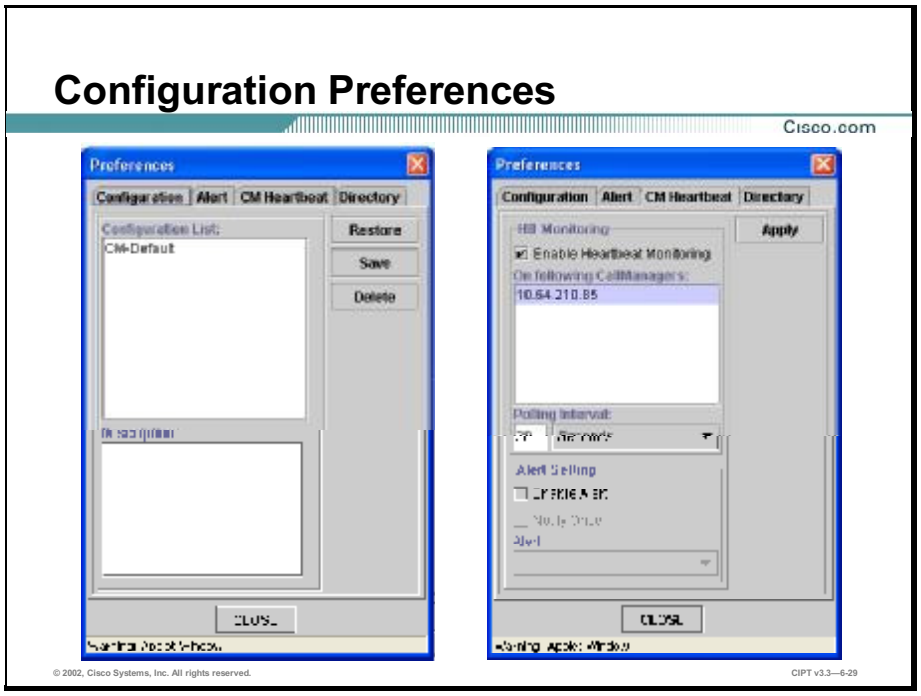
You can select the devices that you wish to monitor based on shared characteristics, such as Registered or Rejected. You can further refine the Device Monitor aspect of AST to narrow the search characteristics to directory numbers or subnet. In addition, you may select only the attributes that you wish to monitor, such as Node or Status Reason. You should select only the values that you wish to monitor, which saves time and eliminates unnecessary data in the monitor window. To access these configuration parameters, select the device for which you wish to view the information. The monitor then prompts you to enter the characteristics to help narrow the search.

Cluster Information

Cisco.com



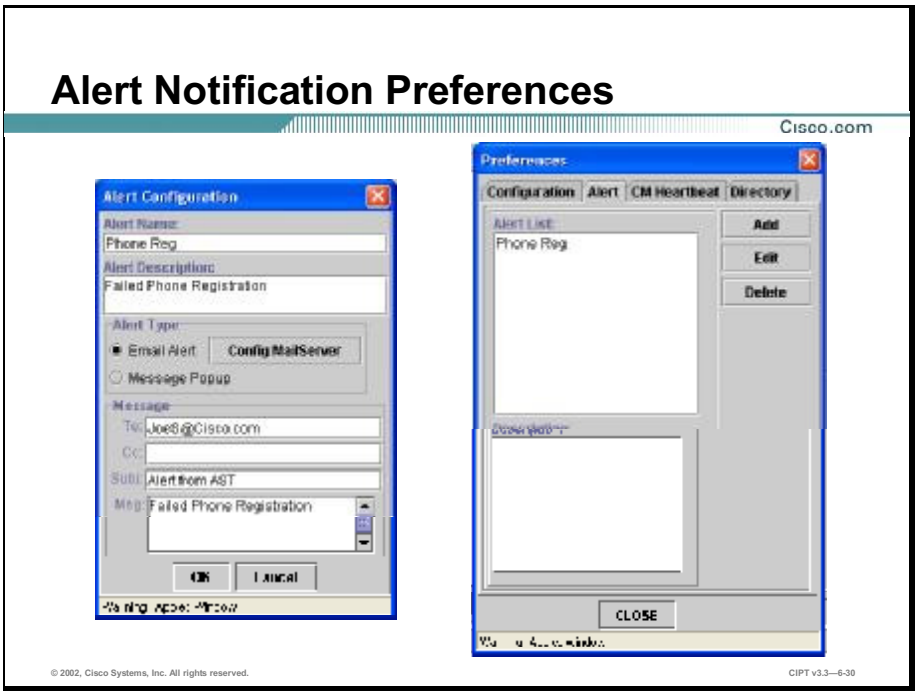
You can also gather information regarding cluster operation by selecting the CCM icon in the bottom right corner of the RTMT. Clicking this icon displays information, such as the number of TFTP requests or system uptime, for quick reference, which helps you isolate the possible problems in the system.



The Preferences icon that is located in the RTMT monitoring window allows the administrator to save, restore, and delete RTMT configuration preferences. The administrator can also add, edit, and delete alert settings and configure the heartbeat monitoring, directory status, and polling rates.

You can configure preferences to save this information:

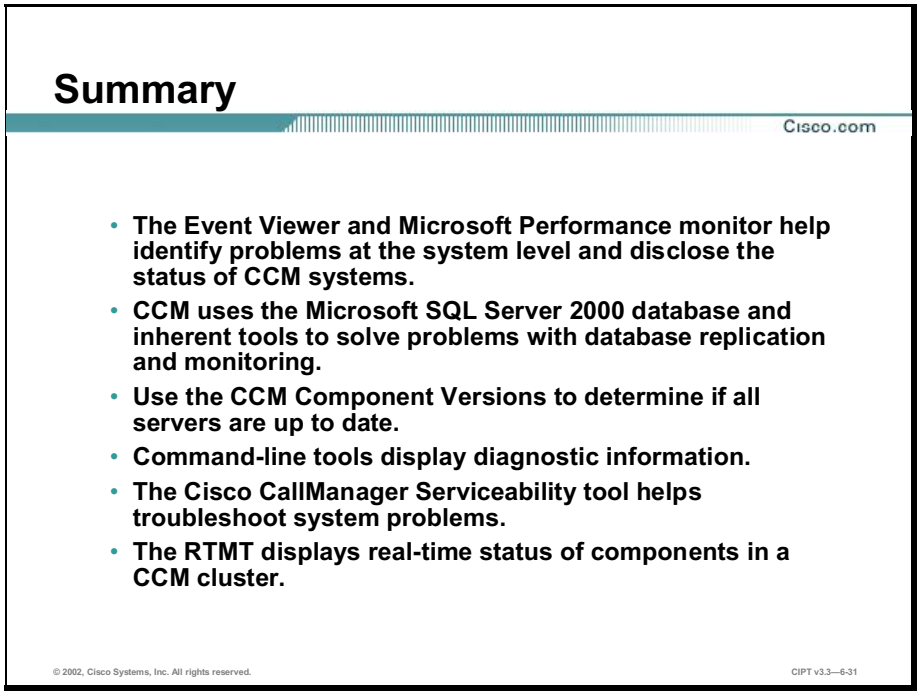
- Performance monitoring categories, including associated counters, counter thresholds, counter alerts, and polling rate
- Monitored devices categories, including search criteria and polling rate
- Heartbeat monitoring polling settings
- Directory status monitoring polling settings



You can configure e-mail-generated alerts by using the AST to define rule sets for their implementation.

Summary

This topic summarizes the key points you learned in this lesson.



Next Steps

After completing this lesson, go to:

- Your individual course curriculum for reference, and begin your next learning activity

References

For additional information, refer to these resources:

- Cisco website:
  http://www.cisco.com
- Cisco Documentation CD-ROM
- Smith, A., C. Pearce, D. Whelton, and J. Alexander. *Cisco CallManager Fundamentals*: *A Cisco AVVID Solution.* San Jose, California: Cisco Press; 2001.

Lesson Review

This practice exercise reviews what you have learned in this lesson.

Q1) Which of these logs from Event Viewer do you use to view system startup errors?

A) Application logs

B) System logs

C) Security logs

D) Diagnostic logs

Q2) Which of these servers contains the read/write copy of the database?

A) publisher

B) subscriber

C) primary

D) secondary

Q3) Where is the current CCM component version located?

A) Application

B) Tools

C) Help

D) Services

Q4) Which of these command-line tools would you use to re-establish a broken MetaLink connection?

A) **show** command-line tools

B) **avvid** command-line tools

C) **ping** command-line tool

D) **netstat** command-line tool

Q5) Which of these tools can you enable to automatically notify the CCM administrator, or other support personnel, in the event of a failed service?

A) Alarm

B) Trace

C) Service Activation

D) Collection

Q6) Which of these counters does the RTMT poll for updated information?

A) performance counters in Windows 2000

B) performance counters in Windows 2000 Event Viewer

C) performance counters in Microsoft SQL

D) performance counters in Trace files

A

Answers to Review Questions

This document contains the answers to the review questions that appear at the end of each lesson.

Module 1: Cisco CallManager

Lesson 1: Introduction to Cisco AVVID and Cisco CallManager

Lesson Review

Q1) What is the maximum number of Cisco IP Phones that can be added to a Cisco Media Convergence Server 7835-1000 if 3000 device weight units are already registered, and BHCA is less than six?

A) 1000

B) 1500

C) 2000

D) 2500

Answer: C

Q2) Which of these functions is NOT a function of CCM?

A) call processing

B) signaling control

C) device control

D) dial plan

E) voice messaging

Answer: E

Q3) Where would you expect to find configuration options relating to CCM redundancy for IP Phones?

A) system menu

B) service menu

C) feature menu

D) device menu

Answer: A

Q4) What type of Cisco Media Convergence Server should you purchase for a small IP telephony deployment in an office that has no dedicated information technology room?

A) Cisco Media Convergence Server 7815

B) Cisco Media Convergence Server 7825

C) Cisco Media Convergence Server 7835

D) Cisco Media Convergence Server 7845

Answer: A

Q5) CCM uses which of these operating systems?

A) Linux

B) Windows 95

C) Windows NT

D) Windows 2000

Answer: D

Q6) Which of these options is a cost-saving benefit of Cisco VoIP?

A) toll bypass

B) integrated website VoIP

C) a single message inbox for all message types

D) all of the above

Answer: D

Q7) What layer of Cisco AVVID contains CCM?

A) client

B) applications

C) call-processing

D) infrastructure

Answer: C

Lesson 2: Cisco CallManager Cluster and Deployment Options

Lesson Review

Q1) What is the maximum one-way delay that is supported between CCMs when using a distributed single-cluster model?

A) 10 ms

B) 20 ms

C) 40 ms

D) 150 ms

Answer: C

Q2) What is the recommended best practice regarding WAN codecs in a distributed call-processing deployment?

A) G.711 only

B) G.729 and G.723

C) a single codec for the WAN

D) multiple codecs between each site

Answer: C

Q3) Which feature provides telephony services to a branch site when the WAN link goes down?

A) locations-based CAC

B) hub and spoke topology

C) extension mobility

D) SRST

Answer: D

Q4) Which codec is most often used in a single-site deployment?

A) G.729

B) G.723

C) GSM

D) G.711

Answer: D

Q5) Which of these servers is NOT required for a CCM cluster?

A) TFTP server

B) Microsoft SQL publisher

C) MS Exchange

D) none of the above

Answer: C

Q6) What does the subscriber do if the publisher does NOT answer its database lookup request?

A) waits for the publisher to become available and then makes a database request

B) sends a reorder tone to the device because it cannot access the database

C) requests the local copy of the database to look up the information

D) forces the device to register to another subscriber for a database lookup

Answer: C

Q7) Which of these options is NOT characteristic of a CCM cluster?

A) at least two servers.

B) at least one publisher server

C) at least 2500 Cisco IP Phones

D) none of the above

Answer: C

Q8) What is the maximum number of IP Phones that the Cisco 7200 router can support at a remote branch location during a loss of connectivity to CCM headquarters in a centralized deployment model?

A) 280

B) 480

C) 580

D) 680

Answer: B

Lesson 3: Installing Cisco CallManager

Lesson Review

Q1) Which two of the following services does Cisco recommend that you stop on a subscriber server? (Choose two.)

A) FTP Publishing Service

B) CCM Service

C) IIS Admin Service

D) World Wide Web Publishing Service

Answers: C and D

Q2) What function does the Cisco Messaging Service provide?

A) support for Cisco Unity

B) allows CCM to interface with SMDI-compliant messaging systems

C) allows CCM to interface with any external messaging system

D) all of the above

Answer: B

Q3) If you are not using DNS, what must be configured to resolve NetBios server names?

A) DHCP

B) backup server

C) lmhost file

D) DNS reverse lookup

Answer: C

Q4) What is the total number of CD-ROMs needed to install CCM?

A) 1

B) 2

C) 3

D) 4

E) 5

F) 6

Answer: C

Q5) What is the first step required when upgrading the CCM publisher server?

A) backup the server data

B) upgrade the backup utility

C) reboot the server using the Hardware Detection CD-ROM

D) run the automated script on the Cisco CallManager 3.3 Software CD-ROM

Answer: B

Module 2: Devices

Lesson 1: Cisco IP Phones

Lesson Review

Q1) Which compressed codec do Cisco second-generation IP Phones support?

A) G.723

B) G.728

C) G.729

D) G.729a

Answer: D

Q2) Which item does a Cisco IP Phone NOT obtain from the DHCP server?

A) CDP

B) IP address

C) TFTP server IP address

D) subnet mask

Answer: A

Q3) A company wants to migrate to a VoIP network, but it has an expensive all-in-one voice/fax/copier device. Which device would you recommend?

A) Cisco 7936 Conference Station

B) Cisco IP SoftPhone

C) Cisco ATA 188

D) Cisco 7914 Expansion Module

Answer: C

Q4) A company is deploying a VoIP network for their call center of 120 employees. The call center employees require an IP Phone that is capable of supporting two directory numbers. In addition, the network administrator would like to run a single cable for the IP Phone and the computer that are collocated in each employee cubical. Which IP Phone will meet this requirement for the least expense?

A) Cisco IP Phone 7910+SW

B) Cisco IP Phone 7910

C) Cisco IP Phone 7940

D) Cisco IP Phone 7960

Answer: C

Q5) 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 meet these requirements?

A) Cisco IP Phone 7902

B) Cisco IP Phone 7905

C) Cisco IP Phone 7910

D) Cisco IP Phone 7912

Answer: B

Q6) Which of the following H.323 codecs do most Cisco end-user devices support?

A) G.711

B) G.723

C) G.711 and G.723

D) G.711 and G.729a

Answer: D

Lesson 2: Configuring Cisco CallManager to Support IP Phones

Lesson Review

Q1) Which setting is NOT required for a device pool?

A) media resource group list

B) CCM group

C) date/time group

D) region

Answer: A

Q2) How does CCM tie configuration information to the IP Phones in the Microsoft SQL database?

A) with an IP address

B) through a unique GUID

C) with a hostname

D) none of the above

Answer: D

Q3) Which IP Phone button template is the default for a Cisco IP Phone 7960?

A) 1 line, 5 speed dials

B) 2 lines, 4 speed dials

C) 3 lines, 3 speed dials

D) 6 lines, 0 speed dials

Answer: B

Q4) Terry is a network administrator for ATTC Inc. Terry wants to configure the Cisco IP telephony network to use only the G.729 codec. Outline the general steps that Terry needs to take to complete this process. Use a minimum number of steps to complete the process.

Answer:

Step 1: Terry needs to modify the default region to use only G.729.

Step 2: Terry needs to verify that all of the existing device pools have the default region selected.

Q5) What do you choose to view the area of the Cisco CallManager Administration that eliminates DNS reliance by changing the CCM server name to an IP address?

A) System>Server

B) System>Cisco CallManager

C) Service>Service Parameters

D) Device>Phone

Answer: A

Lesson 3: Cisco Catalyst Switches

Lesson Review

Q1) What is the default CoS value setting of a Cisco IP Phone?

A) CoS = 0

B) CoS = 2

C) CoS = 5

D) CoS = 7

Answer: C

Q2) What is the recommended IP addressing scheme for a Cisco IP telephony solution?

A) The IP Phones and PCs reside on the same port and use real IP addresses.

B) The IP Phones and PCs reside on the same port as the IP Phones and use a 10.0.0.0 network.

C) The IP Phones and PCs reside on the different ports and use real IP addresses.

D) The IP Phones and PCs reside on the different ports, and the IP Phones use a 10.0.0.0 network.

Answer: B

Q3) How much power does a Cisco 7960 IP Phone use without any expansion modules attached?

A) 5W

B) 7W

C) 10W

D) 12W

Answer: B

Q4) Which device does not support a single port with multiple VLANs?

A) Cisco Catalyst 3524 switch

B) Cisco Catalyst 4224 switch

C) Cisco Catalyst 6000 series switch

D) Cisco power patch panel

Answer: D

Q5) Which item is a network layer QoS marking?

A) CoS

B) ToS

C) QoS

D) DoS

Answer: B

Lesson 4: Cisco Access Gateways

Lesson Review

Q1) What type of voice network connects a Cisco access gateway?

A) H.323

B) the PSTN

C) PBX systems

D) all of the above

Answer: D

Q2) What type of interface is on a digital voice gateway?

A) FXO

B) T1

C) E&M

D) FXS

Answer: B

Q3) Which two switch series are capable of supporting a voice network? (Choose two.)

A) Catalyst 1900

B) Catalyst 4000

C) Catalyst 2800

D) Catalyst 6000

Answers: B and D

Q4) Which two protocol types can the VG200 gateway support? (Choose two.)

A) H.323

B) Cisco IOS MGCP

C) Skinny

D) MGCP

Answers: A and B

Q5) Which item is a core gateway requirement?

A) support for DTMF relay

B) support for inline power

C) support for multiple VLANs on single port

D) support for disconnect supervision

Answer: A

Module 3: Route Plan

Lesson 1: Route Plan Basics

Lesson Review

Q1) Which of the following work together to control and enhance external call routing?

A) route groups and route lists

B) route lists and route patterns

C) translation patterns

D) none of the above

Answer: A

Q2) What is the key to making toll bypass and PSTN Fallback features transparent to your users?

A) Digit Manipulation

B) dialing 9 for second dial tone

C) Route Groups

D) Route Lists

Answer: A

Q3) Which of the following are valid wildcards? (Choose three.)

A) *

B) !

C) .

D) $

Answers: A, B, and C

Q4) Which of the following sets the interdigit timeout to 15 seconds?

A) 15

B) 150

C) 1500

D) 15000

Answer: D

Q5) Which of the following constitutes a basic route plan? (Choose four.)

A) Route Groups

B) Voice Gateways

C) Route Lists

D) Route Patterns

E) CCM Clusters

Answers: A, B, C, and D

Q6) Which type of ports can be configured for an analog gateway? (Choose two.)

A) FXO

B) FXS

C) PRI

D) T1

Answers: A and B

Q7) What can be placed into a Route List?

A) Route Groups

B) Route Patterns

C) Route Lists

D) Devices

Answer: A

Lesson 2: Advanced Route Plan

Lesson Review

Q1) Which of the following file extensions does CCM use by default to generate a route plan report?

A) .csv

B) .doc

C) .pdf

D) .txt

Answer: A

Q2) What does CCM do when dialed digits match a translation pattern?

A) extends the call to the destination

B) forwards the call to a route pattern

C) selects the closest match to that pattern

D) sends the transformed digits through digit analysis one more time

Answer: D

Q3) When DN 8500 calls and a calling transformation mask of 972555*xxxx* is applied, what CLID is sent?

A) 8500

B) 5558500

C) 9725558500

D) 19725558500

Answer: C

Q4) What are the final digits CCM sends when the discard digits instruction PreDot is applied to the 9.8085551212 pattern?

A) 98085551212

B) 5551212

C) 95551212

D) 8085551212

Answer: D

Q5) Network administrators use route filters with which route pattern wildcard?

A) *x*

B) ?

C) !

D) @

Answer: D

Lesson 3: Telephony Class of Service

Lesson Review

Q1) Which three of the following problems are addressed with calling search spaces and partitions? (Choose three.)

A) routing by geographical location

B) routing by tenant

C) routing by class of user

D) routing by devices

Answers: A, B, and C

Q2) Which of the following best describes a partition?

A) a logical grouping of route patterns

B) a logical grouping of telephone devices

C) a logical grouping of gateway devices

D) a logical grouping of route lists

Answer: A

Q3) Which of the following best describes a calling search space?

A) ordered list of partitions

B) ordered list of route patterns

C) route patterns with similar calling capabilities

D) route Groups with similar calling capabilities

Answer: A

Q4) Which of the following should occur during an emergency call?

A) The call should be routed across the WAN to the local PSTN.

B) The call should be routed to the local PSTN.

C) The call should not be routed.

D) The call should be routed using route lists.

Answer: A

Q5) Which of the following is not a deployment scenario recommended to use with Cisco ER?

A) single or multi-cluster call-manager installations with 48+ IP phones per site

B) extends E9-1-1 support to include extension mobility and/or IP phones that move between cubicles, offices, floors, buildings, or campuses

C) shared line appearances on telephones in multiple physical locations

D) small offices with fewer than 48 telephones

Answer: D

Lesson 4: Call Admission Control and Survivable Remote Site Telephony

Lesson Review

Q1) Without CAC, what happens to existing calls when the next call oversubscribes the WAN?

A) all calls are dropped

B) voice quality on all calls degrades

C) voice calls on the last call degrades

D) nothing

Answer: B

Q2) If a gatekeeper is configured as an anonymous device, what other function does the gatekeeper provide besides CAC?

A) intercluster trunk

B) digit analysis extension

C) voice quality debugger

D) firewall

Answer: A

Q3) How do the IP Phones in a branch site know to register to the gateway running SRST?

A) The telephone is part of the CallManager list.

B) The IP address is configured on the gateway.

C) It is the default gateway IP address as part of the DHCP scope.

D) None of the above.

Answer: C

Q4) Which two of these options describe how endpoints achieve gatekeeper discovery? (Choose two.)

A) Autodiscovery

B) Manual discovery

C) assigned by the voice router

D) assigned by the CAC server

Answers: A and B

Q5) Which of these options would you configure for available bandwidth within the CCMAdmin window for CAC?

A) location

B) region

C) device pool

D) device defaults

Answer: A

Module 4: Features Plus

Lesson 1: Media Resources

Lesson Review

Q1) Which of these services does an MTP resource provide for an H.323v1 type gateway?

A) transcoding services

B) MOH

C) conferencing

D) supplementary services

Answer: D

Q2) When is it recommended to run the audio translator?

A) any time of the day

B) during peak call processing hours

C) during off-peak hours

D) none of the above

Answer: C

Q3) Which of these statements best describes MRGLs?

A) an ordered list of media resources

B) an ordered list of media gateways

C) an ordered list of media resource groups

D) none of the above

Answer: C

Q4) Which of these services do media resources provide?

A) MOH

B) unicast conference bridge

C) media streaming application server

D) transcoding

E) multiplexing

Answer: D

Q5) Which of these are needed to configure a Catalyst 6000 hardware CFB?

A) MAC address

B) IP address

C) port address

D) Meet-Me number

Answer: A

Q6) Which of these items takes the output stream of one codec and converts it from one compression type to another?

A) transcoder device

B) MTP

C) CFB

D) device pool

Answer: A

Lesson 2: Softkey Template

Lesson Review

Q1) Which two models of Cisco IP Phones can accept softkey templates? (Choose two.)

A) 7960

B) 7940

C) 7910

D) 7905

Answers: A and B

Q2) Where are softkey templates located?

A) Device Menu

B) Service Menu

C) Tools Menu

D) Plug-ins Menu

Answer: A

Q3) How do you create a nonstandard softkey template?

A) copy the template from a standard template

B) create the template from the beginning

C) you cannot create a nonstandard template

D) add the template to the application

Answer: A

Q4) What must you do after making a modification to a softkey template?

A) restart the device

B) reboot the server

C) reboot the gateway

D) reboot the voice router

Answer: A

Q5) Which three of these areas can you use to assign a softkey template to a device? (Choose three.)

A) device pools

B) user profile

C) device

D) Template Configuration window

Answers: A, B, and C

Q6) What can impact and prevent the deletion of a softkey template?

A) The template is associated with a device.

B) The nonstandard template is associated with a standard template.

C) The standard template is associated with a nonstandard template.

D) None of these.

Answer: A

Lesson 3: Features

Lesson Review

Q1) Which of these provide the configured call park range or DN?

A) publisher server

B) primary CCM

C) backup CCM

D) none of the above

Answer: B

Q2) Who is responsible for configuring all of the Cisco IP Phone services available?

A) end users

B) PBX administrators

C) local CO technician

D) CCM administrator

Answer: D

Q3) Which of these features forwards a call to voice mail?

A) call forward

B) redial

C) barge

D) hold

Answer: A

Q4) Which of these features is NOT an option with shared line appearances?

A) DND

B) auto answer

C) call forward

D) redial

Answer: B

Q5) Which three of these features are configurable for the manager IP Phone in the IPMA configuration? (Choose three.)

A) DND

B) SAC

C) Call filtering

D) call handling from the desktop

Answer: A, B, and C

Lesson 4: Cisco IP Telephony Users

Lesson Review

Q1) Which of these fields is NOT required when configuring a user? (Choose two.)

A) First Name

B) Last Name

C) User ID

D) Manager User ID

Answers: A and D

Q2) Which two of these fields must the user complete in order to log on to the Cisco CallManager User Options page? (Choose two.)

A) User ID

B) Password

C) PIN

D) Full Name

Answers: A and B

Q3) Which protocol does the CCM use to interface with the user database server?

A) X.500

B) LDAP

C) XML

D) TCP/IP

Answer: B

Q4) In order to allow a user to use the Cisco IP SoftPhone, which option must you select?

A) Enable SoftPhone Use

B) Enable XML Application Use

C) Enable Softphone Access

D) Enable CTI Application Use

Answer: D

Q5) What URL should you provide to users to allow access to the User Options page?

A) http://<server_name>/ccmuser/Logon.asp

B) http://<server_name>/ccmuser/Logon.htm

C) http://<server_name>/ccmadmin/Logon.asp

D) http://<server_name>/ccmadmin/Logon.htm

Answer: A

Q6) What option is a user NOT able to configure from the User Options page?

A) Call Forwarding

B) Message Waiting Lamp Policy

C) IP Phone Services

D) Voice Mail Retrieval

Answer: D

Q7) Using the default 7960 phone template, how many speed dials is a user able to configure on their 7960 Cisco IP Phone?

A) 2

B) 4

C) 6

D) 10

Answer: B

Q8) What programming language is used to support the user services on the 7940/7960 Cisco IP Phones?

A) X.500

B) LDAP

C) XML

D) TCP/IP

Answer: C

Q9) How many user locale languages are included in the default CCM installation?

A) 1

B) 2

C) 6

D) 15

Answer: A

Module 5: Applications

Lesson 1: CCM Attendant Console

Lesson Review

Q1) Which of the following terms best describes the number that users would dial to reach a receptionist?

A) hunt group

B) pilot number

C) Cisco Attendant Console DN

D) all of the above

Answer: B

Q2) Which of the following are valid line states in the CCM Attendant Console client? (Choose all that apply.)

A) Idle

B) Active

C) Ringing

D) Unknown

Answers: A, B, C, and D

Q3) The CCM Attendant Console client software interfaces directly with which of the following CCM components?

A) CiscoAC.dll

B) hunt group

C) pilot point

D) TCD

Answer: D

Q4) To function correctly, what user must you create for the CCM Attendant Console?

A) ac

B) proxy

C) transparent

D) CAC

Answer: A

Q5) To run the CCM Attendant Console, what must a client workstation have?

A) a recent Microsoft operating system

B) a Cisco IP Phone in close proximity

C) the LDAP CCM Attendant Console user information

D) all of the above

Answer: D

Lesson 2: Cisco IP SoftPhone

Lesson Review

Q1) Which three of the following are not features of the Cisco IP SoftPhone? (Choose three.)

A) It can function as a stand-alone IP Phone.

B) It can control hardware IP Phone.

C) It can integrate with LDAPv3 directories.

D) It has built-in VPN capabilities.

E) It automatically marks voice traffic with type of service (ToS) or class of service (CoS) of 5

Answers: A, B, and C

Q2) How many device weight units does Cisco IP SoftPhone consume?

A) 1

B) 3

C) 5

D) 20

E) 25

Answer: D

Q3) On the user configuration page, what is the check box that you must check to allow that user to use Cisco IP SoftPhone?

A) enable Cisco IP SoftPhone use

B) enable CTI port use

C) enable CTI application use

D) enable TAPI application use

Answer: C

Q4) Which of the following does the user NOT need to input when installing Cisco IP SoftPhone?

A) CTI port name

B) user ID

C) password

D) CCM IP addresses

Answer: A

Q5) When a user logs into telephone using the Extension Mobility feature, what is pushed to the telephone?

A) the telephone configuration that the user uses at the desk

B) an automatically generated device setting

C) an automatically generated device profile

D) the device profile associated with the user

Answer: D

Q6) The user configured in CRS for the generic application must be configured in CCM for which of the following functions?

A) default device profile

B) default user for device profiles

C) authenticate proxy rights

D) authenticate device profile rights

Answer: C

Lesson 3: Cisco Voice over IP Integrated Applications

Lesson Review

Q1) _____ must be configured if you want to enable rule-based call routing and allow Personal Assistant to intercept calls.

A) partitions

B) gateways

C) gatekeepers

D) all of the above

Answer: A

Q2) Which of the following is NOT part of CRS?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Answer: D

Q3) Which of the following generates interactive voice prompts and provides call automation?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Answer: A

Q4) Which of the following provides simple call-answering and call-forwarding services?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Answer: B

Q5) Which of the following is an inexpensive, easy-to-install, and easy-to-use ACD?

A) IP IVR

B) IP AA

C) IP ICD

D) IPCC

Answer: C

Q6) In IPCC, which of the following products provides the ACD functionality?

A) IP IVR

B) ICM

C) CCM

D) CRS

Answer: B

Q7) Which of the following best describes the Cisco Conference Connection?

A) an audio conference server for scheduled conferences

B) an audio conference server to mix voice streams

C) an audio conference module for scheduled conferences

D) an audio conference module to mix voice streams

Answer: A

Q8) When using Cisco Unity for unified messaging, which three of the following applications are part of the unified messaging solution? (Choose three.)

A) Voice mail

B) E-mail

C) Fax

D) Paging

Answers: A, B, and C

Module 6: Manageability and Monitoring Tools

Lesson 1: Bulk Administration Tool

Lesson Review

Q1) Which of these tools allows you to complete bulk adds, updates, and deletions?

A) TAPS

B) BAT

C) CRA

D) CDR

Answer: B

Q2) Which server must have BAT installed on it?

A) publisher server

B) subscriber server

C) primary server

D) secondary server

Answer: A

Q3) What must you do before you are able to select the IP Phone Button template for the IP Phone template configuration?

A) select the number of lines to configure

B) select the line number to configure

C) select the device type to configure

D) select the device pool of the IP Phone

Answer: A

Q4) Which of these files is necessary to create BAT templates in Excel?

A) BAT.xlt

B) BAT.xls

C) BAT.csv

D) BAT.avr

Answer: A

Q5) Which of the following items should you use to check the status of your insertion process?

A) view latest log file

B) status line

C) Event Viewer

D) CDR Records

Answer: B

Q6) Which two items must be installed for TAPS to function properly? (Choose two.)

A) CRS

B) BAT on the publisher server

C) plug-ins

D) Extension Mobility

Answers: A and B

Lesson 2: Internal Server Tools

Lesson Review

Q1) Which of the following logs from Event Viewer do you use to view system startup errors?

A) Application logs

B) System logs

C) Security logs

D) Diagnostic logs

Answer: A

Q2) Which of these servers contains the read/write copy of the database?

A) publisher

B) subscriber

C) primary

D) secondary

Answer: A

Q3) Where is the current CCM component version located?

A) Application

B) Tools

C) Help

D) Services

Answer: C

Q4) Which of these command-line tools would you use to re-establish a broken MetaLink connection?

A) show command-line tools

B) avid command-line tools

C) ping command-line tool

D) netstat command-line tool

Answer: B

Q5) Which of these tools can you enable to automatically notify the CCM administrator or other support personnel, in the event of a failed service?

A) Alarm

B) Trace

C) Serve Activation

D) Collection

Answer: A

Q6) Which of these counters does the RTMT poll for updated information?

A) performance counters in Windows 2000

B) performance counters in Windows 2000 Event Viewer

C) performance counters in Microsoft SQL

D) performance counters in Trace files

Answer: A

B

Course Glossary

Acronym or Term	Expansion of Acronym
AA	analog access
AAL	ATM adaption Layer
AAR	Automated Alternate Routing
ACD	automatic call distributor
ACF	Admission Confirmation
ALI	Automatic Location Identification
ANI	Automatic Number Identification
API	application programming interface
ARJ	Admission Reject
ARQ	Admission Request or Automatic Repeat Request
ART	Administrative Reporting Tool
ASR	Cisco Application Specific Routing Feature
AST	Admin Serviceability Tool
ATA	Analog Telephone Adaptor
AUCX	AuditConnection
AUEP	AuditEndpoint
AVVID	Cisco Architecture for Voice, Video and Integrated Data
BAT	Bulk Administration Tool
BCF	Bandwidth Confirmation
BCMSN	Building Cisco Multilayer Switched Networks
BHCA	busy hour call attempt
BLF	busy lamp field
BRJ	Bandwidth Reject
BRQ	Bandwidth Request
CAC	Call Admission Control
CAM	content-addressable memory
CAMA	Centralized Automated Message Accounting
CAS	channel- associated signaling
CCM	Cisco CallManager
CCNA	Cisco Certified Network Associate
CCS	common channel signaling
CDP	Cisco Discovery Protocol
CDR	Call Detail Record
CFB	Conference Bridge
CIPT	Cisco IP telephony
Cisco AVVID	Cisco Architecture for Voice, Video and Integrated Data
Cisco TSP	Cisco TAPI Service Provider

Acronym or Term	Expansion of Acronym
Cisco XML SDK	Cisco software development kit
CIT	Computer Telephony Interface
CLI	Call Leg Identifier
CLI	command-line interface
CLID	Calling Line Identifier
CMG	CallManager Group
CO	central office
codec	coder-decoder
CoS	class of service
CQS	Cisco Qualified Specialist
CRCX	create connection
CRS	Cisco Customer Response Solution
CSV	comma separated values
CTI	computer telephony integration
CTIQBE	computer telephony integration quick buffer encoding
CVOICE	Cisco Voice over Frame Relay, ATM and IP
DBL	Database C++ layer
DC	direct current
DC-Directory	Data Connection Directory
DCF	Disengage Confirmation
DCS	Digital Crossconnect System
DDI	discard digits instruction
DE	discard eligible
DHCP	Dynamic Host Configuration Protocol
DIB	Directory Information Database
DID	Direct Inward Dial
DLL	dynamic link library
DN	directory number
DND	Do Not Disturb
DNS	Domain Name System
DOD	Direct Outward Dial
DQoS	Deploying Quality of Service
DRQ	Disengage Request
DSCP	Differentiated Services Code Point
DSL	digital subscriber line
DSP	digital signal processor
DSS	direct station select

Acronym or Term	Expansion of Acronym
DTMF	Dual Tone Multi-Frequency
E&M	recEive and transMit
EFR	enhanced full-rate
EOL	End of Life
ER	Emergency Response
Eru	Cisco Emergency Responder
FIFO	First in First Out
FLP	Fast Link Pulse
FTP	File Transfer Protocol
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GBIC	Gigabit Interface Converter
GCF	Gatekeeper Confirmation
GRJ	Gateway Reject
GRQ	Gatekeeper Request
GUI	graphical user interface
HAC	Hearing-aid-compatible
HSRP	Hot Standby Router Protocol
ICD	Integrated Contact Distribution
IIS	Internet Information Server
ICM	Intelligent Call Management
IP AA	IP Auto Attendant
IP ICD	IP Integrated Content Distribution
IP IVR	IP Interactive Voice Response
IPCC	(Cisco) IP Contact Center
IPMA	IP Manager Assistant
IPTT	IP Telephony Troubleshooting
IRQ	Interrupt Request
IVR	interactive voice response
JTAPI	Java Telephony Application Programming Interface
KA	Keepalive
LCD	liquid crystal display
LDAP	Lightweight Directory Access Protocol
LEC	local exchange carrier
LFI	Link Fragmentation and Interleaving
MCM	Multimedia Conference Manager
MCU	Multipoint Controller Unit

Acronym or Term	Expansion of Acronym
MDCX	CreateConnection
MGCP	Media Gateway Control Protocol
MLPPP	multilink point-to-point protocol
MOH	Music On Hold
MOS	mean opinion score
MRG	media resource group
MRGL	media resource group list
MRM	Media Resource Manager
MRP	multiservice route processor
MTP	Media Termination Point
MTS	Microsoft Transaction Server
NANP	North American Numbering Plan
NM	network module
NT	Network Termination
NTFY	Notify
NXXs	office exchange codes
ODBC	Open DataBase Connectivity
OS	operation system
OSI	Open System Interconnection reference model
PCM	Pulse Code Modulation
PDA	personal digital assistant
PFC	Policy Feature Card
PIN	personal identification number
PLAR	private line, automatic ringdown
POTS	plain old telephone service
PS/ALI	Public Service Automatic Location Information
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTT	Post, Telephone, and Telegraph
PVID	Port VLAN ID
QBE	quick buffer encoding
QM	Queue Manager
QoS	quality of service
QSIG	Q Signaling
RAID	Redundant Array of Independent Disks
RCF	Registration Confirmation
RG	route group

Acronym or Term	Expansion of Acronym
RIS	Real-Time Information Server
ROI	return on investment
RPC	Remote-procedure call
RQNT	NotificationRequest
RRJ	Registration Reject
RRQ	Registration Request
RSIP	RestartInProgress
RTMT	Real-Time Monitoring Tool
RTP	Real-Time Transport Protocol
RU	rack unit
RUDP	Reliable User Data Protocol
SAA	Selsius Analog Access
SAC	Send All Calls
SAP	System alarm processor
SCCP	Skinny Client Control Protocol
SDA	Selsius Digital Access
SDI	Selsius Diagnostic Interface
SDL	system diagnostic layer
SDP	Session Definition Protocol
SEP	Selsius Ethernet Phone
SIP	Session initiation protocol
SIW	Service InterWorking
SMDI	Simplified Message Desk Interface
SNAP	simple network automated provisioning
SNMP	Simple Network Management Protocol
SPE	system processing engine
SQL	Structured Query Language
SRST	survivable remote site telephony
SRTS	Survivable Remote Telephony Solution
SSP	system switch processor
STI	Spirian Technologies, Inc.
TAC	Cisco Technical Assistance Center
TAPI	Telephony Application Programming Interface
TAPS	Tool for Auto Registration Phone Support
TCD	Telephony Call Dispatcher
TCDSRV	Telephony Call Dispatcher Service
TCP KA	TCP Keepalive

Acronym or Term	Expansion of Acronym
TDM	time-division multiplexing
TIFF	Tag Image File Format
TLV	Type-Length-Value
TO	time-out
ToS	type of service
TSPI	TAPI Service Provider Interface
TSS	Transaction Support System
TSV	tab separated values
TTL	Time to Live
UBR	Unspecified bit rate
UCF	Unregister Confirmation
UDP	User Datagram Protocol
UNC	Universal Naming Convention
UPC	usage parameter control
UPS	uninterruptible power supply
URJ	Unregister Reject
URQ	Unregister Request
USB	universal serial bus
UTP	unshielded twisted-pair
VAD	voice activity detection
VBR	variable bit rate
VCard	virtual business cards
VIC	voice interface card
VM	voice mail
VM	voice messaging
VoATM	Voice over ATM
VoFR	Voice over Frame Relay
VoIP	Voice over IP
VQ	Voice Quality
VVID	voice VLAN ID
VWIC	Voice/WAN interface card
WIC	WAN interface card
WINS	Windows Internet Naming Service
WRED	weighted random early detection
WRR	Weighted Round Robin
XCODE	Transcoder
XML	Extensible Markup Language

Cisco IP Telephony Laboratory Exercises

Laboratory Exercise: Installing Cisco CallManager Server Operating System

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Supported Cisco IP Telephony server platform with monitor, keyboard, and mouse
- Installation CDs for the supported platform being installed
- Cisco Catalyst Switch (6000, 4000, 3500, 2900)
- RJ-45 straight through Ethernet cables
- Cisco CallManager (CCM) application installation CD

Exercise Objective

In this exercise, you will install CCM on a supported Cisco IP Telephony server.

After completing this exercise, you will be able to:

- Install the operating system for an IP Telephony server

Command List

The commands used in this exercise are described in the table here.

Table: MS DOS Commands

Command	Description
`Ping`	Packet internet groper, ICMP echo message and its reply, often used in IP networks to test the reachability of a network device

Job Aids

These job aids are available to help you complete the laboratory exercise(s):

Table: Data for Task One

Cluster name	Publisher		Subscriber		Time Zone	Default Gateway IP Address
	Computer Name	IP Address	Computer Name	IP Address		
East 1	EAST1A	172.16.10.5	EAST1B	172.16.10.6	Eastern	172.16.10.1
East 2	EAST2A	172.16.20.5	EAST2B	172.16.20.6	Eastern	172.16.20.1
East 3	EAST3A	172.16.30.5	EAST3B	172.16.30.6	Eastern	172.16.30.1
East 4	EAST4A	172.16.40.5	EAST4B	172.16.40.6	Eastern	172.16.40.1
West 1	WEST1A	172.32.10.5	WEST1B	172.32.10.6	Pacific	172.32.10.1
West 2	WEST2A	172.32.20.5	WEST2B	172.32.20.6	Pacific	172.32.20.1
West 3	WEST3A	172.32.30.5	WEST3B	172.32.30.6	Pacific	172.32.30.1
West 4	WEST4A	172.32.40.5	WEST4B	172.32.40.6	Pacific	172.32.40.1

Table: Configuration Data Sheet for a Cisco IP Telephony Server

Operating System		
Configuration	**Your Entry Data**	
Cisco Product key	`BTOO VQES CCJU IEBI`	
User name	Administrator	
Name of your organization	cisco	
Computer name		
DNS Domain suffix	dal-trn.cisco.com	
Workgroup	CIPT	
Current time zone, date, and time		
DHCP parameters **Cisco recommends that you program a fixed IP address in TCP/IP properties for the server instead of using DHCP**		
TCP/IP properties (required if DHCP is not used) IP address	IP Address:	
Subnet mask Default gateway	Subnet mask: **255.255.255.0**	
	Default gateway:	
DNS servers (optional)	NONE	
LMHost Information	IP Address	Server Name
Publisher Information		
Subscriber Information		
Laboratory Exercise—Cisco CallManager Installation		
Database server		
Password of publisher	cisco	
Backup		
New system administrator password	cisco	
sa password	cisco	
DC Directory	cisco	

Exercise Procedure

Complete these steps:

Step 1 Locate CD #1 supplied by the instructor for the server platform you are working with.

Step 2 Power on the server and insert CD #1 while the server is booting up.

Step 3 The Cisco IP Telephony Application Server QuickBuilder welcome window opens. Click **Next**.

Step 4 The Type of Installation window opens. Select **New Installation**, and click **Next**.

Step 5 The next window displays a warning that your configuration and data will be overwritten. Click **Next**.

Step 6 When a message prompts you to cycle the system power, turn the server off. Wait 10 seconds and then power up the server. (The system will reboot itself a 2nd time. Upon startup, press **F1** to bypass the BIOS setup information when prompted.)

Step 7 If the New Installation and Replacement window opens, click **Next**.

Step 8 If the Configuration Process window opens with a message about hardware detection, click **Next**. The system reboots automatically.

Step 9 When a message prompts you to power off and on the server to complete the installation, turn the server off. Wait 10 seconds and then power up the server. (During the bootup, press **F1** if prompted to continue.)

Step 10 Enter your product key from the worksheet, and click **Next**.

Step 11 The End User License Agreement window opens. Read through the contents of the agreement. If you consent to the terms of the agreement, click **I Agree**. If you do not consent, you must terminate the installation by clicking **Exit**.

Step 12 Depending on the state of your server, the Server Replacement Option window may or may not appear. If it does appear, make sure the **I am recovering a system from backup check box** is not selected, and click **Next**.

Step 13 Click **Next** on the Ready to Complete Installation window. This process takes about five minutes to complete.

Entering Server Configuration Data and Completing the Operating System Installation

Use the data you collected in the worksheet above to complete the following steps to configure each server:

Step 14 The Cisco IP Telephony Applications Server Configuration Wizard begins. Click **Next** to continue.

Step 15 After the Cisco Registration window opens, enter your user name, the name of your organization, a computer name, and the DNS suffix, and click **Next**.

Step 16 Choose to become a workgroup member, and enter the workgroup name. Click **OK**.

Step 17 Choose the appropriate time zone for the server. Set the current date and time, and click **Next**.

Step 18 The Static Dynamic IP Address window opens. Select **Use the following IP address** when prompted about the method used to configure the IP information.

Step 19 Enter the server IP address, subnet mask, and default gateway in the appropriate fields, and click **Next**. (Do not enter a DNS server.)

Step 20 Configure local name resolution by updating the lmhosts file with IP address and hostname information for every server in your cluster in the worksheet.

The Windows 2000 SNMP agent provides security through the use of community names and authentication traps. All SNMP implementations universally accept the default name “public.” You should change this name to limit access.

Step 21 In this laboratory exercise, leave the default name “public”, and select **Next**.

Step 22 The installation process enables Telnet and Terminal services automatically. Select **Next**.

Step 23 The CD-ROM drive automatically opens. Remove the CD from the CD-ROM drive, and insert the CD # that the system is prompting for into the CD-ROM drive. The configuration process continues automatically after detection of the appropriate CD-ROM. The server begins an installation and reboot process that takes about 6 minutes to complete.

Step 24 The CD-ROM drive automatically opens. When prompted, remove the CD and click any key to reboot. Windows 2000 setup begins and takes about 10 minutes to complete. Do not power down the server or click any keys during setup.

Step 25 The server will reboot. If prompted to press F1 to continue, F9 for Rom-Based Setup Utility, F10 for System partition utilities, or F12 for PXE Book, press **F9** to enter the Rom-Based Setup Utility. Arrow down to the advanced options menu, and press **Enter**. Arrow down to the Post F1 Prompt menu option, and press **Enter**. Use the arrow keys again to select **disable**, and press **Enter**. Press **Esc** twice and **F10** to save and exit. The server will then reboot and no longer prompt you to press F1 to continue the bootup process.

Step 26 A dialogue box appears asking for the windows administrator password. Complete this information from the configuration data sheet. Click **OK** and the server will reboot.

Step 27 Press **Ctrl-Alt-Del** to log onto the server. Enter the user name of administrator and the password that you entered for this account.

Exercise Verification

You have completed this exercise when you attain these results:

- The dialog box appears requesting for the Cisco CallManager CD to be installed.

Laboratory Exercise: Installing Cisco CallManager and Post-Installation Tasks

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Supported Cisco IP Telephony server platform with monitor, keyboard, and mouse
- Installation CDs for the supported platform being installed
- Cisco Catalyst Switch (6000, 4000, 3500, 2900)
- RJ-45 straight through Ethernet cables
- Cisco CallManager application installation CD

Exercise Objective

In this exercise, you will install Cisco CallManager on a supported Cisco IP Telephony server.

After completing this exercise, you will be able to:

- Install the Cisco CallManager application that completes the installation of an IP Telephony server
- Change passwords for all the servers in a Cisco IP Telephony server cluster
- Back up the Cisco CallManager Publisher database

Command List

The commands used in this exercise are described in the table here.

Table: MS DOS Commands

Command	Description
`Ping`	Packet internet groper, ICMP echo message and its reply, often used in IP networks to test the reachability of a network device

Job Aids

These job aids are available to help you complete the laboratory exercise(s):

Table: Data for Task One

Cluster name	Publisher		Subscriber		Time Zone	Default Gateway IP Address
	Computer Name	IP Address	Computer Name	IP Address		
East 1	EAST1A	172.16.10.5	EAST1B	172.16.10.6	Eastern	172.16.10.1
East 2	EAST2A	172.16.20.5	EAST2B	172.16.20.6	Eastern	172.16.20.1
East 3	EAST3A	172.16.30.5	EAST3B	172.16.30.6	Eastern	172.16.30.1
East 4	EAST4A	172.16.40.5	EAST4B	172.16.40.6	Eastern	172.16.40.1
West 1	WEST1A	172.32.10.5	WEST1B	172.32.10.6	Pacific	172.32.10.1
West 2	WEST2A	172.32.20.5	WEST2B	172.32.20.6	Pacific	172.32.20.1
West 3	WEST3A	172.32.30.5	WEST3B	172.32.30.6	Pacific	172.32.30.1
West 4	WEST4A	172.32.40.5	WEST4B	172.32.40.6	Pacific	172.32.40.1

Table: Configuration Data Sheet for a Cisco IP Telephony Server

Operating System		
Configuration	**Your Entry Data**	
Cisco Product key	`BTOO VQES CCJU IEBI`	
User name	Administrator	
Name of your organization	cisco	
Computer name		
DNS Domain suffix	dal-trn.cisco.com	
Workgroup	CIPT	
Current time zone, date, and time		
DHCP parameters **Cisco recommends that you program a fixed IP address in TCP/IP properties for the server instead of using DHCP**		
TCP/IP properties (required if DHCP is not used) ■ IP address ■ Subnet mask ■ Default gateway	IP Address: Subnet mask: **255.255.255.0** Default gateway:	
DNS servers (optional)	NONE	
LMHost Information	IP Address	Server Name
Publisher Information		
Subscriber Information		
Laboratory Exercise—Cisco CallManager Installation		
Database server		
Password of publisher	cisco	
Backup		
New system administrator password	cisco	
sa password	cisco	
DC Directory	cisco	

Task 1: Install the Cisco CallManager Application

You will install the Cisco CallManager application and select Cisco CallManager components to install as part of the application.

Exercise Procedure

Note If you are configuring a subscriber database server, make sure the server you are installing can connect to the publishing database server before the installation can continue. This connection is necessary because the subscriber server attempts to connect to the publisher server, so that the publisher database can be copied from that server to the local drive on the subscriber server. To make sure a good connection exists between the servers, issue a **ping** command from the subscriber server to the publisher server before you try to authenticate to it. If the **ping** command is not successful, you must exit the installation program, fix the problem, and begin the installation process again.

Note The publisher database serves as the master database for all servers in the cluster. All servers except the publishing database server maintain subscriber databases, which are copies of the publisher database.

Complete these steps:

Step 1 When prompted to do so, insert the Cisco CallManager 3.3 Installation and Recovery CD-ROM. The installation script automatically continues loading from the CD-ROM.

Step 2 If a warning about running third party software appears, click **Yes** to continue.

Step 3 The Windows installer package begins the installation. (This may take several minutes.)

Step 4 At the Welcome to the Cisco CallManager Installation Wizard window, click **Next**.

Step 5 When the license agreement appears, select **I accept** to continue with the installation or **I do not accept** to terminate the installation.

Step 6 The customer Identification screen appears. Your username, organization, and CD Key information should appear in the text box. Click **Next** to continue.

Step 7 The Setup Type screen appears. Make sure that **Complete** is selected, and click **Next** to continue.

Step 8 At the Server Type window, choose the appropriate server, and click **Next**.

Step 9 You will next be prompted for the Administrator password. See the Configuration Data Sheet for a Cisco IP Telephony Server table (from the Job Aids section of this lab) for the appropriate password. Enter this information, and click **Next** to continue.

Step 10 A window may appear asking for the SQL password. See the configuration data sheet table for the appropriate password, enter this information, and click **Next** to continue.

Step 11 At the Cisco DC Directory password screen, enter the appropriate password from the Configuration Data Sheet for a Cisco IP Telephony Server table (from the Job Aids section of this lab). Click **Next** to continue.

Step 12 The Cisco Backup utility configuration is configured next. Determine whether you are the Backup server (publisher machine) or Backup target (subscriber machine), and click **Next**.

Step 13 At the Ready to Install Program window, click **Install**. The Installing Cisco CallManager screen should appear. (This may take up to 45 minutes to install).

Step 14 The Installation Wizard Complete Window appears. Click **Finish** to exit the wizard.

Step 15 A window appears asking if you would like to reboot the server. Click **Yes**.

Exercise Verification

You have completed this exercise when you attain these results:

- The dialog box appears requesting for the Cisco CallManager CD to be installed.

Task 2: Starting the CallManager Services

In this task, you will start the CallManager Services.

Exercise Procedure

Complete these steps:

Step 1 From the Cisco CallManager Administration window, select the Application window.

Step 2 Select the **Cisco CallManager Serviceability** option, and press **Enter**.

Step 3 Go to **Tools > Service Activation**.

Step 4 Select your server from the list of servers on the left hand side of the Service Activation screen.

Step 5 Select all the services, and click **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- All of the services are active.

Laboratory Exercise: Auto-Register Cisco IP Phones

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco CallManager cluster
- Cisco IP Phones (7910, 7940, 7960)
- RJ-45 straight through Ethernet cables
- Cisco Catalyst switch (6000, 4000, 3500, 2900)
- DHCP server (use Publisher server or Default gateway)

Exercise Objective

In this exercise, you will auto-register Cisco IP Phones in a CIPT cluster.

After completing this exercise, you will be able to:

- Configure a DHCP scope on the Publisher or Default gateway router
- Configure Cisco CallManager, Cisco CallManager group, auto-registration, and device pools to prepare the CIPT cluster to auto-register phones
- Configure the default device pool for devices
- Attach Cisco IP Phones to the network and they will auto-register to a Cisco CallManager

Command List

The commands used in this exercise are described in the table here.

Table: Cisco Router IOS Commands

Command	Description
`enable`	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
`configure terminal` `config t`	Enters global configuration mode.
`ip dhcp excluded-address`	Specifies the IP addresses that the DHCP server should not assign to DHCP clients.
`ip dhcp pool`	Creates a name for the DHCP server address pool and places you in DHCP pool configuration mode (identified by the config-dhcp# prompt).
`network`	Specifies the subnet network number and mask of the DHCP address pool.
`default-router`	Specifies the IP address of the default router for a DHCP client. One IP address is required, although you can specify up to eight addresses in one command line.
`option 150`	DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options.

Job Aids

These job aids are available to help you complete the laboratory exercises:

Table: DHCP Addressing and Scope Information

Cluster Name	Pool Type	Name	Network	Default Router	Option 150	Excluded Addresses
East 1	Voice	EAST1-Voice	10.16.10.0 255.255.255.0	10.16.10.1	172.16.10.5	172.16.10.1 172.16.10.10
	Data	EAST1-Data	172.16.10.0 255.255.255.0	172.16.10.1		
East 2	Voice	EAST2-Voice	10.16.20.0 255.255.255.0	10.16.20.1	172.16.20.5	172.16.20.1 172.16.20.10
	Data	EAST2-Data	172.16.20.0 255.255.255.0	172.16.20.1		
East 3	Voice	EAST3-Voice	10.16.30.0 255.255.255.0	10.16.30.1	172.16.30.5	172.16.30.1 172.16.30.10
	Data	EAST3-Data	172.16.30.0 255.255.255.0	172.16.30.1		
East 4	Voice	EAST4-Voice	10.16.40.0 255.255.255.0	10.16.40.1	172.16.40.5	172.16.40.1 172.16.40.10
	Data	EAST4-Data	172.16.40.0 255.255.255.0	172.16.40.1		
West 1	Voice	WEST1-Voice	10.32.10.0 255.255.255.0	10.32.10.1	172.32.10.5	172.32.10.1 172.32.10.10
	Data	WEST1-Data	172.32.10.0 255.255.255.0	172.32.10.1		
West 2	Voice	WEST2-Voice	10.32.20.0 255.255.255.0	10.32.20.1	172.32.20.5	172.32.20.1 172.32.20.10
	Data	WEST2-Data	172.32.20.0 255.255.255.0	172.32.20.1		
West 3	Voice	WEST3-Voice	10.32.30.0 255.255.255.0	10.32.30.1	172.32.30.5	172.32.30.1 172.32.30.10
	Data	WEST3-Data	172.32.30.0 255.255.255.0	172.32.30.1		
West 4	Voice	WEST4-Voice	10.32.40.0 255.255.255.0	10.32.40.1	172.32.40.5	172.32.40.1 172.32.40.10
	Data	WEST4-Data	172.32.40.0 255.255.255.0	172.32.40.1		

Table: DHCP Scope Options for Windows 2000 Server

Cluster Name	Pool Type	Scope Name	Start IP Address	End IP Address	Subnet Mask	Default Router	Option 150
East 1	Voice	EAST1-Voice	10.16.10.10	10.16.10.30	255.255.255.0	10.16.10.1	172.16.10.5
	Data	EAST1-Data	172.16.10.10	172.16.10.30	255.255.255.0	172.16.10.1	
East 2	Voice	EAST2-Voice	10.16.20.10	10.16.20.30	255.255.255.0	10.16.20.1	172.16.20.5
	Data	EAST2-Data	172.16.20.10	172.16.20.30	255.255.255.0	172.16.20.1	
East 3	Voice	EAST3-Voice	10.16.30.10	10.16.30.30	255.255.255.0	10.16.30.1	172.16.30.5
	Data	EAST3-Data	172.16.30.10	172.16.30.30	255.255.255.0	172.16.30.1	
East 4	Voice	EAST4-Voice	10.16.40.10	10.16.40.30	255.255.255.0	10.16.40.1	172.16.40.5
	Data	EAST4-Data	172.16.40.10	172.16.40.30	255.255.255.0	172.16.40.1	
West 1	Voice	WEST1-Voice	10.32.10.10	10.32.10.30	255.255.255.0	10.32.10.1	172.32.10.5
	Data	WEST1-Data	172.32.10.10	172.32.10.30	255.255.255.0	172.32.10.1	
West 2	Voice	WEST2-Voice	10.32.20.10	10.32.20.30	255.255.255.0	10.32.20.1	172.32.20.5
	Data	WEST2-Data	172.32.20.10	172.32.20.30	255.255.255.0	172.32.20.1	
West 3	Voice	WEST3-Voice	10.32.30.10	10.32.30.30	255.255.255.0	10.32.30.1	172.32.30.5
	Data	WEST3-Data	172.32.30.10	172.32.30.30	255.255.255.0	172.32.30.1	
West 4	Voice	WEST4-Voice	10.32.40.10	10.32.40.30	255.255.255.0	10.32.40.1	172.32.40.5
	Data	WEST4-Data	172.32.40.10	172.32.40.30	255.255.255.0	172.32.40.1	

Table: Cisco CallManager Configuration

Cluster Name	Publisher			Subscriber			Auto Registration Directory Number Range	
	CallManager Name	IP Address	Server Function	CallManager Name	IP Address	Server Function	Start	End
East 1	EAST1A	172.16.10.5	Publisher/Backup	EAST1B	172.16.10.6	Primary/Subscriber	1000	1999
East 2	EAST2A	172.16.20.5		EAST2B	172.16.20.6		2000	2999
East 3	EAST3A	172.16.30.5		EAST3B	172.16.30.6		3000	3999t
East 4	EAST4A	172.16.40.5		EAST4B	172.16.40.6		4000	4999
West 1	WEST1A	172.32.10.5		WEST1B	172.32.10.6		1000	1999
West 2	WEST2A	172.32.20.5		WEST2B	172.32.20.6		2000	2999
West 3	WEST3A	172.32.30.5		WEST3B	172.32.30.6		3000	3999
West 4	WEST4A	172.32.40.5		WEST4B	172.32.40.6		4000	4999

Task 1: Configure the DHCP Service

You will configure the DHCP service on either the Default Router or the Publisher server to provide IP address and other scope options to network devices.

Exercise Procedure

Complete these steps:

DHCP on a Router

You will configure an IP DHCP pool on a given router. Write down the IP address of the router that you will be working on (provided by the instructor):

Step 1 Enter configuration mode. After connecting to the router, you will be in user mode. To enter privilege mode, enter "enable" with password "cisco". From privilege mode, enter configuration mode by entering "configure terminal" or "config t".

Step 2 Exclude IP addresses from the DHCP pool.

```
ip dhcp excluded-address <Excluded Addresses>
```

Step 3 Configure an IP DHCP Pool for Voice by entering the following commands:

```
ip dhcp pool <Voice Name>
network <Voice Network><Subnet mask>
default-router <Voice Default Router>
option 150 ip <Option 150>
```

Step 4 Configure the DHCP Pool for Data using the following commands:

```
ip dhcp pool <Data Name>
network <Data Network><Subnet mask>
default-router <Data default router>
option 150 ip <Option 150>
```

DHCP on the Publisher

You will configure the DHCP service to run on the Publisher.

Note	Cisco Systems, Inc. does not recommend this lab for a CIPT solution, but if you have not configured the DHCP service on a Windows 2000 platform, this will provide the basic steps.

Step 5 On the Publisher, go to **Start** > **Programs** > **Administrative Tools** > **Services** to open the services.

Step 6 Scroll down to the DHCP Server service, and right-click to select **Properties**.

Step 7 Set the Startup Type to Automatic, and click **Apply**. Click **Start** to start the service, and click **OK**.

Step 8 Open the DHCP server service by going to **Start** > **Programs** > **Administrative Tools** > **DHCP**.

Step 9 Click the "plus" symbol next to the "server name [IP Address]" to view the Server Options folder.

Step 10 Right-click the **server name [IP address]**, and select **Set Predefined Options**.

Step 11 When the Predefined Options and Values box is opened, click **Add**.

Step 12 For the Name, enter "Cisco TFTP", for the Data Type, select **IP Address**, for the Code, enter "150", and for the Description, enter "Cisco TFTP server IP Address".

Step 13 Click **OK**.

Step 14 In the Predefined Options and Value box, enter the IP address of the Publisher server for the Value, and click **OK**.

Step 15 Right-click the **server name [IP address]**, and select **New Scope**.

Step 16 When the New Scope Wizard opens, click **Next**.

Step 17 Enter "Data Scope Name" for the scope Name, enter "Network devices not phones" for the Description, and click **Next**.

Step 18 Using the information in the DHCP Scope Options for Windows 2000 Server table (from the Job Aids section of this lab), enter the Start, End, and Subnet Mask IP addresses, and click **Next**.

Step 19 At the Add Exclusions page, click **Next**.

Step 20 At the Lease Duration page, click **Next**.

Step 21 At the Configure DHCP Options page, ensure that the **Yes, I want to configure these options now** option is selected, and click **Next**.

Step 22 Enter the Default Router IP address, and click **Add**. Click **Next**.

Step 23 At the Domain Name and DNS Servers page, click **Next**.

Step 24 At the WINS Servers page, click **Next**.

Step 25 At the Activate Scope page, ensure that the **Yes, I want to activate this scope now** option is selected, and click **Next**.

Step 26 Click **Finish**.

Step 27 Next to the Scope[IP Address]"scope name" folder, click the "plus" sign to expand that directory.

Step 28 Right-click the **Scope Options** folder, and select **Configure Options** to add option 150 to this scope.

Step 29 Scroll down to select the **Option code 150** check box and ensure that the IP address is the IP address of the Publisher server (where the Cisco TFTP service is running).

Step 30 Click **Apply**, and click **OK**.

Step 31 Repeat Steps 18 through 26 to add a scope for the IP Phones (Voice).

Exercise Verification

You have completed this exercise when you attain these results:

- After plugging in the IP Phones in Task 4, the phones will obtain an IP address. Retrieve the IP address of the Cisco TFTP server and register to the Cisco CallManager.

Task 2: Configure Cisco CallManager Administration for Auto-Registration

You will to configure the servers and Cisco CallManagers in your cluster to prepare for connecting devices.

Exercise Procedure

Complete these steps:

Step 1 From the Publisher server, go to **Start > Programs > Cisco CallManager 3.3 > Cisco CallManager Administration**, and enter the user name and password to open the Cisco CallManager administration page.

Step 2 In Cisco CallManager administration, go to **System > Server** to open the Server Configuration page.

Step 3 Enter the server name and the IP address of the servers in your cluster into the following table:

Server Name	IP Address			

Step 4 Select one of the servers from the left column. Change the name of the server to the IP address of that server by deleting the name that appears in the DNS/IP Address field and replacing it with the IP address for that server.

Step 5 Select **Update**.

Step 6 Repeat Steps 4 and 5 for the next server.

Cisco CallManager Configuration

Step 7 Go to **System > Cisco CallManager** to open the Cisco CallManager Configuration page.

You are now going to select the publisher server in the cluster, edit the Cisco CallManager name, and fill in the description with the function of the server from the table above.

Step 8 Select the name of the publisher server from the left column.

Step 9 Delete the “CM_” that prefixed the Cisco CallManager name.

Step 10 Enter the function of the server in the cluster into the Description box.

Step 11 Select **Update**.

You are now going to select the other server in the cluster, edit the Cisco CallManager name, fill in the description with the function of the server, and set up auto-registration.

Step 12 Select the name of the other server still prefixed with “CM_”.

Step 13 Delete the “CM_” that prefixed the Cisco CallManager name.

Step 14 Enter the function of the server in the cluster in the Description box.

Step 15 Scroll down to deselect the **Auto-registration Disabled on this Cisco CallManager** check box.

Step 16 Enter the starting and ending directory number from the Cisco CallManager Configuration table.

Step 17 Select **Update**.

Cisco CallManager Groups

Step 18 Go to **System > Cisco CallManager Group** to open the Cisco CallManager Group Configuration page in the CCM Administrator page.

Step 19 Enter "AB_CMG" for Cisco CallManager Group 1 for the Cisco CallManager Group name.

Step 20 Highlight the server **XXXXNA** (where XXXX is the cluster identification and N is the cluster number, e.g. EAST1) in the Available Cisco CallManagers box and using the arrow between the two boxes, move it to the Selected Cisco CallManagers box.

Step 21 Highlight the server **XXXXNB** (where XXXX is the cluster indentification and N is the cluster number, e.g. EAST1) in the Available Cisco CallManagers box, and using the arrow between the two boxes move it to the Selected Cisco CallManagers box.

Step 22 Use the up and down arrows to ensure that the "A" CallManager is at the top of the list, making it the primary CallManager for the group.

Step 23 Select **Insert**. Verify in the left hand column that the AB_CMG Cisco CallManager Group is shown.

Step 24 Create a new Cisco CallManager Group "BA_CMG".

Step 25 Highlight the server **XXXXNA** (where XXXX is the cluster identification and N is the cluster number, e.g. EAST1) in the Available Cisco CallManagers box and using the arrow between the two boxes, move it to the Selected Cisco CallManagers box.

Step 26 Highlight the server **XXXXNB** (where XXXX is the cluster indentification and N is the cluster number, e.g. EAST1) in the Available Cisco CallManagers box and using the arrow between the two boxes, move it to the Selected Cisco CallManagers box.

Step 27 Use the up and down arrows to ensure that the "B" CallManager is at the top of the list, making it the primary CallManager for the group. Select the **Auto-registration Cisco CallManager Group** check box for this CallManager Group.

Step 28 Select **Insert**.

Note The CallManager Groups are named to indicate their primary CallManager.

Configure Device Pools

Step 29 Go to **System > Device Pool** to open the Device Pool Configuration page in the CCM Administrator.

In this section, you are going to create Device Pools that are named to reflect their CallManager Group, Date/Time Group, and Region. A Device Pool is named "AB_Default_CMLocal_DP" if it uses the "AB_CMG" CallManager Group, the Default Region, and the "CMLocal" Date/Time Group.

Step 30 Use the menus to select the characteristics from the table above. For example, the Device Pool Name should be AB_Default_CMLocal_DP, and it should have the following characteristics:

- Cisco CallManager Group: AB_CMG
- Date/Time Group: CMLocal (because it is in the Campus Region)
- Region: Default
- Soft key Template: Standard User

Step 31 Select **Insert**.

Note	The Device Pool name, **AB_Default_CMLocal_DP** is self-documenting.

Step 32 Use the menus to select the characteristics from the table above. For example, the Device Pool Name should be BA_Default_CMLocal_DP, and it should have the following characteristics:

- CiscoCallManager Group: BA_CMG
- Date/Time Group: CMLocal (because it is in the Campus Region)
- Region: Default
- Soft key Template: Standard User

Step 33 Select **Insert**.

Step 34 Note that the Device Pool name, **BA_Default_CMLocal_DP** is self-documenting.

Exercise Verification

You have completed this exercise when you attain these results:

- In Cisco CallManager Administration, go to **System > Device Pool**. Select each device pool from the left column, and ensure the names reflect the device pool settings.

Task 3: Setting the Default Pool for Devices

In this task, you will configure a default Device Pool for specific devices. If you do not change this default parameter all devices will use the "Default" device pool. The Default device pool is configured to use the Default Cisco CallManager Group (Cisco CallManager "A" only), the CMLocal Date/Time Group and the Default Region (G711 codec).

Exercise Procedure

Complete these steps:

Step 1 Go to **System > Device Defaults**.

Step 2 Scroll down the screen to IP Phone 7960.

Step 3 Select the **Device Pool** column menu, and choose the **BA_Default_CMLocal_DP Device Pool**.

Step 4 Repeat Steps 2 and 3 for the following devices:

H.323 Phone

IP Phone 7960

IP Phone 7940

IP Phone 7910

Conference Bridge WS-X6608

Digital Access WS-X6608

Media Termination Point WS-X6608

Analog Access WS-X6624

Conference Bridge

Media Termination Point

Step 5 When you have changed the specified device defaults scroll to the top of the screen and select **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- The Cisco IP Phones have auto-registered to the correct CallManager and are configured with the correct Device Pool.
- Verification of this exercise will be part of the last task of this section.

Task 4: Plug Cisco IP Phone into Network

Plug the Cisco IP Phones to the network and the phones will auto-register, getting the DN from the Cisco CallManager configuration page and register to the Cisco CallManager group of the device pool on the Default Devices Configuration page.

Exercise Procedure

Complete these steps:

Step 1 Determine the correct switch ports for your Lab Pod. Insert the appropriate cable into one of those ports and the other end into the IP Phone.

Exercise Verification

You have completed this exercise when you attain these results:

- The Cisco IP Phones have directory numbers and you are able to call from one phone to another within the cluster.

Step 1 Observe the IP Phone cycle through functions to register the phone.

Step 2 When the phone has successfully registered the appropriate date and time will appear and the phone will display its directory number.

Step 3 Call another registered phone in your cluster and verify that you can talk over the connection.

Step 4 On a registered phone, select the “Settings” key, and enter “3”. This will take you to the CallManager parameter settings in the phone. The IP address of the primary CallManager will be displayed first with the word “Active” to the right and the IP address of the backup CallManager will be displayed next with the word “Standby” to its right.

Step 5 Go to **Device** > **Phone** and select **Find Phone** without changing any parameters. The phone’s Device Pool and name of the CallManager to which it is registered will be displayed.

Laboratory Exercise: Configure Auxiliary or Voice VLANs

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco IP Phones
- Cisco Catalyst Switch (6000, 4000, 3500, 2900)

Exercise Objective

In this exercise, you will be able to configure auxiliary or voice VLANs to distinguish between voice and data traffic.

After completing this exercise, you will be able to:

- Configure auxiliary or voice VLANs on the provided Catalyst switch

Command List

The commands used in this exercise are described in the table here.

Table: Catalyst 3500 Commands

Command	Description
`enable`	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
`interface fastethernet`	Begins interface configuration for the Catalyst 3500 series.
`switchport trunk encapsulation dot1q`	Configure the port to support 802.1Q encapsulation. You must configure each end of the link with the same encapsulation type.
`switchport trunk native vlan <number>`	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. Valid IDs are from 1 to 1001.
`switchport mode trunk`	Configure the port as a VLAN trunk.
`switchport voice vlan <number>`	Configure the voice VLAN that is sending and receiving tagged traffic on the trunk port.
`spanning-tree portfast`	Spanning-tree PortFast causes a port to enter the spanning-tree forwarding state immediately, bypassing the listening and learning states.

Table: Catalyst 4000 and 6000 Commands

Command	Description
`enable`	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
`set vlan <number> name <name>`	Begins interface configuration for the Catalyst 3500 series.
`set vlan <number> [module/port]`	Configure the port to support ISL or 802.1Q encapsulation. You must configure each end of the link with the same encapsulation type.
`set port auxiliaryvlan [module/port] <number>`	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. Valid IDs are from 1 to 1001.

Job Aids

These job aids are available to help you complete the laboratory exercise:

Table: VLAN Information

Cluster Name	Voice VLAN	Data VLAN
East 1	10	15
East 2	20	25
East 3	30	35
East 4	40	45
West 1	10	15
West 2	20	25
West 3	30	35
West 4	40	45

Exercise Procedure

Complete these steps:

Step 1 Write down the IP address of the switch you will be working on.

Step 2 Document the type of switch you are working on (Catalyst 2900XL, 3500XL, 4000, 6000).

Step 3 Configure voice and data VLANs on switchports. Below are configuration commands for a Catalyst 3500XL, 4000 and 6000. Go to the section for the type of switch you are configuring, and enter the configuration commands using your cluster number for "x".

Catalyst 35XX

From configuration mode, enter the following commands to configure voice and data VLANs on a Catalyst 3500XL using your cluster number of "x":

```
interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport trunk native vlan x5

switchport mode trunk

switchport voice vlan x0

spanning-tree portfast
```

Catalyst 4000

From configuration mode, enter the following commands to configure voice and data VLANs on a Catalyst 4000 using your cluster number of "x" and your cluster code for "XXX". For `[module/port]`, you can configure a single port or a range or ports. For example, to configure a range of ports on a module, enter "`5/1-48`".

```
set vlan x5 name XXX-data
```

```
set vlan x0 name XXX-IP-phones

set vlan x5 [module/port]

set port auxiliaryvlan [module/port] x0
```

Catalyst 6000

From configuration mode, enter the following commands to configure voice and data VLANs on a Catalyst 6000 using your cluster number of "x" and your cluster code for "XXX". For `[module/port]`, you can configure a single port or a range or ports. For example, to configure a range of ports on a module, enter "`5/1-48`".

```
set vlan x5 name XXX-data

set vlan x0 name XXX-IP-phones

set vlan x5 [module/port]

set port auxiliaryvlan [module/port] x0
```

When configuring Catalyst 4000 and/or 6000 switches the following commands are associated with configuring data VLANs:

- **set vlan x5 name XXX-data**
- **set vlan x5 (module/port)**

The following commands are associated with configuring voice VLANs:

- **set vlan x0 name XXX-IP-phones**
- **set port auxiliaryvlan [mod/port] x0**

When using the commands above for both voice and data VLAN assignments, the first command listed creates the VLAN and the second command listed assigns that VLAN to specific ports.

Exercise Verification

You have completed this exercise when you attain these results:

- The Cisco IP Phone will obtain an IP address within the subnet configured in the DHCP scope that is consistent with the auxiliary or voice VLAN configured on the switch.

Laboratory Exercise: Configure Cisco Access Gateways

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco Catalyst 6000 with a T-1 or E-1 module (WS-X6608-T/E-1)
- Remote Cisco CallManager (CCM) cluster
- IOS-MGCP gateway (VG200, 2600, 3600)
- H323 gateway (2600, 3600)
- Gatekeeper device (2600 or 3600)

Exercise Objective

In this exercise, you will configure CIPT gateways in CCM administration.

After completing this exercise, you will be able to:

- Configure intercluster trunks
- Configure a non-IOS-MGCP (T/E-1 ports) gateway
- Configure an IOS-MGCP gateway (VG200, 2600, 3600)
- Configure an H323 gateway (2600, 3600)

Command List

The commands used in this exercise are described in the table here.

Table: Catalyst 6000 Commands

Command	Description
enable	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
show port [module/port]	Displays the attributes of the module or the port on the module.

Table: IOS MGCP Gateway Commands

Command	Description
enable	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
configure terminal	Enters global configuration mode.
mgcp	Enables the mgcp application on the gateway.
mgcp call-agent [primary ccm ip address]	Identifies the primary CCM for the gateway.
mgcp dtmf-relay codec all mode out-of-band	Configures the gateway to use simple desktop messaging protocol.
mgcp sdp simple	Configures the gateway to use simple desktop messaging protocol.
ccm-manager switchback [immediate|graceful|time]	Configures the switchback settings for the gateway.
ccm-manager redundant-host [backup ccm ip address]	Identifies the secondary and/or tertiary CCM for the gateway.
ccm-manager mgcp	Identifies that the CCM is using the mgcp application.
dial-peer voice [tag] pots	Configures a plain old Telephony service dial-peer on the gateway.
application MGCPAPP	Configures the dial-peer to use the mgcp application.
port [x/x/x]	Specifies the voice port used with the configured dial peer.

Table: H.323 Gateway Commands

Command	Description
enable	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
configure terminal	Enters global configuration mode.
voice class h323 <tag>	Creates an H323 voice class that is used to configure a TCP timeout duration.
H225 timeout tcp establish [seconds]	Configures the H225 TCP timeout duration in seconds.
dial-peer voice [tag] pots	Configures a plain old Telephony service dial-peer on the gateway.

Job Aids

These job aids are available to help you complete the laboratory exercises:

Table: Intercluster Trunk Gateway Information

Cluster Name	Cluster Number	Device Name	Description
East 1	1	172.16.30.6	East 3 Primary
		172.16.30.5	East 3 Publisher
East 2	2	172.16.40.6	East 4 Primary
		172.16.40.5	East 4 Publisher
East 3	3	172.16.10.6	East 1 Primary
		172.16.10.5	East 1 Publisher
East 4	4	172.16.20.6	East 2 Primary
		172.16.20.5	East 2 Publisher
West 1	1	172.32.30.6	West 3 Primary
		172.32.30.5	West 3 Publisher
West 2	2	172.32.40.6	West 4 Primary
		172.32.40.5	West 4 Publisher
West 3	3	172.32.10.6	West 1 Primary
		172.32.10.5	West 1 Publisher
West 4	4	172.32.20.6	West 2 Primary
		172.32.20.5	West 2 Publisher

Table: MGCP Gateway Information

MGCP Gateway CLI Configuration		
Cluster Name	**Call-agent**	**Redundant-host**
East 1	172.16.10.6	172.16.10.5
East 2	172.16.20.6	172.16.20.5
East 3	172.16.30.6	172.16.30.5
East 4	172.16.40.6	172.16.40.5
West 1	172.32.10.6	172.32.10.5
West 2	172.32.20.6	172.32.20.5
West 3	172.32.30.6	172.32.30.5
West 4	172.32.40.6	172.32.40.5

Cisco CallManager Administration Configuration	
Parameter	**Data**
Network Module	NM-2V
Sub-Unit 0	FXS
Sub-Unit 1	FXO
FXS Endpoint Identifier	1/0/1
FXO Endpoint Identifier	1/1/0
Num Digits	4
Expected Digits	4
Directory Number DN	<Cluster Number>051
Display	<Cluster name> Conf Room 51
Port Direction	Bothways

Table: H.323 Gateway Information

H.323 Gateway CLI Configuration				
Cluster Name	**Session Targets**		**Pots Destination-pattern**	
	Preference 0	**Preference 1**	**Number 1**	**Number 2**
East 1	172.16.10.6	172.16.10.5	4…	2…
East 2	172.16.20.6	172.16.20.5	3…	1…
East 3	172.16.30.6	172.16.30.5	2…	4…
East 4	172.16.40.6	172.16.40.5	1…	3…
West 1	172.32.10.6	172.32.10.5	4…	2…
West 2	172.32.20.6	172.32.20.5	3…	1…
West 3	172.32.30.6	172.32.30.5	2…	4…
West 4	172.32.40.6	172.32.40.5	1…	3…

Cisco CallManager Administration Configuration	
Parameter	**Data**
Device Name	<IP Address>
Description	<Type of H.323 gateway>
Device Pool	BA_DP
Calling Party Selection	Originator
Presentation Bit	Allowed

Task 1: Configure Intercluster Trunks

Using the IP address of the CCM in the remote cluster, you will add intercluster trunk gateways in CCM Administration utility.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Device > Trunk**.

Step 2 Select **Add a New Trunk** from the Find and List Trunks page.

Step 3 Select **Inter-Cluster Trunk** (Non-Gatekeeper Controlled), and select **Inter-Cluster Trunk** from the device protocol menu. Select **Next**.

Step 4 Enter the device name and description of the gateway from the Intercluster Trunk Gateway Information table.

Step 5 Select **BA_DP** for the device pool.

Step 6 Select **Originator** for the Calling Party Selection, and select **Allowed** for the Presentation Bit.

Step 7 Enter the Publishers IP address for the Server1 IP Address/Host Name.

Step 8 Click **Insert**, and then click **OK** at the dialog box that appears stating the gateway needs to be reset for changes to take affect.

Step 9 Select **Reset Trunk**, and click **Reset** from the dialog box. Select **OK**.

Step 10 Repeat Steps 1 through 8 to add the other gateway.

Exercise Verification

You have completed this exercise when you attain these results:

- The intercluster trunk gateways will appear in the gateway list in CCM Administration utility.

Task 2: Configure a Non-IOS MGCP Gateway

In this task, you will be configuring the Cisco Catalyst T/E-1 port in the CCM Administration utility.

Exercise Procedure

Complete these steps:

Step 1 Go to **Start > Run**, and enter "telnet <ip address>" to telnet into the Catalyst 6000.

Step 2 Enter the password "cisco", and then enter "enable" and the password "cisco" to enter global configuration mode.

Step 3 Enter "show port [mod/port]" to get the MAC address of the T/E-1 port you are going to configure in Cisco CallManager.

Step 4 Write the MAC address below:

_____

Step 5 In CCM Administration, go to **Device > Add a New Device** to select a device type to configure.

Step 6 Use the menu to choose **gateway**, and select **Next**.

Step 7 Choose the **Cisco Catalyst 6000 T1 or E1 VoIP Gateway**, and choose **Digit Access PRI** for the device protocol. Click **Next**.

Step 8 For the MAC address, enter the MAC address from Step 4.

Step 9 Enter the IP address, module, and port number for the description so it looks like the following:

172.16.1.5 5/3

Step 10 Select **BA_DP** for the device pool.

Step 11 Select **United States** for the Network Local.

Step 12 If you are working in an even numbered group, choose **User** for the Protocol Side. If you are working in an odd numbered group, choose **Network** for the Protocol Side.

Step 13 If you are working in an even numbered group, choose **Network** for the Clock Reference. If you are working in an odd numbered group, choose **Internal** for the Clock Reference.

Step 14 Click **Insert**, and click **OK**.

Step 15 Select **Reset Gateway**, and click **Reset** from the dialog box. Select **OK**.

Step 16 Using a T-1 cross over cable, connect your port to your partner's port. (Group 1 connects to group 2 and group 3 connects to group 4).

Exercise Verification

You have completed this exercise when you attain these results:

- The non-IOS MGCP gateway will appear in CCM Administration utility and from the CLI, the type of that port will show T1 or E1.

Task 3: Configure an IOS MGCP Gateway

In this task, you will be configuring the dial-peer statements and configuration information in CCM Administration utility of an IOS-MGCP gateway (VG200, 2600, 3600).

Exercise Procedure

Complete these steps:

Step 1 Gather gateway information. Write down the MGCP gateway IP address and port information below:

IP Address	Type (2600 or VG200)	FXS Port: 1/0/1 FXO Port: 1/1/0

Step 2 Telnet into the MGCP Gateway and use "cisco" as the password to get in. Enter "enable" and password "cisco" to enter enable mode.

Step 3 Use the command **configuration terminal** or **config t** to enter configuration mode.

Step 4 To configure the Primary CCM in the MGCP gateway, enter the following in the configuration mode using your cluster number when you see "x":

```
mgcp

mgcp call-agent <Call-agent>

mgcp dtmf-relay voip codec all mode out-of-band

mgcp sdp simple
```

Step 5 Configure CCM redundancy in the MGCP gateway. Enter the following in configuration mode:

```
ccm-manager switchback graceful

ccm-manager redundant-host <Redundant-host>

ccm-manager mgcp
```

Step 6 Configure the dial-peer and the physical port so that the port uses the MGCP application using the following commands in configuration mode: (Note—A tag number is an unique number that separates dial peers on the same router. Use your cluster number when you see "**x**")

```
dial-peer voice x05 pots

 application MGCPAPP

 port 1/0/1

dial-peer voice x15 pots

 application MGCPAPP

 port 1/1/0
```


You should have configured an FXS (1/0/1) and an FXO (1/1/0) port.

Step 7 Write down the hostname of the MGCP gateway below:

Hostname: _____

Step 8 In Cisco CallManager Administration, go to **Device > Add a New Device** to select a device type.

Step 9 Use the menu to choose **gateway**, and click **Next**.

Step 10 Select **product type** (26xx or VG200) as the type of gateway, and click **Next**.

Step 11 Enter the hostname (from Step 7) of the device for the domain name. For the description, enter the physical location of the gateway device.

Step 12 From the Module in Slot 1 menu, choose **NM-2V** for the type of network module (network module with two VIC slots).

Step 13 Select **Insert**.

Step 14 From the Sub-Unit (0 and 1) menu, choose the type of voice interface card (VIC) from table x-x. Select **Update**.

Step 15 Select the FXS endpoint identifier **1/0/1**. Configure the gateway information by selecting **BA_DP** for the device pool

Step 16 Enter "4" for the Num Digits, and enter "4" for the Expected Digits.

Step 17 Select **Insert**, and click **OK**.

Step 18 Select **Add DN**, which is in the left hand column next to the endpoint identifier you just configured. Enter "<cluster number>051" for the directory number.

Step 19 Leave the directory number settings as is. Enter "<Cluster name> Conf Room 51" for Display. This information is seen on the called phone internally within a CIPT network.

Step 20 Plug an analog phone into FXS port **1/0/1**.

Step 21 Configure the FXO port endpoint identifier by selecting **1/1/0** from the left column.

Step 22 Select **Ground Start** for the Port Type.

Step 23 Configure Gateway information by selecting **BA_DP** for the Device Pool. For Port information, leave the Port Direction as **Bothways**.

Step 24 Enter "#000" (where # is your cluster number) for the Attendant DN.

Step 25 Select **Insert**, and click **OK**.

Step 26 Reset the gateway for changes to take affect and you will want to wait for the gateway to get back online before making a call.

Step 27 Select **Back to Find/List Gateways** to view the gateways added in CCM administration. If the gateways are not listed, select **Find** to list all the gateways.

Note In global configuration mode of the IOS MGCP device, you can shutdown/no shutdown the voice ports to quickly get the MGCP endpoints registered and operating.

Exercise Verification

You have completed this exercise when you attain these results:

- The MGCP endpoints will be configured and you will be able to call the analog phone connected to the FXS port. You will also be able to call phone the analog phone connected to the FXS port to a valid DN within your cluster.

Task 4: Configure an H323 Gateway

In this task, you will be configuring the dial-peer statements and configuration information in CCM Administration utility of an H323 gateway (2600, 3600).

Exercise Procedure

Complete these steps:

Step 1 Gather gateway information. Write down the H.323 gateway IP address and port information below:

IP Address: Port: 1/0/0

Step 2 Telnet into the H323 Gateway and use "cisco" as the password to get in. Enter "enable" and password "cisco" to enter enable mode.

Step 3 Use the command **configuration terminal** or **config t** to enter configuration mode.

Step 4 Configure the H225 TCP timeout interval using the following commands using your data VLAN number for the <tag>.

```
Voice class h323 x5

   H225 timeout tcp establish 5 (five seconds)
```

Step 5 Enter the following commands to configure the FXS port information:

```
Dial-peer voice x0 pots

   Destination-pattern [number 1]

   Preference 1

   Port 1/0/0

Dial-peer voice x1 pots

   Destination-pattern [number 2]

   Preference 1

   Port 1/0/0
```

Step 6 Do a shut/no shut on the voice ports just configured.

Step 7 Configure the dial-peer that allows the analog phone to call Cisco IP Phones registered in the cluster. You will also be configuring redundancy on the gateway so that if one CCM is not available the other can be used. Your cluster number will be used for "x" when configuring the following commands in configuration mode:

```
Dial-peer voice x00 voip

   Destination-pattern x . . .
```

```
    Session target ipv4: [ip address]

    Preference 0

    Voice-class h323 x5

Dial-peer voice x000 voip

    Destination-pattern x . . .

    Session target ipv4: [ip address]

    Preference 1

    voice class h323 x5
```

Step 8 Write down the IP address of the H.323 gateway below:

IP Address: _____

Step 9 In CCM Administration go to **Device > Add a New Device** to open Add a New Device page.

Step 10 Use the menu to choose **gateway**, and select **Next**.

Step 11 Select **H.323** for a gateway, and select **H.225** for the device protocol. Select **Next**.

Step 12 Enter the IP address for the device name, and enter the information from table x-x for the description and device pool. Enter "Originator" for the Calling Party Selection, and enter "Allowed" for the Presentation Bit.

Step 13 Select **Insert**, and click **OK**.

Exercise Verification

You have completed this exercise when you attain these results:

- With an analog phone connected to the FXS port of the H323 gateway, you will be able to dial a DN of a Cisco IP Phone within the cluster. (To call the analog phone connected to the FXS port of the H323 gateway, you will need to configure a route pattern.)

Laboratory Exercise: Building Basic Route Plans

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco IP Telephony servers (two)
- Remote Cisco CallManager (CCM) clusters
- Gateway devices (intercluster trunks, non-IOS MGCP, MGCP [FXS, FXO], H.323 [FXS, FXO]).
- Gatekeeper device (2600, 3600)

Exercise Objective

In this exercise, you will build simple route plans that access the gateway devices that were added in a previous laboratory exercise.

After completing this exercise, you will be able to:

- Configure a route pattern to the H.323 gateway to ring the analog phone connected to the FXS port
- Create a route pattern directed to a non-IOS MGCP gateway that allows calls to another cluster
- Configure the intercluster trunk gateways in route groups, place the route group into a route list and then create a route pattern directed to the route list that allows calls to another cluster
- Configure the MGCP (FXO) and H.323 (FXS) gateways into a route group, place the route group into a route list and then create a route pattern to the route list that allows calls to another cluster

Command List

The commands used in this exercise are described in the table here.

Table: Catalyst 6000 Commands

Command	Description
enable	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
show port [module/port]	Displays the attributes of the module or the port on the module.

Job Aids

These job aids are available to help you complete the laboratory exercise(s):

Table: Route Groups and Route Lists

Cluster Name	ICT_RG Name	ICT_RG Gateway Order	H.323_MGCP_RG Name	H.323_ MGCP_RG Gateway Order
East 1	E3_ICT_RG	172.16.30.6	E4_H323_MGCP_RG	H323-FXS
		172.16.30.5		MGCP-FXO
East 2	E4_ICT_RG	172.16.40.6	E3_H323_MGCP_RG	H323-FXS
		172.16.40.5		MGCP-FXO
East 3	E1_ICT_RG	172.16.10.6	E2_H323_MGCP_RG	H323-FXS
		172.16.10.5		MGCP-FXO
East 4	E2_ICT_RG	172.16.20.6	E1_H323_MGCP_RG	H323-FXS
		172.16.20.5		MGCP-FXO
West 1	W3_ICT_RG	172.32.30.6	W4_H323_MGCP_RG	H323-FXS
		172.32.30.5		MGCP-FXO
West 2	W4_ICT_RG	172.32.40.6	W3_H323_MGCP_RG	H323-FXS
		172.32.40.5		MGCP-FXO
West 3	W1_ICT_RG	172.32.10.6	W2_H323_MGCP_RG	H323-FXS
		172.32.10.5		MGCP-FXO
West 4	W2_ICT_RG	172.32.20.6	W1_H323_MGCP_RG	H323-FXS
		172.32.20.5		MGCP-FXO

Table: Route Patterns for Gateways

Cluster Name	H.323 Gateway	Non-IOS MGCP Gateway	ICT_RL	MGCP_H.323 _RL
East 1	4000	2XXX	3XXX	4XXX
East 2	3000	1XXX	4XXX	3XXX
East 3	2000	4XXX	1XXX	2XXX
East 4	1000	3XXX	2XXX	1XXX
West 1	4000	2XXX	3XXX	4XXX
West 2	3000	1XXX	4XXX	3XXX
West 3	2000	4XXX	1XXX	2XXX
West 4	1000	3XXX	2XXX	1XXX

Task 1: Configure a Route Pattern to the H.323 Gateway

This is the simplest route plan to build. You are going to create a route pattern to the H.323 gateway that is already added in the CCM database.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Route Pattern**, and then select **Add a New Route Pattern** to open the Route Pattern Configuration page.

Step 2 Enter the route pattern in the Route Patterns for Gateways table (from the Job Aids section of this lab) for the H.323 gateway.

Step 3 Choose the **H.323 gateway (IP address)** from the Gateway/Route List menu.

Step 4 Deselect the **Provide outside dial tone** check box.

Step 5 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- Dial the route pattern to ring the analog phone plugged into the H.323's FXS port.

Task 2: Configure a Route Pattern to the Non-IOS MGCP Gateway

This is another simple route plan to build. You are going to create a route pattern to the digital gateway (non-IOS MGCP) that is already added in the CCM database.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Route Pattern**, and select **Add a New Route Pattern** to open the Route Pattern Configuration page.

Step 2 Enter the route pattern in the Route Patterns for Gateways table (from the Job Aids section of this lab) for the Non-IOS MGCP gateway.

Step 3 Choose the **non-IOS MGCP gateway** from the Gateway/Route List menu.

Step 4 Deselect the **Provide outside dial tone** check box.

Step 5 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- Check if the other group is ready and get a valid directory number for that group. Dial the route pattern that includes the DN to successfully call another cluster.

Task 3: Configure Route Plan of Route Group, Route List, and Route Pattern Using the Intercluster Trunks

Add the intercluster trunks gateways devices to a route group, then add that route group to a route list, and finally build a route pattern directed at the route list to allow calls to another cluster via the intercluster trunks.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Route Group**, and select **Add a New Route Group** to open the Route Group Configuration page.

Step 2 Using the information in the Route Groups and Route Lists table (from the Job Aids section of this lab), enter "ICT_RG" for the route group name, and click **Continue**.

Step 3 Select the first gateway in the Route Groups and Route Lists table (from the Job Aids section of this lab) to add to this route group.

Step 4 Select **Insert**.

Step 5 Select **Add Device** to add the second gateway from the Route Groups and Route Lists table (from the Job Aids section of this lab), and select **2** for the Order.

Step 6 Select **Insert**.

Configure Route List

Step 7 In CCM Administration, go to **Route Plan > Route List**, and select **Add a New Route List** to open the Route List Configuration page.

Step 8 Enter "ICT_RL" for the route list name, and enter "Intercluster to <Cluster Name>" for the description.

Step 9 Select **Insert**.

Step 10 Select **Add Route Group** to add a route group to the route list.

Step 11 Choose a route group **XX_ICT_RG**, and click **Add**.

Step 12 Leave the Route Details Configuration page alone. This page is used for transformation information.

Step 13 Select **Insert**.

Route Pattern

Step 14 In CCM Administration, go to **Route Plan > Route Pattern**, and select **Add a New Route Pattern** to open the Route Pattern Configuration page.

Step 15 Enter the ICT_RL route pattern from the Route Patterns for Gateways table (from the Job Aids section of this lab) for the route pattern.

Step 16 Choose **ICT_RL** from the Gateway/Route List menu.

Step 17 Deselect the **Provide outside dial tone** check box.

Step 18 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- Get a valid directory number for that group. Dial the route pattern that includes the DN to successfully call another cluster.

Laboratory Exercise: Configuring Complex Route Plans

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Two Cisco IP Telephony servers
- Remote Cisco CallManager (CCM) clusters
- Gateway devices (intercluster trunks, non-IOS MGCP, MGCP [FXS, FXO], H.323 [FXS, FXO])
- Gatekeeper device (2600, 3600)

Exercise Objective

In this exercise, you will be able to apply complex route plan concepts to the simple route plans.

After completing this exercise, you will be able to:

- Configure translation patterns to handle all directory numbers within the clusters DID range
- Configure the External Phone Number Mask on the Cisco IP Phones and apply the calling party transformation settings in the route pattern or in the route details of the route list configuration page
- Modify route patterns by adding an access code (use the "." Wildcard) and the discard digits instructions
- Configure a route pattern that has a route filter to block "900" numbers

Job Aids

These job aids are available to help you complete the laboratory exercises:

Table: Transformation Masks

Cluster Name	External Phone Number Mask
East 1	555341XXXX
East 2	555412XXXX
East 3	555123XXXX
East 4	555234XXXX
West 1	777341XXXX
West 2	777412XXXX
West 3	777123XXXX
West 4	777234XXXX

Table: Destination Patterns for H.323 FXO Ports

Cluster Name	Number 1	Number 2
East 1	4…	2…
East 2	3…	1…
East 3	2…	4…
East 4	1…	3…
West 1	4…	2…
West 2	3…	1…
West 3	2…	4…
West 4	1…	3…

Table: Route Filter Called Party Transformation Settings

Cluster Name	Number 1	Number 2
East 1	3XXX	2XXX
East 2	4XXX	1XXX
East 3	2XXX	4XXX
East 4	2XXX	3XXX
West 1	3XXX	2XXX
West 2	4XXX	1XXX
West 3	1XXX	4XXX
West 4	2XXX	3XXX

Task 1: Configure a Translation Pattern

To ensure that the company does not miss-dialed calls, configure a translation pattern to handle all calls with the given DID range.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Translation Pattern**, and select **Add a New Translation Pattern** to open the Translation Pattern Configuration page.

Step 2 Enter "<Your Own Cluster Number>XXX" for the translation pattern.

Step 3 Deselect the **Provide Outside Dial Tone** check box.

Step 4 Enter "<Your Own Cluster Number>000" for the Called Party Transform Mask.

Step 5 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- From a phone other than DN #000, call an unassigned DN in your cluster; it should ring the directory number configured in Step 4.

- Check with another cluster to see if they have configured their translation pattern, and then call an unassigned DN in another cluster and it should ring the directory number the other cluster has configure in Step 4.

Task 2: Configuring Transformation Masks

Configure the External Phone Number Masks on the Cisco IP Phones and apply calling transformation settings on the Route Pattern Configuration page or in the route details of the route list.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Device** > **Phone** and click **Find** to list the phones in the cluster.

Step 2 Select a phone from the list to get to the phone's Phone Configuration page.

Step 3 From the Phone Configuration page for the selected phone, select **Line 1** to open the Directory Number Configuration page.

Step 4 Scroll down to the Line Settings for this Device section, and enter the External Phone Number Mask from the Transformation Masks table (from the Job Aids section of this lab).

Step 5 Click **Update**.

Step 6 Select **Configure Device (SEP<MAC Address>)** to return to the Phone Configuration page.

Step 7 Click **Reset Phone**, click **Reset**, and then click **OK** to reset the phone.

Step 8 Repeat Steps 1 though 7 for the other phones in your cluster.

Step 9 Apply the **External Phone Number Mask** to the **FXS** endpoint (**1/0/1**) of the **MGCP** gateway.

Step 10 In CCM Administration, go to **Device** > **Gateway** and click **Find** to list the gateways in the cluster.

Step 11 Select the **MGCP gateway**.

Step 12 Select the FXS endpoint **1/0/1**.

Step 13 Select the **DN (#051)** from the left column.

Step 14 Scroll down to the Line Settings for this Device section, and enter the External Phone Number Mask from the Transformation Masks table (from the Job Aids section of this lab).

Step 15 Click **Update**.

Step 16 Click **Reset Devices**, click **OK**, and the click **OK** again.

Step 17 In CCM Administration, go to **Route Plan** > **Route Pattern** and find the route pattern to the Non-IOS MGCP gateway (T/E-1 port).

Step 18 At the Route Pattern Configuration page to the Non-IOS MGCP gateway in the Calling Party Transformations section, select the **Use Calling Party's External Phone Number Mask** check box.

Step 19 Click **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- Dial the route pattern from a Cisco IP phone to the non-IOS MGCP gateway and the receiving phone will see the External Phone Number Mask applied to the calling phone's DN.

- Dial the route pattern from the analog phone plugged into the MGCP FXS port and the receiving phone will see the External Phone Number Mask applied to the calling phone's DN.

Task 3: Modify Route Patterns to use Access Codes and Discard Digit Instructions

Using the route patterns already in the CCM database, modify those route patterns to use an "outside line" access code. Apply the discard digit instruction to send the correct expected digits to the next call processing agent.

Exercise Procedure

Complete these steps:

Delete Route Patterns and Route Lists

Step 1 In CCM Administration, go to **Route Plan** > **Route Pattern** and click **Find** to list the route patterns configured in the cluster.

Step 2 Select the check boxes of the route patterns to the Non-IOS MGCP gateway and to the MGCP_H323_RL.

Step 3 Click **Delete Selected**, and click **OK** to delete the route patterns.

Step 4 In CCM Administration, go to **Route Plan** > **Route List** and click **Find** to list the route lists configured in the cluster.

Step 5 Select the **H323_MGCP_RL** check box.

Step 6 Click **Delete Selected**, and click **OK** to delete the route list.

Modify Route Group

Step 7 In CCM Administration, go to **Route Plan** > **Route Group** and select **Add a New Route Group** to get to the Route Group Configuration page.

Step 8 Enter "Digital Gateway" for the Route Group Name, and click **Continue**.

Step 9 Select the **non-IOS MGCP** gateway (S0/DS1-0@SDA<MAC_Address>) for the device name, and click **Insert**.

Step 10 In CCM Administration, go to **Route Plan** > **Route List** and select **Add a New Route List** to get to the Route List Configuration page.

Step 11 Enter "PSTN_RL" for the Route List Name, enter "Digital H323 MGCP gws" for the Description, and click **Insert**.

Step 12 Select **Add Route Group** to add a route group to the route list.

Step 13 Select a route group **Digital Gateway**, and click **Add**.

Step 14 Leave the Route Details Configuration page alone. This page is used for transformation information.

Step 15 Select **Insert**.

Step 16 Select **Add Route Group to the current Route List** from the top right of the page.

Step 17 Select a route group **XX_H323_MGCP_RG**, and click **Add**.

Step 18 Leave the Route Details Configuration page alone. This page is used for transformation information.

Step 19 Select **Insert**.

Configure Dial Peers on H.323 and MGCP Gateway

Step 20 Telnet into the H.323 Gateway and use "**cisco**" as the password to get in. Enter "enable" and password "cisco" to enter enable mode.

Step 21 Use the command **configuration terminal** or **config t** to enter configuration mode.

Step 22 Enter the following commands to configure the FX0 port information:

```
Dial-peer voice x1 pots

   Destination-pattern [number 1]

   No digit strip

   Port 1/1/1

Dial-peer voice x1 pots

   Destination-pattern [number 2]

   No digit strip

   Port 1/1/1
```

Step 23 Disconnect the analog phone plugged into the MGCP gateway's FXS port. Connect an RJ-11 cable from the H.323 gateway's FX0 port (1/1/1) to the other groups MGCP gateway's FXS port (1/0/1).

Route Pattern Configuration

Step 24 In CCM Administration, go to **Route Plan > Route Pattern**, and select **Add a New Route Pattern** to open Route Pattern Configuration page.

Step 25 Enter "9.XXXX#" for the route pattern.

Step 26 Choose **PSTN_RL** from the Gateway/Route List menu.

Step 27 Deselect the **Provide outside dial tone** check box.

Step 28 In the Calling Party Transformations section, select the **Use Calling Party's External Phone Number Mask** check box.

Step 29 In the Called Party Transformation section, select **PreDot Trailing-#** for the Discard Digits parameter.

Step 30 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- You are able to call a DN in the cluster that is connected via the digital gateway.
- You are able to call a DN in the cluster that is connected to via the H.323 and MGCP gateway. The call route is through the digital gateway and then through the intercluster trunks configured between the other cluster.

- You are able to unplug the T-1 crossover cable and call a DN in the cluster connected via the H.323 and MGCP gateway and the cluster not connected via T-1. The call is routed through the H.323 FXO port to the MGCP FXS port passed to the remote CCM, then through intercluster trunk.

- Shut down the FXO voice ports. Calls will now be routed to the H.323 FXS port to the MGCP FXO port and because the MGCP FXO port is assigned an Attendant DN, all calls will be routed to the Attendant DN.

Note	To shut down a voice port, enter configuration mode (configuration terminal), enter voice-port [x/x/x] (FXO port <1/1/1>), and enter shutdown.

Reconnect all cables (T-1) and enable all voice ports (no shutdown) in preparation for the next laboratory exercise.

Task 4: Configure Route Filters to Apply to Route Patterns

To ensure that employees are productive, block phone numbers using a route filter applied to a route pattern.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Route Filter**, and select **Add a New Route Filter** to get to the Route Filter Configuration page.

Step 2 Enter "Block 900 Calls" for the Route Filter Name, and click **Continue**.

Step 3 Select == and enter "900" for AREA-CODE, and click **Insert**.

Step 4 In CCM Administration, go to **Route Plan > Route Pattern**, and select **Add a New Route Pattern** to open the Route Pattern Configuration page.

Step 5 Enter "9.@" for the route pattern.

Step 6 Select **Block 900 Calls** for the Route Filter, and select the **ICT_RL** for the Gateway/Route List.

Step 7 Deselect the **Provide outside dial tone** check box.

Step 8 In the Called Party Transformation section, select **PreAt** for the Discard Digits parameter, and enter "<9.@ with Filter>" for the Called Party Transform Mask.

Step 9 Click **Insert**.

Step 10 Select **Add a New Route Pattern** to get to the Route Pattern Configuration page.

Step 11 Enter "9.@" for the route pattern.

Step 12 Select the **ICT_RL** for the Gateway/Route List.

Step 13 Deselect the **Provide outside dial tone** check box.

Step 14 In the Called Party Transformation section, select **PreAt** for the Discard Digits parameter and enter "<9.@ without Filter>" for the Called Party Transform Mask.

Exercise Verification

You have completed this exercise when you attain these results:

- Dial a phone number with a "900" area code from a phone within your cluster and you will connect to the cluster via the intercluster trunk.
- Dial a NANP phone number without a "900" area code from a phone within your cluster and you will connect to the cluster via the digital gateway.

Note Although you have not blocked the "900" area code calling, you can easily block it by going to the route pattern that has the "Block 900 Calls" Route Filter, selecting the **Block this pattern** option, and clicking **Update**.

- Dial a phone number with a “900” area code from a phone within your cluster and you will get a fast busy.

Laboratory Exercise: Configure a Telephony Class of Service for Devices

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco IP Telephony server cluster
- Three Cisco IP Phones
- Gateway devices

Exercise Objective

In this exercise, you will configure partitions and calling search spaces to apply a Telephony class of service for Cisco IP Telephony devices.

After completing this exercise, you will be able to:

- Configure partitions in Cisco CallManager (CCM) Administration
- Configure calling search spaces in CCM Administration
- Assign route patterns and directory numbers to the configured partitions, assign CIPT devices (phones and gateways) to the configured calling search spaces and test the Telephony class of service
- Using calling search spaces, partitions and a translation, configure a phone to use the private line automatic ringdown (PLAR) feature

Job Aids

These job aids are available to help you complete the laboratory exercises:

Table: Partitions

Partition Name	Description	Assigned to DNs and Route Patterns
Employee	All Regular Employees	#000
Lobby	Lobby Directory Numbers	#001
Executive	Executive Employees	#002
ConfRoom	Conference Room DNs	#051
PSTN	PSTN Route Patterns	9.XXXX#
ICT	ICT Route Patterns	#XXX 9.@
INTRA	Translation Pattern	#XXX

Table: Calling Search Spaces

Calling Search Space	Description	Partitions	Assigned to Devices
Unlimited Access	Unlimited Calling Privileges	Employee Lobby Executive ConfRoom PSTN ICT INTRA	Executive Phone
Company Only	Intra and Inter Cluster Calling Only	Employee Lobby ConfRoom ICT INTRA	Employee Phone
Cluster Only	Intra Cluster Calling Only	Employee Lobby ConfRoom INTRA	Lobby Phone Non-IOS MGCP Gateway MGCP Gateway H323 Gateway Translation Pattern ICT Gateways

Table: PLAR Called Party Transformation Mask

Cluster Name	PLAR Number
East 1	92000#
East 2	91000#
East 3	94000#
East 4	93000#
West 1	92000#
West 2	91000#
West 3	94000#
West 4	93000#

Task 1: Configuring Partitions

Configure partitions in CCM Administration with a partition name and description.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Partition**, and select **Add a New Partition** to open the Partition Configuration page.

Step 2 Using the partition configuration data in the Partitions table (from the Job Aids section of this lab), enter all the partition names and the description assigned to your group using the following format:

<< partitionName >> , << description >>

<< partitionName >> , << description >>

…

Step 3 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- To view all partitions you added, select **Back to Find/List Partitions**, and click **Find**.

Task 2: Configure Calling Search Spaces

Configure calling search spaces and assign CIPT devices (phones and gateways) to the configured calling search spaces to apply a Telephony class of service.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Calling Search Space**, and select **Add a New Calling Search Space** to open the Calling Search Space Configuration page.

Step 2 Using the Calling Search Spaces table (from the Job Aids section of this lab), enter a calling search space name and description.

Step 3 Using the information in the Calling Search Spaces table (from the Job Aids section of this lab), choose partitions to add to the calling search space from the available partition box. Highlight a partition, and use the arrows between the available partition box and the selected partition box to move the highlighted partition to the selected partition box.

Step 4 Highlight a partition in the selected partition box, and use the arrows keys to the right of the selected partitions box to place them in the same order as in the Calling Search Spaces table (from the Job Aids section of this lab).

Step 5 Select **Insert**.

Step 6 Select **Add a New Calling Search Space** to open the Calling Search Space Configuration page.

Step 7 Select **Copy** and repeat Steps 2 through 6 to create all calling search spaces listed in the Calling Search Spaces table (from the Job Aids section of this lab).

Exercise Verification

You have completed this exercise when you attain these results:

- To view all calling search spaces you added, select **Back to Find/List Calling Search Spaces**, and click **Find**.

Task 3: Assign Partitions and Calling Search Spaces to Configure a Telephony Class of Service

Assign partitions to directory numbers and route patterns and assign calling search spaces to devices to apply a telephony class of service within a CIPT cluster.

Exercise Procedure

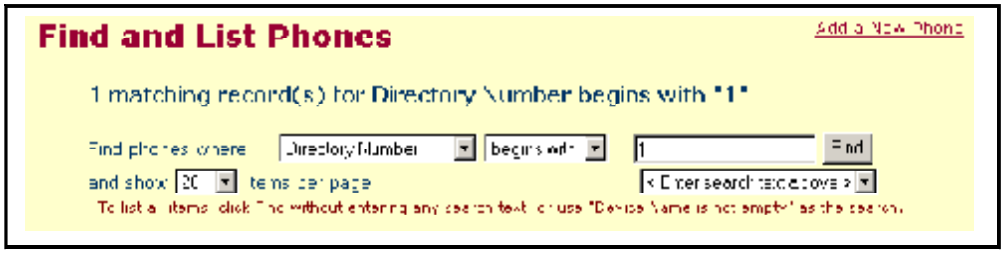
Complete these steps:

Configure Partition and Calling Search Spaces to Directory Numbers and Phones

Step 1 In CCM Administration go to **Device** > **Phone**.

Step 2 Set the search parameters to "Find phones where [**Directory Number**] [**begins with**] [# (cluster number)] as shown in this figure, and then click **Find** to list the phones registered in the cluster by directory numbers.

Figure: Finding Phones by Directory Number



Step 3 Select the phone with directory number "#000" to open the Phone Configuration page.

Step 4 Select **Line 1 - #000** from the left column to get to the Directory Number Configuration page.

Step 5 Choose the **Employee partition** for the Partition, and click **Update**.

Step 6 Select **Configure Device (SEP<MAC Address>)** to return to the Phone Configuration page.

Step 7 Select **Company Only** for the Calling Search Space, click **Update**, and click **OK**.

Step 8 Select **Reset Phone**, click **Reset**, and click **OK**.

Step 9 Select **Back to Find/List Phones** to list the phones registered in the cluster by directory numbers.

Step 10 Repeat Steps 3 through 9 for the other two phones, using the Partitions table and the Calling Search Spaces table (from the Job Aids section of this lab) for partition and calling search space configuration parameters.

Step 11 The executive phone (#002) is able to call both the employee (#000) and lobby (#001) phones.

Step 12 The employee (#000) and lobby (#001) phones can call between each other, but cannot call the executive phone (#002).

Configure Partitions and Calling Search Spaces to Route Patterns and Gateways

Step 13 In CCM Administration, go to **Route Plan > Route Pattern**, and click **Find** to list all the Route Patterns.

Step 14 Select a route pattern from the list to get to the Route Pattern Configuration page for the selected route pattern.

Step 15 Select the partition from the Partitions table (from the Job Aids section of this lab) that corresponds to the route pattern selected.

Step 16 Select **Update**.

Step 17 Select **Back to Find/List Route Patterns**, and repeat Steps 14 through 16 for all the other route patterns.

Step 18 In CCM Administration, go to **Route Plan > Translation Pattern**, and click **Find** to list all the Translation Patterns.

Step 19 Select the translation pattern from the list to get to the Translation Pattern Configuration page.

Step 20 Select the partition from the Partitions table (from the Job Aids section of this lab) that corresponds to the translation pattern.

Step 21 Select the calling search space from the Calling Search Spaces table (from the Job Aids section of this lab) that corresponds to the translation pattern.

Step 22 Select **Update**.

Step 23 In CCM Administration, go to **Device > Gateway**, and click **Find** to list all the Gateways.

Step 24 Select a gateway from the list to get to the Gateway Configuration page for the selected gateway.

Step 25 Select the calling search space from the Calling Search Spaces table (from the Job Aids section of this lab) that corresponds to the selected gateway.

Note	To configure the calling search space for an MGCP gateway, select the endpoints.

Step 26 Select **Update**, and click **OK**.

Note	All gateways must be reset for changes to take place. After all the gateways have been configured with calling search spaces, you will reset the gateways in Steps 28 and 29.

Step 27 Select **Back to Find/List Gateways**, and repeat Steps 24 through 26 for all the other gateways.

Step 28 From the Find and List Gateways page, and select the check box in the table header field so that all the gateways have been selected.

Step 29 Click **Reset Selected**, click **Reset**, and click **OK**.

Exercise Verification

You have completed this exercise when you attain these results:

- From the employee phone (#000) you will be able to dial within the cluster and use the inter cluster trunk route pattern, you will not be able to dial the PSTN route pattern.

- From the executive phone (#002) you will be able to call anywhere, however, other clusters will not be able to call the executive phone, because the gateways calling search space (Company Only) does not have the executive partition listed in the selected partitions.

Task 4: Private Ling Automatic Ringdown (PLAR)

Configure calling search spaces and assign CIPT devices (phones and gateways) to the configured calling search spaces to apply a telephony class of service.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Route Plan > Partition**, and select **Add a New Partition** to open the Partition Configuration page.

Step 2 Create a partition with the name “Hotline” and description “PLAR Translation Pattern”.

<< partitionName >> , << description >>

Step 3 Select **Insert**.

Step 4 In CCM Administration, go to **Route Plan** > **Calling Search Space**, and select **Find a New Calling Search Space** to open the Calling Search Space Configuration page.

Step 5 Select the **Unlimited Access** calling search space to open the Calling Search Space Configuration page for that calling search space.

Step 6 Add the Hotline partition as the first partition listed in the selected partitions box for the Unlimited Access calling search space.

Step 7 Select **Update**.

Step 8 In CCM Administration, go to **Route Plan > Translation Pattern**, and select **Add a New Translation Pattern** to get to the Translation Pattern Configuration page.

Step 9 Leave the translation pattern blank.

Step 10 Select **Hotline** for the partition, and select **Unlimited Access** for the calling search space.

Step 11 Deselect the **Provide Outside Dial Tone** check box.

Step 12 From the PLAR Called Party Transformation Mask table (from the Job Aids section of this lab), enter “<PLAR Number>” for the Called Party Transformation Mask.

Step 13 Select **Insert**.

Step 14 In CCM Administration, go to **Device** > **Phone** and select **Find** to list all the phones in the cluster.

Step 15 From the Find and List Phones page, select the check box in the table header field so that all the phones have been selected.

Step 16 Click **Reset Selected**, click **Reset**, and click **OK**.

Exercise Verification

You have completed this exercise when you attain these results:

- Lift the handset of the Executive phone (#002) and it will ring the phone in the other cluster.

Note The “blank” translation pattern is equal “no-digits”, and the called party transformation mask specifies the DN or route pattern to be dialed.

Task 5: Clean Up

Configure calling search spaces and assign CIPT devices (phones and gateways) to the configured calling search spaces to apply a Telephony class of service.

Exercise Procedure

Complete these steps:

Step 1 Remove the **Hotline** partition from the **Unlimited Access** calling search space.

Step 2 Assign phone lines (directory numbers) to the **Employee** partition.

Step 3 Assign all phones and the #XXX translation pattern to the **Unlimited Access** calling search space.

Exercise Verification

You have completed this exercise when you attain these results:

- All phones and gateways are able to dial all directory numbers and route patterns.

Laboratory Exercise: Configuring CAC and SRST

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Gatekeeper device (2600 or 3600)

Exercise Objective

In this exercise, you will be configuring bandwidth, zone settings, and configuration information for Cisco CallManager (CCM) Administration of a gatekeeper device (2600, 3600).

After completing this exercise, you will be able to:

- Configure a gatekeeper for call admission control (CAC) and as an “anonymous device”
- Configure Locations in CCM administration
- Configure the SRST feature on the default gateway

Command List

The commands used in this exercise are described in the table here.

Table: Gatekeeper Commands

Command	Description
enable	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
configure terminal	Enters global configuration mode.
zone local <name> cisco.com	Specifies the zone controlled by the gatekeeper.
zone subnet <name> [ip address/bit mask] enable	Gatekeeper to accept discovery and registration messages sent by endpoints in designated subnets.
no zone subnet <name> [ip address/bit mask] enable	Gatekeeper to deny discovery and registration messages sent by endpoints in the configured subnets.
zone prefix <name> [digits]	Configures the prefix or digits associated to a zone.
gw-type-prefix 1#* default-technology	Configures the default technology.
bandwidth total zone <name> [kbps]	Configures the total bandwidth allowed in the specified zone.
bandwidth session zone <name> [kbps]	Configures the total bandwidth allowed during a session (call) in a zone.
no shutdown	Enables gatekeeper.

Task 1: Configure Gatekeeper

In this task, you will configure the gatekeeper.

Exercise Procedure

Complete these steps:

Step 1 Gather gateway information. Write down the gatekeeper IP address information below:

IP Address: _____

Step 2 Telnet into the gatekeeper and use “cisco” as the password. Enter “enable” and the password “cisco” to enter enable mode.

Step 3 Use the command **configuration terminal** or **config t** to enter configuration mode.

Step 4 Enter gatekeeper configuration mode. Enter gatekeeper from configuration mode. The prompt should be: Gatekeeper(config-gk)#.

Step 5 Configure gatekeeper parameters. Use the information from the command table, and enter the following commands to configure the gatekeeper:

```
zone local <Cluster code> cisco.com

zone subnet <Cluster code> <(1)> enable

zone subnet <Cluster code> <(2)> enable

no zone subnet <Cluster code> 0.0.0.0/0 enable

zone prefix <Cluster code> <zone prefix>




gw-type-prefix 1#* default-technology




bandwidth total zone <Cluster code> 256

bandwidth session zone <Cluster code> 256

no shutdown
```

Step 6 Save the configuration. Enter “end”, and enter “write terminal” in enable mode to save the configuration. Enter “exit” to close the telnet session.

Step 7 In CCM Administration, go to **Device > Add a New Device** to open the Add a New Device page.

Step 8 Choose **gatekeeper** from the list of device types, and select **Next**.

Step 9 Enter the IP address of the gatekeeper.

Step 10 For the description, enter the type of device being used as the gatekeeper.

Step 11 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- The gatekeeper device is identified in the CCMAdmin.

Task 2: Configure Locations

Configure locations to provide call admission control in a centralized call processing model.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **System >Locations** to open the Location Configuration page.

Step 2 Enter “Branch_1” as the location name, and enter “256” for the bandwidth.

Step 3 Click **Insert**.

Step 4 Open the Phone Configuration page for a phone device registered in the cluster.

Step 5 Select **Branch_1** as the location for that device.

Step 6 Update and reset the phone.

Exercise Verification

You have completed this exercise when you attain these results:

- When a call is established between the updated phone and another phone in the cluster, place the updated phone on hold. The “tone on hold” (beep) will be played instead of the music on hold.

Task 3: Configuring SRST

In this task, you will configure SRST on the default gateway. This will provide phone service to Cisco IP Phones when the phones are unable to connect to their Cisco CallManager(s).

Exercise Procedure

Complete these steps:

Step 1 Telnet to the default router.

Step 2 Enter the global configuration mode so the prompt looks like the following:

```
Hostname(config)#
```

Step 3 At the prompt, enter “call-manager-fallback”.

Step 4 You are now in the call-manager-fallback configuration mode; the prompt will look like the following:

```
Hostname(config-cm-fallback)#
```

Step 5 Enter the following command to enable the router to receive messages from the Cisco IP Phones through the specified IP addresses and ports. The default port is 2000:

```
ip source address <router ip address> port 2000
```

Step 6 Enter the following command to configure the maximum number of Cisco IP Phones that can be supported by the router. The default is zero.

```
max-ephones <number>
```

Step 7 Enter the following command to set the maximum number of directory numbers or virtual voice ports that can be supported by the router. The default is zero.

```
max-dn <number>
```

Step 8 In the Cisco CallManager Administration, go to **System > Device Pool** to open the Device Pool Configuration screen.

Step 9 For the Device pools you have created, select the **SRST Reference** and use the menu to select **Use default gateway**. By specifying Use Default Gateway, if a phone cannot reach any CCMs, it tries to connect to its IP gateway as an SRST gateway.

Step 10 Click **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- You can fail both CCM in the cluster or disconnect the WAN link. The Cisco IP Phones fail to the default router and display that the phones are in CallManager Fallback Mode.

Laboratory Exercise: Configuring Media Resources

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco IP Telephony server cluster (two Cisco CallManager [CCM] servers)
- Cisco Catalyst 6000 with a T/E-1 module (WS-X6608-T/E-1)
- Three Cisco IP Phones
- Audio files (MP3 or WAV format)

Exercise Objective

In this exercise, you will configure media resources (MTP, CONF, XCODE and MOH) for devices to use.

After completing this exercise, you will be able to:

- Configure hardware media resources (CONF and XCODE) in a CCM database
- Configure Meet-Me directory numbers to support Meet-Me conferences
- Configure media resource groups (MRG) and media resource group lists (MRGL) and assign the MRGL to devices
- Configure and add new audio source files used by the music on hold servers and assign the new audio source files to devices

Command List

The commands used in this exercise are described in the table here.

Table: Catalyst 6000 Commands

Command	Description
`enable`	To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.
`show port [module/port]`	This command shows the settings of a port.
`Set vlan <vlan number> <mod/port>`	This command assigns a port to a VLAN.

Job Aids

These job aids are available to help you complete the laboratory exercise(s):

Table: Standard Table

Cluster Name	Voice VLAN	Data VLAN
East 1	10	15
East 2	20	25
East 3	30	35
East 4	40	45
West 1	10	15
West 2	20	25
West 3	30	35
West 4	40	45

Pre-Test Task: Default Media Resource Availability

This section has you test the default media resources available when the IP Voice Media Streaming Application service is selected during the Cisco CallManager installation.

Step 1 Set up a call between two phones within your cluster.

Step 2 Select the “Hold” soft key, and the held phone will play the sample audio source file.

Step 3 Select the “Resume” soft key to reconnect the call.

Step 4 Select the “more” soft key, and select the “Confrn” soft key. (Audio will play on the “automatically” held phone).

Step 5 Dial a directory number of another phone in the cluster to set up a call. Select the “Confrn” soft key to establish an ad-hoc conference.

Step 6 From the phone that set up the conference, select the “more” soft key. Press the third soft key from the left (soft key should be labeled “RmLstC”) to remove the last person added to the conference from the conference.

Without extra configuration, ad-hoc conference and MOH are available.

Task 1: Configure Hardware Media Resources

Configure hardware media resources in the CCM database.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Services > Media Resources** and select **Conference Bridge** to open the Conference Bridge Configuration page.

Step 2 The following are three conference bridge types that you can choose from:

- Cisco Conference Bridge Software
- Cisco Conference Bridge Hardware
- Cisco IOS Conference Bridge

Step 3 Choose **Cisco Conference Bridge Hardware** as the conference bridge type.

Step 4 Telnet into the Catalyst 6000 (use the IP address from above) by going to **Start > Run**. In the box, enter "telnet [ip address]". At the prompt, enter the password "cisco". Enter enable mode by entering "enable". If prompted for a password, enter the password "cisco".

Step 5 In the Catalyst 6000, enter "show port [module number]". In the space below, write down the MAC address of the port number your group is assigned:

_____

Step 6 If the port is not in the correct VLAN, assign the port to the voice VLAN for your cluster using the following command: **set vlan <vlan> <mod/port> .**

Step 7 In the CCM Administration, on the Conference Bridge Configuration page, enter the MAC address from Step 5.

Step 8 For the Description, enter the IP address of the Catalyst switch followed by the module and port number as shown below:

```
<IP Address> <mod/port>

172.16.1.3 3/2
```

Step 9 Select the **BA_DP** for the **device pool**.

Step 10 Select **Insert**.

Step 11 Reset the device from the Cisco CallManager Administration page.

Configure Transcoder

Step 12 In CCM, go to **Services > Media Resources** and select **Transcoder** to open the Transcoder Configuration page.

Step 13 Telnet into the Catalyst 6000 (use the IP address from above) by going to **Start** > **Run**. In the box, enter "telnet [ip address]". At the prompt, enter the password

"cisco". Enter enable mode by entering "enable". If prompted for a password, enter "cisco".

Step 14 In the Catalyst 6000, enter "show module [module number]". (Use the module number from above). In the space below, write down the MAC address of the port number your group is assigned:

Step 15 If the port is not in the correct VLAN, assign the port to the voice VLAN for your cluster using the following command: **set vlan <vlan> <mod/port>**.

Step 16 In the CCM Administration, on the Transcoder Configuration page, enter the MAC address from Step 14.

Step 17 For the Description, enter the IP address of the Catalyst switch followed by the module and port number as shown below:

```
<IP Address> <mod/port>

172.16.1.3 3/2
```

Step 18 Select the **BA_DP** for the device pool.

Step 19 Select **Insert**.

Step 20 Reset the device from the CCM Administration page.

Exercise Verification

You have completed this exercise when you attain these results:

- Telnet into the Catalyst 6000, enter the global configuration mode, and enter the command **show port <mod/port>** to view the settings of the conference resource. The type will be CFB and the IP address of the CCMs will be listed. Now the device is ready to be used.

- Telnet into the Catalyst 6000, enter the global configuration mode, and enter the command **show port <mod/port>** to view the settings of the transcoder resource. The type will be MTP and the IP address of the CCMs will be listed. Now the device is ready to be used.

Task 2: Configure Meet-Me Directory Numbers

Configure a meet-me directory number range to use the conferencing media resource.

Exercise Procedure

Complete these steps:

Step 1 Select **Meet-Me Number/Pattern Configuration** from the top right of the Conference Bridge Configuration page to open the Meet-Me Number/Pattern Configuration page. Or, go to **Feature > Meet-Me Number/Pattern**.

Step 2 Enter "<Cluster number>58X", and place it in the Employee partition to configure a Directory Number or Pattern.

Step 3 Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- Set up a Meet-Me conference using a directory number within the range of Meet-me pattern configured.

Note To set up a Meet-Me conference, go off-hook on a phone, select the "more" soft key, select the "Meetme" soft key, and enter the Meet-Me directory number. Once the Meet-Me conference is established, dial the Meet-Me directory number to join the Meet-Me conference from another phone.

Task 3: Configure Media Resource Groups and Media Resource Group Lists

Configure media resource groups and media resource group lists and apply the MRGL to devices to allow devices access to media resources.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Service** > **Media Resource** > **Media Resource Group** to open the Media Resource Group Configuration page.

Step 2 Enter the name “SoftwareMRG”. For the description, enter “Software type media resources”. Select all software type (MTP and CFB<server name>) available media resources (excluding MOH) to the selected media resources box and prioritize your resources. Select **Insert**.

Step 3 Add another Media Resource Group by selecting **Add new Media Resource Group** in the left column, or copy an existing media resource group and change the name and modify the media resources. Create the following MRGs and assign media resources accordingly:

- HardwareMRG
- MOH_MRG
- MTP_MRG
- CFB_MRG
- XCODE_MRG

Configure Media Resource Group Lists

Step 4 In CCM Administration, go to **Service** > **Media Resource** > **Media Resource Group List** to open the Media Resource Group List Configuration page.

Step 5 Enter the name “All_MRGL”. For a description, enter “All configured media resources”. Then add all available media resource groups to the selected media resource group box and prioritize your groups. Select **Insert**.

Step 6 Add another Media Resource Group List by selecting **Add new Media Resource Group List** in the left column, or copy an existing media resource group list and change the name and modify the media resource groups. Create the following MRGL and assign media resource groups accordingly:

- NOCFB_MRGL
- MOH_MRGL

Apply Media Resource Group List to Devices

Step 7 In CCM Administration, go to **System > Device Pool** to open the Device Pool Configuration page.

Step 8 Select the **BA_DP** device pool, and select **All_MRGL** from the menu for Media Resource Group List.

Step 9 Find a Cisco IP Phone and select a MRGL from the menu for Media Resource Group List. Select **Update** and then reset the phone.

Exercise Verification

You have completed this exercise when you attain these results:

- Set up conferences when all devices have access to all media resources.
- Assign MRGL that has no conference resources to a phone, and try to set up a conference.

Task 4: Configure Audio Sources for Music On Hold

Add audio source files to customize the music on hold. Assign the new audio source files to devices in the cluster.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Service** > **Media Resources** > **Music On Hold Audio Source** to open the Music On Hold Audio Source Configuration page.

Step 2 Select the **SampleAudioSouce** from the left column, and view the settings for this audio source.

Step 3 Most standard wav and mp3 files serve as valid input audio source files. Get these files from your instructor or provide some of your own mp3 files. Get a wav or mp3 file and copy it to the directory **C:\Cisco\DropMOHAudioSourceFilesHere** on the **publisher**.

Step 4 Open the Music On Hold Audio Source Configuration page. From the MOH Audio Source File, verify the audio file and check the MOH Audio Source File Status.

Step 5 Choose a number from the Audio Source ID, and select the **Play continuously** check box. Select **Insert**.

Step 6 Repeat Steps 3 through 5 to add more audio files.

Step 7 At the bottom of the page, select **Reset MOH servers**.

Assign MOH to Device Pools

Step 8 Open the Device Pool Configuration page.

Step 9 Choose an Audio Source from the menu for User Hold Audio Source.

Step 10 Choose an Audio Source from the menu for Network Hold Audio Source.

Step 11 Click **Update**, and click **Reset**.

Assign MOH to Phones

Step 12 Open the Cisco IP Phone Configuration page for a phone in your cluster.

Step 13 Choose an Audio Source from the menu for User Hold Audio Source.

Step 14 Choose an Audio Source from the menu for Network Hold Audio Source.

Step 15 Click **Update**, and click **Reset**.

Exercise Verification

You have completed this exercise when you attain these results:

- Depending on the type of hold (user or network) and where the audio source files are assigned, did the correct audio play.

Laboratory Exercise: Configuring Features

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco IP Telephony server cluster (two Cisco CallManager (CCM) servers)
- Remote Cisco IP Telephony server cluster
- Three Cisco IP Phones
- Cisco Router (default gateway) that supports SRST

Exercise Objective

In this exercise, you will be able to configure and use the call park and call pickup features.

After completing this exercise, you will be able to:

- Configure and use the call park feature
- Configure and use the call pickup feature
- Configure IP Phone Services

Task 1: Configure Call Park

Configure a call park directory number range and then use the call park feature within your cluster.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Feature > Call Park** to open the Call Park Configuration page.

Step 2 Enter "<Cluster number>66X" for the call park number or range. Assign it to the Employee partition, and select a CCM to which to assign it. Select **Insert**.

Step 3 Select **Add new Call Park Number/Range** from the left column. Enter "<Cluster number>67x" for the call park number or range. Assign it to the Employee partition, and select the other CCM to which to assign it. Select **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- Establish a call between two phones, and park the call. (Select the "more" soft key, and then select the "park" soft key.) Take note of the call park number, go to another phone, and pick up the call.

Task 2: Configure Call Pickup

Configure a call pickup group and assign the call pickup group to the phones in your cluster and then use the call pickup feature within your cluster.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Feature > Call Pickup** to open the Call Pickup Configuration page.

Step 2 Enter "<Cluster number>685" for the directory number, assign it to the Employee partition, and select **Insert**.

Step 3 Repeat Step 3 to create another call pickup group. Use "<Cluster number>686" for the directory number, and assign it to the Employee partition.

Assign Call Pickup to a Directory Number

Step 4 Find a phone, and open the Phone Configuration page.

Step 5 Select a line number for that phone, and scroll down to the Call Forward and Pickup Settings.

Step 6 Choose a call pickup group from the Call Pickup Group menu.

Step 7 Select **Update** and then reset the phone.

Step 8 Repeat Steps 4 through 7 for all phones in your cluster.

Exercise Verification

You have completed this exercise when you attain these results:

- Call a directory number in your cluster. From a phone not ringing in the cluster, pick up the call.

Note If the phone you use to pickup the call is in the same call pickup group as the phone that is ringing, go off-hook and select the "Pickup" soft key. To get to the "Pickup" soft key, select the "more" soft key and then you can select the "Pickup" soft key. This phone will ring and you will need to answer the call.

Note If the phone you use to pickup the call is NOT in the same call pickup group as the phone that is ringing, go off-hook and select the "GPickup" soft key. To get to the "GPickup" soft key, select the "more" soft key and then you can select the "GPickup" soft key. Enter the call pickup group number. This phone will ring; you will need to answer this call.

Laboratory Exercise: Configuring Cisco IPMA

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco CallManager (CCM) cluster

Exercise Objective

In this exercise, you will configure a Cisco IP Manager Assistant (IPMA).

After completing this exercise, you will be able to:

- Configure Cisco CallManager Administration for Cisco IPMA use
- Configure the Cisco IPMA Wizard

Task 1: Running the IPMA Wizard

This task will guide you through the IPMA Configuration Wizard.

Exercise Procedure

Complete these steps:

Cisco CallManager IPMA Configuration Wizard

Step 1 Install the BAT utility on the Publisher server. Go to **Applications > Install plugins** to select the BAT tool. Run this service from the current location and follow the on screen prompts. You do not need to install the TAPS utility.

Step 2 Go to **Service > Cisco IPMA Configuration Wizard**. Click **Next**.

Note	The Cisco IPMA Configuration Wizard is only run on the Publisher.

Step 3 Review the default partitions created for the IPMA Managers, and click **Next**. (You can keep the defaults.)

Step 4 Review the partitions for the IPMA computer Telephony integration (CTI) route point, and select **Next**. (You can keep the defaults.)

Step 5 Review the IPMA partitions for All Users except the managers, use the defaults, and select **Next**.

Step 6 You are prompted for the Managers Calling Search Space. The Calling Search Space already contains the necessary partitions for IPMA along with all the other partitions that you have created. You may remove any unnecessary partitions from the list. Click **Next**.

Step 7 You are prompted with the IPMA Calling Search Space used for the manager's and assistant's own lines and user lines. Select the defaults, and click **Next**.

Step 8 The Configuration Wizard prompts you with information to prepend the existing Calling Search Spaces. Keep the defaults, and click **Next**.

Step 9 Accept the default settings to configure the CTI route point and translation patterns. Select the device pool for your cluster, and click **Next**.

Step 10 Configure the IPMA phone service for your cluster. Choose the **Publisher service** and the **Primary IPMA server**, and click **Next**.

Step 11 The Wizard window displays the information that you have configured for the IPMA service. Select **Submit** if all the information appears to be correct; otherwise, use the back button to make any changes.

Step 12 When the Wizard is finished configuring this information, a window appears prompting you to click **Finish**.

Step 13 Close the **IPMA Configuration Wizard**. Start and stop the IPMA service through the service activation screen located in the Cisco CallManager Serviceability window under tools.

Exercise Verification

You have completed this exercise when you attain these results:

- The Configuration Wizard runs successfully.

Task 2: Configuring Manager and Assistant IPMA Phone Parameters

This task will configure the IPMA manager and IPMA assistant.

Exercise Procedure

Complete these steps:

Cisco CallManager IPMA Manager and Assistant IP Phone Parameters

Step 1 Configure two 7960 IP Phones to be used as the manager and assistant.

Step 2 Select one of the IP Phone devices to configure as the manager's phone. Create or update a directory number (DN) to be the primary line. Add the partition on the primary line of the manager's phone to be in the Generated_IPMA_Manager partition and the CSS-I-E Calling Search Space. Create an intercom line and assign it to the Generated_IPMA_Everyone partition and assign it to the CSS_I_E Calling Search Space. Update this information.

Step 3 Return to the configure device, and select the soft key template for the Standard IPMA Manager.

Step 4 Update the phone, select the **Subscribe/Unsubscribe services** window, and subscribe to the IPMA Phone service. Update the information and reset the phone.

Step 5 Select the IP Phone to designate as the assistant. Create or update the intercom line to include the partition Generated_IPMA_Everyone and a CCS_I_E Calling Search Space. Create a second DN to be the proxy line, assign this line to the Generated_IPMA_Everyone partition and the CSS_M_E Calling Search Space. Update this information.

Step 6 From the phone configuration window, select the soft key template for the Standard IPMA Assistant.

Step 7 Update the phone, select the **Subscribe/Unsubscribe services** window, and subscribe to the IPMA Phone service. Update the information and reset the phone.

Step 8 Change the other phones in the cluster to include the Generated_IPMA_Everyone partition and the Calling Search Space of CSS_I_E for these phones to be able to reach the manager and assistant.

Configuring the IPMA Manager and IPMA Assistant Users

Note	Ensure that there are two users already created. One will be the Manager, the other will be the assistant. If you have not created users, create them now, and then continue.

Step 9 To configure the IPMA manager and assign an IPMA assistant to an existing user, go to **User > Global Directory**.

Step 10 Select the user that will be the IPMA manager, and click **Search**. Or, enter the user name in the field, and click **Search**.

Step 11 Display user information for the chosen manager, and click the user name. The User Information window displays.

Step 12 Configure the IPMA information for the manager, and click **Cisco IPMA** from the Application Profiles list box.

Step 13 The first time that the user is configured for IPMA, the User Information window displays a message to continue configuration for a manager or to cancel if the user is not a manager. Click **Continue**.The User Information window redisplays and contains Manager Configuration information such as device name/profile and intercom lines.

Note To view existing assistant configuration information, click the assistant name in the Assigned Assistants list. The assistant IPMA configuration information displays. To return to the manager configuration information, click the manager name in the Associated Managers list on the Assistant Configuration window.

Step 14 To assign an assistant to the manager, click the **Add/Delete Assistants** link.The Assign Assistants windows displays.

Step 15 To find an assistant, click **Search** or enter the name of the assistant in the search field. A list of available assistants displays in the window.

Step 16 Select the check box next to the name of the assistant that you want to assign to the manager. A manager can have a maximum of five assigned assistants.

Step 17 To save and continue, click **Update**. To return to the IPMA manager configuration window, click **Update and Close**. The User Information displays the manager configuration, and the assistant that you configured displays in the Assigned Assistants list.

Step 18 A dialog box appears letting you know that you must restart the Tomcat service for the changes to take place. Select **OK**.

Perform the following procedure to configure the primary and incoming intercom line appearances for a manager.

Step 19 The User Information window redisplays and contains manager configuration and IPMA controlled lines information.

Step 20 From the Device Name/Profile selection box, choose the device name or device profile to associate with the manager.

Note If a Device Profile is chosen, the manager must log on the phone using Extension Mobility before accessing IPMA. However, if the manager telecommutes, Device Profile should be chosen.

Step 21 From the Intercom Line section, use the selection box to choose the intercom line appearance for the manager.

Step 22 In the IPMA Controlled Lines area, in the associate manager lines to the assistant proxy line, choose the line number of the manager phone from the Available Lines selection box. (Use the right and left arrows to choose the lines.) Configure up to five IPMA-controlled lines.

Step 23 When the configuration is complete, click **Update**.The update takes effect immediately.

Configuring the IPMA Assistant

Step 24 Configure the IPMA assistant and assign proxy and incoming intercom lines by choosing **User > Global Directory**.

Step 25 To find the user that will be the IPMA assistant, click **Search**, or enter the user name in the field and click **Search**.

Step 26 Display the user information by clicking the user name. The User Information window displays.

Step 27 Configure IPMA information for the assistant by clicking **Cisco IPMA** from the Application Profiles list.

Step 28 If this user has not been assigned to a manager as an assistant, the User Information window displays a message to continue configuration for a manager or cancel if the user is not a manager. Click **Cancel**.

Step 29 From the Device Name selection box, choose the device name to associate with the assistant.

Step 30 From the Intercom Line Appearance selection box, choose the incoming intercom line appearance for the assistant.

Note To view existing manager configuration information, click the manager name in the Associated Managers list. The manager IPMA configuration information displays. To return to the assistant configuration information, click the assistant name in the Assigned Assistants list on the manager configuration window.

Step 31 Use the selection boxes in the Manager Association to Assistant Proxy Line area to assign and associate manager line numbers to the assistant line numbers.

Step 32 In the Proxy Line selection box, choose the assistant line.

Step 33 In the Manager Name selection box, choose the manager for whom this proxy line will apply.

Step 34 In the Manager Line selection box, choose the manager line for which this proxy line will apply.

Step 35 Click **Update**. The update takes affect immediately.

Service Parameters Configuration

Step 36 Confirm that the service parameters are properly configured for the IPMA by going to **Service > Service Parameters** and selecting the server address for the IPMA server and the Cisco IP Manager Assistant Service. Make sure the IP address for the CTI Manager (Primary) and the Cisco IPMA Server (Primary) are correctly included. This address should reflect the primary IP address of the publisher CallManager.

Step 37 Start and stop the Tomcat service for the settings to take affect.

Installing the Assistant Console Application

Step 38 Begin the installation by accessing the following URL: http://<IPMA server>/ma/Install/IPMAConsoleInstall.jsp. (IPMA server is the IP address of the server that has the IPMA service running on it.)

Step 39 The installation will create an Icon on the desktop to launch the IPMA Assistant. Click the icon and configure the IP address of the IPMA server. Save this information.

Installing the Manager Configuration Window

Step 40 Begin the installation by accessing the following URL: http://<IPMA server>/ma/desktop/maLogin.jsp. (The IPMA server is the IP address of the server that has the IPMA service running on it.)

Step 41 The URL will launch the Managers configuration window and allow you to login and customize the managers IPMA settings.

Exercise Verification

You have completed this exercise when you attain these results:

- The IPMA Assistant runs correctly.
- The IPMA assistant and manager can make and receive calls.

Laboratory Exercise: Adding and Configuring a User and User Options

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco IP Telephony server cluster (two Cisco CallManager [CCM] servers)
- Three Cisco IP Phones

Exercise Objective

In this exercise, you will add users to the CCM database and configure user options using the Cisco IP User Option pages.

After completing this exercise, you will be able to:

- Add a user to the CCM database
- Configure user options using the CCM User Option pages

Task 1: Add Users in Cisco CallManager

You will be adding a list of users into CCM and associating those users to devices.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **User > Add a New User** to open the User Information page.

Step 2 Enter complete user information, which is required information. Write down the user ID and password that you create.

Step 3 If you know the directory number that you are going to assign to this user, enter that directory number in the telephone setting.

Step 4 Select **Insert**.

Step 5 Select **device association** from the left column. Select **select devices** from the Available Device List Filters section.

Step 6 Select a phone device in your cluster, and select the **primary extension**. Select **Update**.

Step 7 Create another user. Repeat Steps 1 through 6.

Exercise Verification

You have completed this exercise when you attain these results:

- Go to **User > Global Directory** and select **Search**. All the users that have been added are listed.

Task 2: Activating the User Option Service

In this task, you will activate the user option services.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Features > Cisco IP Phone Services** to open the Cisco IP Phone Service Configuration page.

Step 2 Enter “CCMUser” as the service to create, and enter a description.

Step 3 Enter the URL for the CCMUSER page: HTTP://<Server Name or IP Address>/CCMUser.

Exercise Verification

You have completed this exercise when you attain these results:

- Open a web page, and enter the URL that was created to view the user option web page.

Task 3: Configure User Options from the User Options Configuration Page

Log on to the CCM User Options page and configure options for the devices that the user is associated with.

Exercise Procedure

Complete these steps:

Step 1 Open the CCM User Options logon page by browsing to the following:

http://<server_ip_address_or_server_name>/ccmuser/logon.asp

Step 2 Enter the user ID and password of one of the users created in Task 1.

Step 3 Click **Log On**.

Step 4 Select a device to configure.

Step 5 Change settings on the Cisco CallManager User Options page for the device that the user is associated with such as adding speed dials, forward all calls, and changing the locale of the pages and the phone.

Exercise Verification

You have completed this exercise when you attain these results:

- The changes made in the CCM User Options pages are reflected on the device to which the user is assigned.

Task 4: Configure Cisco IP Phone Service

Using the sample Cisco IP Phone services file, add Cisco IP Phone services to the CCM database.

Exercise Procedure

Complete these steps:

Step 1 Write down the path where the sample services self-extracting zip file is located.

_____

Step 2 Get the sample file and copy to the publisher, or open it from the current location.

Step 3 Open the file, and unzip it. Select **OK** at the dialog box stating "12 files unzipped successfully." The files will extract to C:/CiscoWebs/User. Select **Close**.

Configure the Cisco IP Phone Service

Step 4 In CCM Administration, go to **Feature > Cisco IP Phone Service** to open the Cisco IP Phone Service Configuration page.

Step 5 Enter a service name of your choice, enter the URL below, and provide a description.

http://<ip_address>/ccmuser/sample/sample.asp

Step 6 Select **Insert**.

Step 7 In CCM Administration, go to **System > Enterprise Parameters**. At the URL Services parameter, change the server name in the URL to the IP address of the server, if this has not already been done. Select **Update**.

Subscribe to the Cisco IP Phone Service

Step 8 Open the Phone Configuration page in CCM Administration, and find your phone. Then, go to the Phone Configuration page.

Step 9 Select **Subscribe/Unsubscribe Services** from the top right of the page. Choose a service from the menu, and select **Continue**.

Step 10 The Service Name will be displayed on your phone. Edit the service name to "**<Cluster Code> Sample**". Select **Subscribe** and close the dialog box.

Exercise Verification

You have completed this exercise when you attain these results:

- Press the services button from the phone, and select the service from the list.

Laboratory Exercise: Configuring Cisco CM Attendant Console

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco CallManager (CCM) Cluster

Exercise Objective

In this exercise, you will install and configure Cisco CM Attendant Console.

After completing this exercise, you will be able to:

- Configure the Cisco CM Attendant Console server
- Install and configure the Cisco CM Attendant Console client

Task 1: Creating the ac User Account

You must configure one user named "ac" in CCM Administration and associate the attendant phones and the pilot points with the user. If you do not configure this user, the attendant console cannot interact with CTIManager. Perform the following procedure to configure the ac user.

Exercise Procedure

Complete these steps:

Step 1 From CCM Administration, go to **User > Add a New User**. The User Information window displays.

Step 2 In the First Name and Last Name fields, enter “ac”.

Step 3 In the User ID field, enter “ac”.

Step 4 In the User Password field, enter “12345”.

Step 5 In the Confirm Password field, enter “12345”.

Step 6 Enter a PIN and telephone number.

Step 7 Select the **Enable CTI Application Use** check box. You must select this box for the attendant console to interact with CTIManager.

Step 8 Click **Insert**.

Exercise Verification

You have completed this exercise when you attain these results:

- The ac user that you created is displayed in the global directory.

Task 2: Associating Devices and Pilot Points with the ac User

Before the attendant uses the attendant console, you must associate the attendant console phones and pilot points to the ac user.

Exercise Procedure

Complete these steps:

Step 1 In the Application Profiles column of the User Information window, click **Device Association**.

Step 2 Perform one of the following tasks: Click **Select Devices**.

Step 3 Select the check box of the attendant console phones/pilot points you must associate with the user.

Step 4 Click **Update** to assign the phones/pilot points to the "ac" user.

Exercise Verification

You have completed this exercise when you attain these results:

- The ac user is associated with the phones/pilot points.

Task 3: Server Configuration (Cisco Telephony Call Dispatcher)

Configure the Cisco CM Attendant Console server in preparation for installing and configuring the Cisco CM Attendant client.

Exercise Procedure

Complete these steps:

Step 1 In CCM Administration, go to **Service > Cisco CM Attendant Console**.

Step 2 Select **Cisco CallManager Attendant Console User Configuration** from the top right of the page, and enter the user ID and password. Select for the station type "Attendant". (Users should be predefined in DCDir via the CCM Administration User page).

Step 3 Click **Insert**.

Step 4 Select **Pilot Point Configuration** from the top right of the page, and enter the Pilot Name, BA_DP for the device pool, and Pilot DirN. (This is the Directory number used to call the Cisco CM Attendant Console, which is usually a main number.)

Step 5 Click **Insert**.

Step 6 Select **Hunt Group Configuration** from the top right of the page.

Step 7 Click the new Pilot Point in the left column.

Step 8 Enter Device or User Member Information. (The User Member method is preferred.) Choose the user and line appearance for each member of the Hunt group. The last member of the group should be the AutoAttendant or VoiceMail DirN that will be called when the user is offline.

Step 9 Build a phone for the Cisco CM Attendant Console user that includes the lines defined in the Hunt Group.

Step 10 Restart Cisco TCD from Control Center.

Exercise Verification

You have completed this exercise when you attain these results:

- The TCD service is running.

Task 4: Cisco CM Attendant Console Client Installation and Configuration

Install and configure the Cisco CM Attendant Console client to use with the user and within the cluster.

Exercise Procedure

Complete these steps:

Step 1 From the Client PC, use Internet Explorer to browse to the CCMAdmin page. Go to **Applications > Install** > **Plugins > Cisco CallManager Attendant Console** to start the installation. Follow the onscreen prompts to complete the installation.

Step 2 For the Attendant Console Login ID, choose the user that was defined in Server Configuration..

Step 3 Enter the CM IP address, port 4321, and MAC address of the Attendant's phone.

Step 4 Complete the installation and reboot.

Step 5 Start the Cisco Attendant Console Client.

Step 6 Select **Settings**, and enter the phone MAC. Leave the Cisco TCD Database Path blank, and enter the CCM IP address, User Login info, and Line State Server IP address. Click **OK**.

Step 7 Close and restart the Client.

Exercise Verification

You have completed this exercise when you attain these results:

- Log in and go online from the Cisco Attendant Console application. From a phone, call the pilot directory number and the call will appear in the Attendant Console UI.

Laboratory Exercise: Configuring Cisco IP SoftPhone

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco CallManager (CCM) cluster
- Cisco IP SoftPhone application

Exercise Objective

In this exercise, you will configure a Cisco IP SoftPhone.

After completing this exercise, you will be able to:

- Configure CCM Administration for Cisco IP SoftPhone use
- Install and configure the Cisco IP SoftPhone application

Exercise Procedure

Complete these steps:

Cisco CallManager Administration Configuration

Step 1 In CCM Administration, go to **Phones > Add new phone > Phone type = CTI Port**.

Step 2 Enter the name, device pool, and DN. (This can be a prime line of the controlled phone; this DN cannot be shared as a prime line on another phone.)

Step 3 Next you will need to associate your user(s) to phones that you want to have Softphone control.

Step 4 Select **user** from the Global Directory, and click **Associate devices**.

Step 5 Be sure to select the check box for CTI enable on the user page.

Step 6 Use the device List Filter to find a Softphone DN (CTI port).

Cisco IP SoftPhone Installation and Configuration

Step 7 Install package. Set user name password to match existing users in DC directory. Set CM IP address and reboot when prompted.

Step 8 If changes are needed after installation, go to **Control Panel > Phone** and **Modem options > Advanced**. Go to **Cisco IP PBX Service Provider > Configure**. Enter the user name and password. (Match CCM user entries.) Enter the CM IP address. Start Softphone. Select a device to control. Softphone should now be operational.

Creating and Using Directory

Step 9 From the Softphone GUI, go to **Settings > Directories**.

Step 10 Enter the directory name.

Step 11 Enter the CM IP or hostname.

Step 12 The port is 8404 (DC directory port). The search base is ou=users, o=cisco.com.

Exercise Verification

You have completed this exercise when you attain these results:

- After installing Cisco IP SoftPhone and rebooting the PC, launch the Cisco IP SoftPhone application and select a line to control.
- Start using Cisco IP SoftPhone.

Laboratory Exercise: Configuring Extension Mobility

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Cisco CallManager (CCM) cluster

Exercise Objective

In this exercise, you will configure and use the extension mobility feature.

After completing this exercise, you will be able to:

- Install the Extension Mobility Service
- Configure CCM for Extension Mobility

Task 1: Adding the Cisco CallManager Extension Mobility Service

In this task, you will be configuring the CCM Extension Mobility Service.

Exercise Procedure

Complete these steps:

Adding the Cisco CallManager Extension Mobility Service

Step 1 From CCM Administration, go to **Features > Cisco IP Phone Services**.

Step 2 At the Service Name field, enter a name for the service.The user sees this name on the phone when the user presses the Services button. Use a meaningful name to identify the service for the user, for example, Extension Mobility.

Step 3 At the Service URL field, enter the IP address of the Cisco CallManager server: http://IPAddrOFCM/emapp/EMAppServlet?device=#DEVICENAME#

Caution	Because the URL is case-sensitive, make sure that you enter the name exactly as described.

Step 4 At the Character Set menu, choose the language that the user will see displayed on the phone.

Step 5 Click **Insert**, and click **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- You can verify the service listed in the IP Phone Services configuration screen.

Task 2: Setting the Service Parameters

Set the Service Parameters in the CallManager Service Parameters Configuration window to accomplish the following tasks:

- Define a system-wide maximum login time
- Define the multi-login behavior, that is, whether you allow the user to log in to more than one device at a time
- Enable the CCM Extension Mobility debug traces

Exercise Procedure

Complete these steps:

Configuring the Service Parameters

Step 1 From CCM Administration, go to **Service > Service Parameters**. The Service Parameters Configuration window displays.

Step 2 From the menu, choose the server address of your CCM.

Step 3 From the Services menu, choose the service that you added. A new Service Parameters Configuration page displays.

Step 4 At the Use 2-Line Template for 7940 Login field, choose **True** if the Cisco IP 7940 is configured for two lines.

The default value specifies False.

CCM Extension Mobility requests a fixed name for the device template on a Cisco IP 7940 phone. The name of the device template for the Cisco IP 7940 phone must be defined and the name of the template is context-sensitive.

Make sure that the device template for the Cisco IP 7940 is 7940 1--Line **or** 7940 2--Line. Use a dash (--) (not a hyphen [-]) and match this capitalization.

Step 5 At the Login Service Enabled field, choose **True** to enable the user login service. Choosing False disables the user login service.

The default value specifies False.

Step 6 At the Enforce Maximum Login Time, choose **True** to specify a system-wide maximum time for logins. After this time, the system automatically logs out the device.

Choosing False means that no system-wide maximum time for logins exists.

The default value specifies False.

Note To set an automatic logout, you must choose **True** in Step 6 and specify a system maximum login time in Step 7. The CCM then uses the automatic logout service for all logins.

Step 7 If you specified True at the Maximum Login Time field in Step 6 of this procedure, specify the maximum login time in Hours:Minutes from 0:01 to 168:00 (one minute to one week).

The default value specifies 8:00 (eight hours).

Step 8 At the Multi Login Behavior field, choose one of the following responses:

- Multiple Logins Allowed: A user can log in to more than one device at a time
- Multiple Logins Not Allowed: The second and subsequent login attempts after a user successfully logs in once will fail
- Auto Logout: After a user logs in to a second device, the CCM automatically logs the user out of the first device

The default value specifies Multiple Logins Not Allowed.

Step 9 At the Enable Debug Traces on field, choose **True** to enable the CCM Extension Mobility Application debug tracing.

The default value specifies False.

Step 10 At the User Alphanumeric userid field, choose **True** to allow the UserID to contain alphanumeric characters. Choosing False allows the UserID to contain numeric characters only.

The default value specifies False.

Step 11 Click **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- You can view the service parameters in the Service Parameters window.

Task 3: Creating the Device Profile for a User

In this task, you will add a device profile for a new user of CCM Extension Mobility.

Exercise Procedure

Complete these steps:

Step 1 From CCM Administration, go to **Device > Device Settings > Device Profile**.

The page refreshes to the Find and List Device Profiles window.

Step 2 Click the **Add a New User Device Profile** link in the upper right corner.

The User Device Profile Configuration window displays.

Step 3 At the User Device Profile Name field, enter a name of your choice for the device profile. You can make this text anything that describes this particular user device profile.

Step 4 From the Phone Button Template field, use the list to perform one of the following tasks:

- Choose **Standard 7960** for Cisco IP Phone Model 7960 only
- Choose **Default 7960** for either the Cisco IP Phone Model 7960 or 7940; the default applies to both the Cisco IP Phones Models 7960 and 7940

Step 5 You can configure one or two Cisco IP Phone 7914 Expansion Modules for this device profile by choosing from the add-on module lists.

Note You may view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate window pops up and displays the phone buttons for that particular expansion module.

Step 6 Click **Insert**.

The Directory Number Configuration page displays.

Step 7 At the Directory Number field, enter the directory number, and click **Insert**.

Step 8 The following prompt displays: The Directory Number has been assigned to the current device. Click **OK** to return to the current device.

Step 9 Click **OK**.

Step 10 The page refreshes to the User Device Profile Configuration window for this device profile.

Step 11 On the User Device Profile Configuration window, choose **Update Service**.

Step 12 To update services, choose the service that you added.

Step 13 Click **Continue**.

Step 14 Click **Subscribe**.

Exercise Verification

You have completed this exercise when you attain these results:

- You can subscribe to the phone services.

Task 4: Associating a User Device Profile to a User

In this task, you will associate a user device profile to a user for CCM Extension Mobility.

Exercise Procedure

Complete these steps:

Step 1 From CCM Administration, go to **User > Add a New User**.

Step 2 At the Add a New User window, enter the first name (for example, jean), last name (for example, brody), and UserID (for example, jbrody).

Note With CCM 3.3 and later, you can specify Alphanumeric/Numeric user IDs for the user logins, instead of just Alphanumeric user IDs. The user IDs remain case-sensitive.

Step 3 At the User Password and Confirm Password fields, enter a password of your choice.

Step 4 At the PIN field, enter a numeric Personal Identification Number (PIN) of your choice. Confirm the PIN number.

Step 5 To save your changes and add the user, click **Insert**.

Step 6 From the left pane, select **Extension Mobility**.

Step 7 Click **Select Profiles** to display the profile that you created. Select the appropriate profile by clicking the box next to the device profile.

Note The first profile selected becomes the default profile.

Step 8 Click **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- The appropriate device profile is assigned to the user.

Task 5: Subscribing Cisco IP Phones to Cisco CallManager Extension Mobility

In this task, you will subscribe to the Cisco CallManager Extension Mobility feature.

Exercise Procedure

Complete these steps:

Subscribing IP Phones to the Cisco CallManager Extension Mobility

Step 1 From the Phone Configuration window, click the **Subscribe Services** link.

Step 2 Using the arrow, choose the service name that you added in the Adding the Cisco CallManager Extension Mobility Service topic (for example, Extension Mobility).

Step 3 Click **Continue**.

Step 4 Click **Subscribe**, and close the window.

Step 5 On CCM Phone Configuration, scroll down to the bottom of the window. Select the **Enable Extension Mobility Feature** check box.

Step 6 At the Log Out Profile field, choose **Use Current Device Settings**.

This action creates an Autogenerated Device Profile as the default device profile. When a logout executes, the Autogenerated Device Profile (the default device profile) replaces the current configuration (the User Device Profile).

Note You could assign a user device profile as the default device profile by selecting **Select a User Device Profile**. Cisco recommends that you use the Autogenerated Device Profile.

Step 7 The remaining fields show the current device information regarding the login status of the device: Log in UserID; Log In Time; Log Out Time.

Step 8 Click **Update**.

Exercise Verification

You have completed this exercise when you attain these results:

- You have now completed the necessary steps for configuring CCM Extension Mobility.
- Log in and out of a phone device and have the user profile appear.

