

CIPT1

Implementing Cisco Unified Communications IP Telephony Part 1

Volume 1

Version 6.0

Student Guide

Editing, Production, and Web Services: 02-15-08



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 563-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www.europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

©2008 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, Gigabit Drive, Gigastack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

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

Table of Contents

Volume 1

<u>Course Introduction</u>	1
Overview	1
Learner Skills and Knowledge	1
Course Goal and Objectives	3
Course Flow	4
Additional References	5
Cisco Glossary of Terms	5
Your Training Curriculum	6
<u>Introduction to Cisco Unified Communications Manager</u>	1-1
Overview	1-1
Module Objectives	1-1
<u>Understanding Cisco Unified Communications Manager Architecture</u>	1-3
Overview	1-3
Objectives	1-3
Cisco Unified Communications	1-4
Cisco Unified Communications Manager	1-6
Cisco Unified Communications Manager Signaling and Media Paths	1-8
Cisco Unified Communications Manager Hardware, Software, and Clustering	1-9
Cisco Unified Communications Manager Cluster	1-11
Cisco Unified Communications Manager Hardware Requirements	1-12
Third-Party Hardware Solutions Approved by Cisco	1-13
Cisco Unified Communications Operating System	1-14
Cisco Unified Communications Operating System Access	1-15
Cisco Unified Communications Manager Database	1-16
Services That Rely on the Publisher	1-17
User-Facing Features	1-18
Cisco Unified Communications Manager Release 6.0 Database Replication	1-19
Database Access Control	1-20
Cisco Unified Communications Manager Licensing Model	1-21
Device License Units	1-23
License File Specifics	1-24
Example License File	1-26
License File Request Process (FlexLM)	1-27
Obtaining Additional Licenses	1-28
Cisco Unified Communications Manager Licensing Tools	1-29
Calculating License Units	1-32
Generating License Unit Report	1-33
Uploading License File	1-34
Summary	1-37
References	1-38
<u>Understanding Cisco Unified Communications Manager Deployment and Redundancy Options</u>	1-39
Overview	1-39
Objectives	1-39
Cisco Unified Communications Manager Deployment Options	1-40
Cisco Unified Communications Manager Single-Site Deployment	1-41
Single Site: Design Guidelines	1-42
Single Site: Benefits	1-43
Cisco Unified Communications Manager Multisite Deployment with Centralized Call Processing	1-44
Multisite WAN with Centralized Call Processing: Design Guidelines	1-46
Multisite WAN with Centralized Call Processing: Benefits	1-47
Cisco Unified Communications Manager Multisite Deployment with Distributed Call Processing	1-48
Multisite Distributed Call Processing: Design Guidelines	1-49
Multisite WAN with Distributed Call Processing: Benefits	1-50

Cisco Unified Communications Manager Multisite Deployment with Clustering Over the WAN	1-51
Clustering Over the IP WAN: Design Guidelines	1-52
Clustering Over the IP WAN: Benefits	1-54
Cisco Unified Communications Manager Call-Processing Redundancy	1-55
1:1 Redundancy Design	1-57
2:1 Redundancy Design	1-59
Summary	1-60
References	1-61
Installing and Upgrading Cisco Unified Communications Manager	1-63
Overview	1-63
Objectives	1-63
Cisco Unified Communications Manager Installation and Upgrade Overview	1-64
Cisco Unified Communications Manager Installation and Upgrade Options	1-65
Software Sources	1-67
Installation Disc	1-68
Hardware Configuration	1-69
Cisco Unified Communications Manager Basic Installation	1-70
Important Configuration Information	1-71
Installation Procedures for Basic Install (Using Installation DVD)	1-75
Basic Installation Flow (Installation DVD)	1-77
Installation Procedures for Basic Install (Preinstalled)	1-78
Basic Installation Flow (Preinstalled)	1-79
Cisco Unified Communications Manager Upgrade During Installation	1-80
Installation Procedures for Upgrade During Installation	1-81
Upgrade During Installation Flow	1-83
Upgrade During Installation (Retrieval Mechanism)	1-85
Upgrade During Installation (Remote Patch Access Information)	1-86
Upgrade During Installation (Patch Location)	1-87
Cisco Unified Communications Manager Windows Upgrade	1-88
Cisco DMA	1-89
Data Not Exported by Cisco DMA	1-90
Windows Upgrade Installation Option	1-91
Cisco Unified Communications Manager Upgrade	1-92
Dual Partitions	1-93
Installation Procedures for Cisco Unified Communications Manager Upgrade	1-94
Upgrade Process on Cisco Unified Communications Manager Releases 5.x and 6.x	1-95
Summary	1-96
References	1-96
Module Summary	1-97
References	1-97
Module Self-Check	1-98
Module Self-Check Answer Key	1-102
Administration of Cisco Unified Communications Manager	2-1
Overview	2-1
Module Objectives	2-1
Understanding Cisco Unified Communications Manager Administration Options	2-3
Overview	2-3
Objectives	2-3
Cisco Unified Communications Manager Administration and User Interfaces	2-4
Cisco Unified Communications Manager Administration and User Interface Functions	2-5
Cisco Unified Communications Manager User Web Interface	2-6
Accessing the User Web Interface	2-7
Cisco Unified Communications Manager User Main Page	2-8
Cisco Unified Communications Manager Administration Web Interface	2-9
Accessing the Administration Web Interface	2-10
Cisco Unified Communications Manager Administration Main Page	2-11
Cisco Unified Communications Manager Serviceability Web Interface	2-12
Accessing the Serviceability Web Interface	2-13

Cisco Unified Communications Manager Serviceability Main Page	2-14
Cisco Unified Communications Manager Disaster Recovery Web Interface	2-15
Accessing the Disaster Recovery Web Interface	2-16
Cisco Unified Communications Manager Disaster Recovery Main Page	2-17
Cisco Unified Communications Manager Operating System Web Interface	2-18
Accessing the Cisco Unified Communications Manager Operating System Web Interface	2-19
Cisco Unified Communications Manager Operating System Main Page	2-20
Cisco Unified Communications Manager Administration CLI	2-21
Accessing the Administration CLI	2-22
Cisco Unified Communications Manager Administration CLI Main Page	2-23
Summary	2-24
References	2-24
Managing Services and Initial Configuration of Cisco Unified Communications Manager	2-25
Overview	2-25
Objectives	2-25
Cisco Unified Communications Manager Initial Configuration	2-26
Cisco Unified Communications Manager Network Configuration Options	2-27
Network Components	2-28
Cisco Unified Communications Manager NTP and DHCP Considerations	2-29
Changing NTP Settings	2-31
DHCP Server Feature Support	2-32
Steps to Configure DHCP Phone Support	2-33
Step 1: Activate DHCP Monitor Service	2-34
Step 2: Configure the DHCP Server	2-35
Step 3: Configure the DHCP Subnet	2-36
DHCP Migration Considerations	2-37
DNS Reliance of IP Phones	2-38
SCCP Call Flow with DNS	2-39
SCCP Call Flow Without DNS	2-40
Removing DNS Reliance	2-41
Cisco Unified Communications Manager Network and Feature Services	2-42
Network Services	2-43
Feature Services	2-44
Service Activation	2-45
Service Activation Screenshot	2-46
Control Center Screenshot	2-47
Cisco Unified Communications Manager Enterprise Parameters	2-48
Example of Enterprise Parameters	2-49
Changing Enterprise Parameters	2-50
Enterprise Parameters Screenshot	2-51
Phone URL Enterprise Parameters	2-52
Cisco Unified Communications Manager Service Parameters	2-53
Example of Service Parameters	2-54
Changing Service Parameters	2-55
Service Parameter Configuration Screenshot	2-56
Cisco CallManager Service Parameter Screenshot	2-57
Summary	2-58
References	2-58
Managing User Accounts in Cisco Unified Communications Manager	2-59
Overview	2-59
Objectives	2-59
Cisco Unified Communications Manager User Accounts	2-60
Two Types of User Accounts in Cisco Unified Communications Manager	2-61
Data Associated with User Accounts	2-62
User Privileges	2-63
User Privilege Component Interaction	2-64
Roles and User Groups Example	2-65
User Management Options	2-67

LDAP	2-68
Cisco Unified Communications Manager End-User Data Location	2-69
Managing User Accounts Using the Administration GUI	2-71
Application User Configuration Page	2-72
End User Configuration Page	2-74
Roles	2-75
Role Configuration Page	2-76
User Groups	2-77
User Group Configuration Page: User Assignment	2-78
User Group Configuration Page: Role Assignment	2-79
Cisco Unified Communications Manager BAT	2-80
Cisco Unified Communications Manager BAT Characteristics	2-81
Bulk Administration Menu	2-82
Cisco Unified Communications Manager BAT Components	2-83
Bulk Provisioning Service	2-85
Managing User Accounts Using the Cisco Unified Communications Manager BAT	2-87
Step 1: Configuring Cisco Unified Communications Manager BAT User Template	2-88
Step 2: Creating the CSV Data Input File	2-89
Step 3: Uploading CSV Data Input Files	2-90
Step 4: Starting Cisco Unified Communications Manager BAT Job to Add Users	2-91
Step 5a: Job Status – List of Jobs	2-92
Step 5b: Verifying Job Status – Job Details	2-93
LDAP Overview	2-94
LDAP Directory Integration with Cisco Unified Communications Manager	2-95
LDAP Support in Cisco Unified Communications Manager	2-97
LDAP Integration: Synchronization	2-98
Cisco Unified Communications Manager LDAP Synchronization Data Storage	2-99
LDAP Integration: Authentication	2-100
Cisco Unified Communications Manager LDAP Authentication Data Storage	2-101
LDAP Integration Considerations	2-102
Using LDAP for User Provisioning	2-103
LDAP Synchronization – Data Attributes Imported by Cisco Unified Communications Manager	2-104
LDAP Attributes Mapping	2-105
Synchronization Agreements	2-106
User Search Bases	2-107
Synchronization Mechanism	2-109
LDAP Synchronization Best Practices	2-110
Integrating Microsoft Active Directory with Multiple Active Directory Domains	2-111
Integrating Microsoft Active Directory with Multiple Active Directory Trees	2-112
LDAP Synchronization Configuration Procedure	2-113
Step 2: Activate Cisco DirSync Service	2-114
Step 3: LDAP System Configuration	2-115
Step 4a: Adding LDAP Directory	2-116
Step 4b: LDAP Directory Configuration	2-117
LDAP Synchronization Verification	2-118
Using LDAP for User Authentication	2-120
LDAP Authentication – End Users, Application Users, and Extension Mobility	2-121
LDAP Authentication Best Practices	2-122
LDAP Authentication When Using Microsoft Active Directory with Multiple Domains or Trees	2-124
LDAP Authentication Configuration Procedure	2-126
Step 2: LDAP Authentication Configuration	2-127
LDAP Authentication Verification	2-128
Summary	2-129
References	2-129
Module Summary	2-130
References	2-130
Module Self-Check	2-132
Module Self-Check Answer Key	2-136

Single-Site On-Net Calling	3-1
Overview	3-1
Module Objectives	3-1
Understanding Endpoints in Cisco Unified Communications Manager	3-3
Overview	3-3
Objectives	3-3
Cisco Unified Communications Manager Endpoints	3-4
Cisco Unified Communications Manager Endpoint Support	3-5
Cisco Unified Communications Manager Endpoint Feature Support	3-6
Cisco Unified Communications Manager Telephony Feature Support by Protocol and Type of Endpoint	3-7
Cisco IP Phone Model Differences	3-8
Entry-Level Cisco IP Phones	3-9
Midrange Cisco IP Phones	3-10
Upper-End Cisco IP Phones	3-11
Other Cisco IP Phones	3-12
Special Functions Used By Cisco IP Phones	3-14
Cisco IP Phones Boot Sequence	3-16
Boot Sequence Differences Between Cisco SCCP and SIP Phones	3-19
Cisco SIP Phone Startup Process	3-20
H.323 Endpoint Support in Cisco Unified Communications Manager	3-22
H.323 Endpoints	3-23
Features Not Supported for H.323 Endpoints	3-24
H.323 Phone Configuration Requirements	3-25
SIP Third-Party IP Phone Support in Cisco Unified Communications Manager	3-26
Third-Party SIP Phones	3-28
Features Not Supported for Third-Party SIP Endpoints	3-29
SIP Digest Authentication	3-30
Third-Party SIP Phone Registration Process Using Digest Authentication	3-31
Third-Party SIP Phone Configuration Requirements	3-33
Summary	3-34
References	3-34
Configuring Cisco Catalyst Switches for Endpoints	3-37
Overview	3-37
Objectives	3-37
Cisco LAN Switch Essentials	3-38
Applying Switch Features	3-39
Cisco Catalyst Family of Switches	3-40
Providing Power to IP Phones	3-42
Two Types of PoE Delivery	3-43
Cisco Prestandard Device Detection	3-45
IEEE 802.3af Device Detection	3-46
Configuring Cisco LAN Switches to Provide Power to IP Phones	3-47
Cisco Catalyst Switch: Show Inline Power Status	3-48
Voice VLAN Support in Cisco IOS LAN Switches	3-49
Voice VLAN Support	3-51
Single VLAN Access Port	3-52
Multi-VLAN Access Port	3-53
Trunk Ports	3-55
Limiting VLANs on Trunk Ports	3-56
Limiting VLANs on Trunk Ports at the Switch	3-57
Configuring Voice VLANs in Cisco IOS LAN Switches	3-58
Configuring Trunk Port Using Native Cisco IOS Software	3-60
Verifying Voice VLAN Configuration Using Native Cisco IOS Software	3-61
Configuring Voice VLANs in Cisco Catalyst Operating System LAN Switches	3-62
Configuring Trunk Ports Using Cisco Catalyst Operating System	3-63
Verifying Voice VLAN Configuration Using Cisco Catalyst Operating System	3-64
Summary	3-65

References	3-65
Implementing and Hardening IP Phones	3-67
Overview	3-67
Objectives	3-67
Examining Endpoint Configuration Tools and Elements	3-68
Endpoint Basic Configuration Elements	3-70
Phone NTP Reference	3-71
Date/Time Group Configuration	3-73
Device Pools	3-75
Cisco Unified CM Group	3-77
Regions	3-78
Locations	3-79
Phone Security Profile	3-80
Device Settings	3-81
Device Defaults Configuration	3-82
Phone Button Template	3-83
Softkey Template	3-84
SIP Profile	3-85
Common Phone Profile	3-86
Relationship Between Phone Configuration Elements	3-87
IP Phone Autoregistration	3-88
Autoregistration Process	3-89
Considerations for Autoregistration	3-91
Configuring Autoregistration	3-92
Step 1: Assigning the Default Autoregistration Protocol	3-93
Step 2: Cisco Unified CM Group Configuration	3-94
Step 3: Cisco Unified CM Configuration	3-95
Cisco Unified Communications Manager BAT and Auto-Register Phone Tool	3-96
Cisco Unified Communications Manager Auto-Register Phone Tool	3-97
Cisco Unified Communications Manager Auto-Register Phone Tool Requirements	3-98
Process of Adding IP Phones Using the Cisco Unified Communications Manager Auto-Register Phone Tool	3-99
Using Cisco Unified Communications Manager BAT for Adding Phones to Cisco Unified Communications Manager	3-101
Step 2: Configuring Cisco Unified Communications Manager Phone Template	3-102
Step 3: Uploading CSV Files	3-105
Step 4: Validating Phones Configuration	3-106
Step 5: Inserting IP Phones into Cisco Unified Communications Manager Database	3-107
Manually Adding Phones to Cisco Unified Communications Manager	3-109
Step 1: Adding an IP Phone	3-110
Step 2: Phone Configuration	3-111
Step 3: Directory Number Configuration	3-112
Verify Endpoint Configuration	3-113
Third-Party SIP Phone Configuration Steps	3-115
Steps 1 to 3: Third-Party SIP Phone Configuration in Cisco Unified Communications Manager	3-116
Step 4: Third-Party SIP Phone Configuration	3-117
Hardening Cisco IP Phones	3-118
Disabling PC Port and Settings Access	3-119
Disabling IP Phone Web Service	3-120
Disabling GARP	3-121
GARP Attack	3-122
Disabling Voice VLAN Access	3-123
Blocking PC VLAN Access On Cisco IP Phones	3-124
Summary	3-125
References	3-125
Module Summary	3-125
References	3-125
Module Self-Check	3-127
Module Self-Check Answer Key	3-131

Course Introduction

Overview

Implementing Cisco Unified Communications IP Telephony Part 1 (CIPT1) v6.0 prepares you for installing and configuring a Cisco Unified Communications Manager solution at a single site. This course focuses primarily on Cisco Unified Communications Manager Release 6.0, which is the call routing and signaling component for the Cisco Unified Communications solution.

This course includes lab activities in which you will perform post-installation tasks, configure Cisco Unified Communications Manager and switches, implement Media Gateway Control Protocol (MGCP) gateways, and build dial plans to place on-net and off-net phone calls. You will also implement media resources, Lightweight Directory Access Protocol (LDAP), voice mail integration, and numerous user telephone features.

Learner Skills and Knowledge

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

Learner Skills and Knowledge

- Working knowledge of fundamental terms and concepts of computer networking, to include LANs, WANs, and IP switching and routing
- Ability to configure and operate Cisco routers and switches and to enable VLANs and DHCP
- Fundamental knowledge of converged voice and data networks
- Working knowledge of the MGCP and its implementation on Cisco IOS gateways

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3

Learner Skills and Knowledge (Cont.)

- Cisco learning offerings:
 - Interconnecting Cisco Network Devices 1 (ICND1) v1.0
 - Cisco CCNA® certification recommended prerequisite
 - Building Cisco Multilayer Switched Networks (BCMSN) v3.0
 - Cisco Voice Over IP (CVOICE) v6.0

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4

Course Goal and Objectives

This topic describes the course goal and objectives.

“To provide learners with the necessary knowledge and skills to install and configure a Cisco IP Telephony solution based on Cisco Unified Communications Manager Release 6.0, the call-routing and signaling component of the Cisco IP Telephony solution, in a single site.”

Implementing Cisco Unified Communications IP Telephony Part 1

© 2008 Cisco Systems, Inc. All rights reserved.

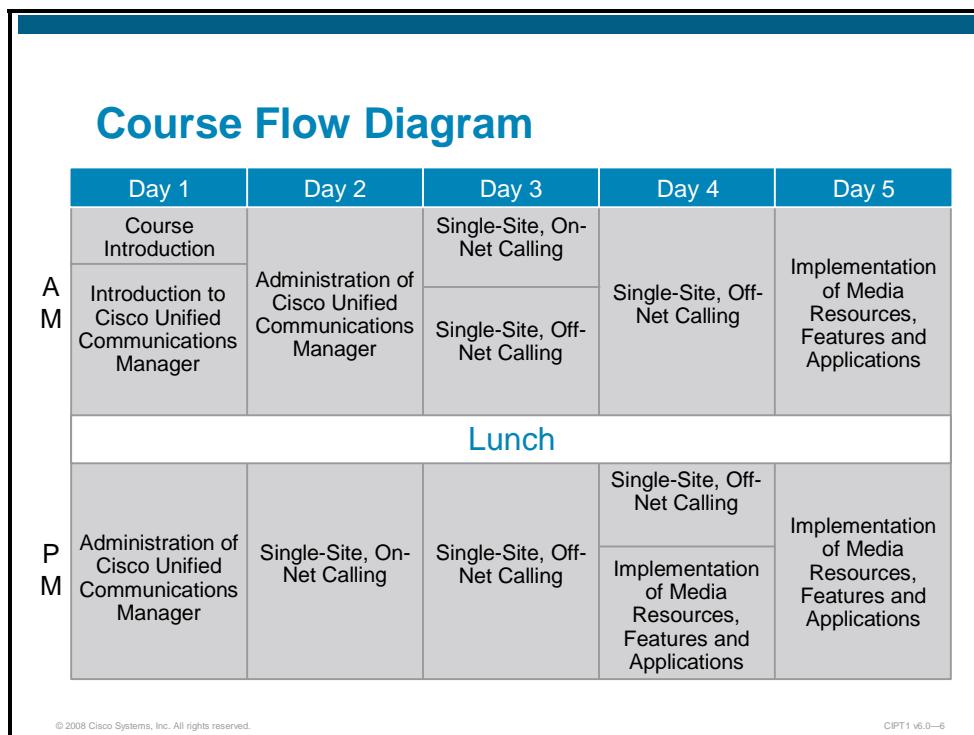
CIPT1 v6.0—5

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

- Describe Cisco Unified Communications Manager, including its functions, architecture, deployment and redundancy options, and how to install or upgrade
- Perform Cisco Unified Communications Manager platform and general administration, initial configuration, and user management
- Configure Cisco Unified Communications Manager to support on-cluster calling in a single-site deployment
- Implement a dial plan in Cisco Unified Communications Manager to make internal calls and place calls to the PSTN
- Configure Cisco Unified Communications Manager media resources, features, and voice-mail integration

Course Flow

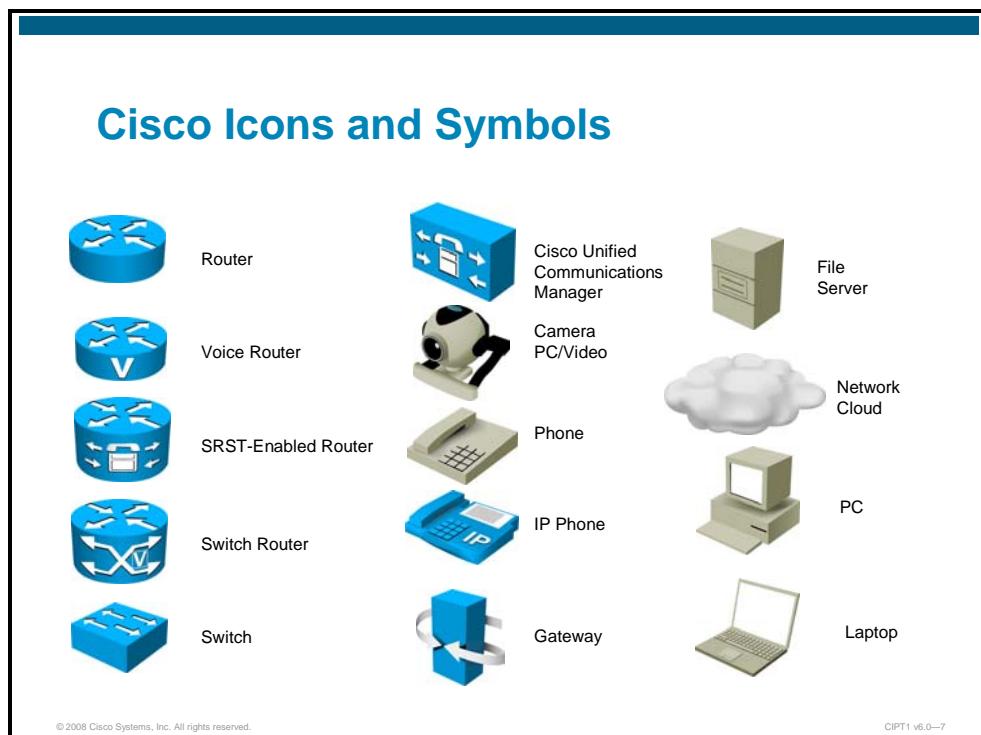
This topic presents the suggested flow of the course materials.



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 lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

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



Cisco Glossary of Terms

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

Your Training Curriculum

This topic presents the training curriculum for this course.

Cisco Certifications



www.cisco.com/go/certifications

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—8

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

Cisco Career Certifications: CCVP

Expand Your Professional Options
and Advance Your Career

Professional-level recognition in IP Telephony (VoIP)



- Recommended Training Through Cisco Learning Partners
- Quality of Service
- Cisco Voice over IP
- Troubleshooting Cisco Unified Communications Systems or IP Telephony Troubleshooting
- Implementing Cisco Unified Communications Manager Part 1
- Implementing Cisco Unified Communications Manager Part 2

www.cisco.com/go/certifications

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—9

Module 1

Introduction to Cisco Unified Communications Manager

Overview

Cisco Unified Communications Manager is the software-based, call-processing component of the Cisco Unified Communications solution.

This module describes the characteristics of Cisco Unified Communications Manager, explores the available deployment models for using Cisco Unified Communications Manager in a Cisco Unified Communications solution, and explains the Cisco Unified Communications Manager installation process and licensing model.

Module Objectives

Upon completing this module, you will be able to describe Cisco Unified Communications Manager, including its functions, architecture, deployment and redundancy options, and how to install or upgrade. This ability includes being able to meet these objectives:

- Describe Cisco Unified Communications Manager requirements for hardware, operating system, database, communication, and licensing
- Describe Cisco Unified Communications Manager deployment options and redundancy designs
- Describe how to install or upgrade Cisco Unified Communications Manager

Lesson 1

Understanding Cisco Unified Communications Manager Architecture

Overview

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

This lesson introduces the Cisco Unified Communications solution and describes the Cisco Unified Communications Manager role, architecture and characteristics, hardware and software requirements, and the licensing model of the Cisco Unified Communications Manager.

Objectives

Upon completing this lesson, you will understand Cisco Unified Communications Manager architecture. This ability includes being able to meet these objectives:

- Describe the components of a Cisco Unified Communications solution and each component's functionality
- Describe the architecture and role of Cisco Unified Communications Manager
- Describe the hardware requirements for Cisco Unified Communications Manager Release 6.0
- Describe the characteristics of the Cisco Unified Communications Operating System
- Describe the characteristics of the Cisco Unified Communications Manager database and how it provides redundancy
- Describe the licensing model of Cisco Unified Communications Manager
- Describe how to calculate, verify, and add license units to Cisco Unified Communications Manager

Cisco Unified Communications

This topic provides an overview of Cisco Unified Communications.

Cisco Unified Communications Architecture

- IP telephony
- Customer contact center
- Video telephony
- Rich-media conferencing
- Third-party applications

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-4

The Cisco Unified Communications system fully integrates communications by enabling data, voice, and video to be transmitted over a single network infrastructure using standards-based IP. Leveraging the framework provided by Cisco IP hardware and software products, the Cisco Unified Communications system has the capability to address current and emerging communications needs in the enterprise environment. The Cisco Unified Communications family of products is designed to optimize feature functionality, reduce configuration and maintenance requirements, and provide interoperability with a wide variety of other applications. The Cisco Unified Communications system provides and maintains a high level of availability, quality of service (QoS), and security for the network.

The Cisco Unified Communications system incorporates and integrates the following communications technologies:

- **IP telephony:** IP telephony refers to technology that transmits voice communications over a network using IP standards. Cisco Unified Communications includes hardware and software products, such as call-processing agents, IP phones (both wired and wireless), voice-messaging systems, video devices, and many special applications.
- **Customer contact center:** Cisco IP Contact Center products are a combined strategy with architecture to enable efficient and effective customer communications across a globally capable network. This strategy allows organizations to draw from a broader range of resources to service customers. They include access to a large pool of agents and multiple channels of communication, as well as customer self-help tools.

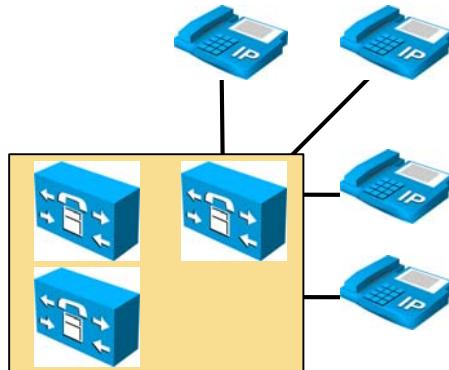
- **Video telephony:** The Cisco Unified Video Advantage products enable real-time video communications and collaboration using the same IP network and call-processing agent as Cisco Unified Communications. With Cisco Unified Video Advantage, making a video call is just as easy as dialing a phone number.
- **Rich-media conferencing:** Cisco Conference Connection and Cisco Unified MeetingPlace enhance the virtual meeting environment with an integrated set of IP-based tools for voice, video, and web conferencing.
- **Third-party applications:** Cisco works with leading-edge companies to provide a broad selection of third-party IP communications applications and products. This collaboration helps businesses focus on critical needs such as messaging, customer care, and workforce optimization.

Cisco Unified Communications Manager

This topic describes the functions that are provided by Cisco Unified Communications Manager.

Cisco Unified Communications Manager Functions

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Programming interface to external applications
- Includes a backup-and-restore tool (disaster recovery system)



© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—1-6

Cisco Unified Communications Manager extends enterprise telephony features and functions to packet telephony network devices. These packet telephony network devices include Cisco 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 Cisco Unified Communications Manager application programming interface (API).

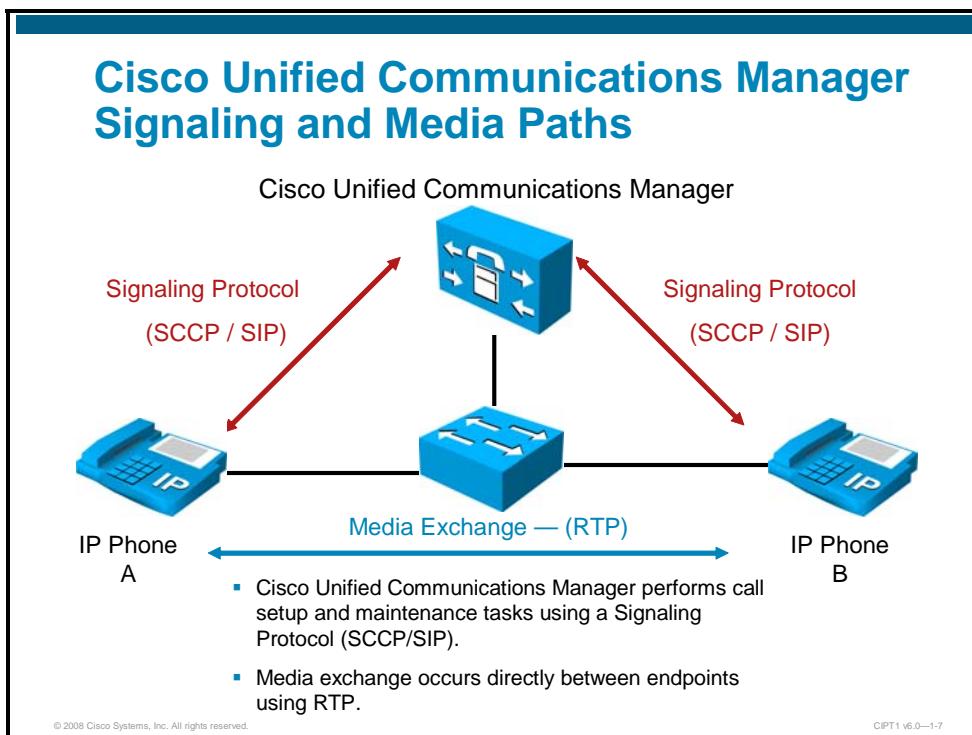
Cisco Unified Communications Manager provides these functions:

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

- **Directory services:** Cisco Unified Communications Manager uses its own database to store user information. You can authenticate users either locally or against an external directory. You can provision users by directory synchronization. With directory synchronization, you can automatically add users from the directory to the local database. Microsoft Active Directory (2000 and 2003), Netscape 4.x, iPlanet 5.1, and Sun ONE 5.2 are supported.
- **Programming interface to external applications:** Cisco Unified Communications Manager provides a programming interface to external applications such as Cisco IP SoftPhone, Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IVR), Cisco Personal Assistant, and Cisco Unified Communications Manager Attendant Console.
- **Backup and restore tools:** Cisco Unified Communications Manager provides the Disaster Recovery System (DRS) tools to provide a means of backing up and restoring the Cisco Unified Communications Manager configuration database, as well as the Call Detail Records (CDR) and the Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) database.

Cisco Unified Communications Manager Signaling and Media Paths

You can better understand how Cisco Unified Communications Manager performs key functions by tracking the signaling and media path of a basic IP telephony call.



Cisco Unified Communications Manager uses the session initiation protocol (SIP) or the Skinny Client Control Protocol (SCCP) to communicate with Cisco IP phones for call setup and maintenance tasks.

When the call is set up, media exchange occurs directly between the Cisco IP phones using Real-Time Transport Protocol (RTP) to carry the audio.

Example: Basic IP Telephony Call

In the figure, User A on Phone A (left telephone) wants to make a call to Phone B (right telephone). User A picks up the handset and dials the number of User B. In this environment, dialed digits are sent to Cisco Unified Communications Manager, the call-processing engine. Cisco Unified Communications Manager finds the address and determines where to route the call.

Using the SCCP or SIP protocol, Cisco Unified Communications Manager signals the calling party over IP to initiate a ringback, and Party A hears the ringback tone. Cisco Unified Communications Manager also signals the call to the destination phone, which starts ringing.

When User B accepts the call, the RTP media path opens between the two stations. User A or User B may now initiate a conversation.

The Cisco IP phones require no further communication with Cisco Unified Communications Manager until either User A or User B invokes a feature, such as call transfer, call conferencing, or call termination.

Cisco Unified Communications Manager Hardware, Software, and Clustering

This topic describes the Cisco Unified Communications Manager hardware, software, and clustering.

Cisco Unified Communications Manager Hardware, Software, and Clustering

- Complete hardware and software solution (appliance model)
 - Factory-installed and field-configured
 - Can be installed on Cisco 7800 MCS server platform or on approved third-party servers from IBM and HP
 - No customer access to operating system
 - Only GUI and CLI access to appliance system
 - Third-party access via documented APIs only
 - Supports clusters for redundancy and load sharing
 - Provides database redundancy by sharing a common database
 - Provides call-processing redundancy by Cisco Unified Communications Manager groups
 - Cluster includes the following:
 - One publisher
 - Total maximum of 20 servers (“nodes”) running various services, including TFTP, media resources, conferencing, and call processing
 - Maximum of eight nodes can be used for call processing (running the Cisco Unified Communications Manager service)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-8

Cisco Unified Communications Manager Release 6.0 is a complete hardware and software solution that works as an appliance. The appliance is essentially a closed system that supports only applications and utilities authorized by Cisco. Key goals of the appliance model are to simplify the installation and upgrade of the system and to hide the underlying operating system and its tools. An appliance-based model makes it possible for an administrator to install, implement, and manage a Cisco Unified Communications Manager server without requiring knowledge or having access to the underlying operating system.

The Cisco Unified Communications Manager appliance has these features:

- Complete hardware and software solution
 - Cisco Unified Communications Manager servers are preinstalled with all software that is required to operate, maintain, secure, and manage a server or cluster of servers (including Cisco Security Agent).
 - Can also be field-installed on supported Cisco Media Convergence Servers (MCSs) or third-party server platforms approved by Cisco.
- Appliance operating system improves installation and upgrade and increases security and reliability
 - You can upgrade Cisco Unified Communications Manager servers while they continue to process calls.

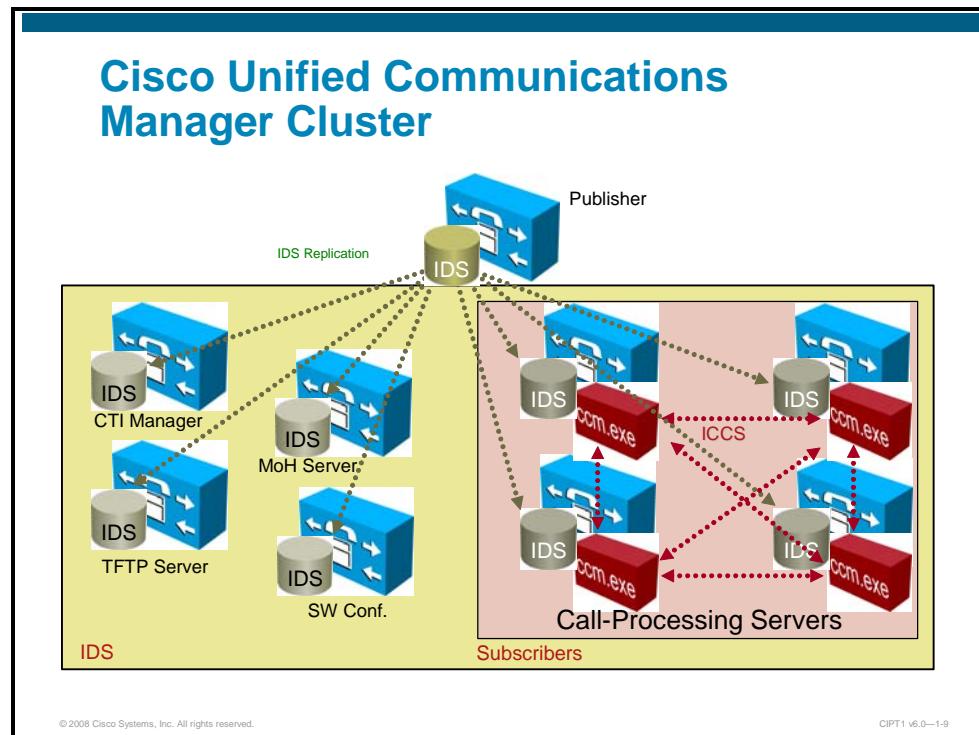
- Interfaces provide access to the system via either command-line interface (CLI) and GUI for administration purposes or through documented APIs for third-party access
 - Outputs a variety of management parameters via a published interface to provide information to approved management applications such as, but not limited to, NetIQ Vivinet Manager, HP OpenView, and Integrated Research PROGNOSIS.
- Operates in a headless manner (without keyboard, mouse, or video graphics array (VGA) monitor support) or, in the case of some of the hardware platforms, in a headed manner (with keyboard, mouse, and monitor)
- Third-party access via documented APIs only

The Cisco Unified Communications Manager appliance supports clusters for redundancy and load sharing. Database redundancy is provided by sharing a common database, whereas call-processing redundancy is provided by Cisco Unified Communications Manager groups:

- A cluster consists of one publisher and a total maximum of 20 servers (nodes) running various services, including TFTP, media resources, conferencing, and call processing.
- You can have up to a maximum of eight nodes for call processing (running the Cisco CallManager service).

Cisco Unified Communications Manager Cluster

This section describes database operation in Cisco Unified Communications Manager Release 6.0.



The Cisco Unified Communications Manager service provides call routing, signaling, and media control for an IP telephony enterprise deployment.

A cluster is a set of networked services that work together to provide the Cisco Unified Communications Manager service in addition to dedicated servers providing database, application, TFTP, and media services such as conferencing and music on hold (MOH). These services can be provided by the subscribers and the publisher and can be shared by all servers.

Clustering provides several benefits. It allows the network to scale to several thousands of endpoints, provides redundancy in case of network or server failures, and provides a central point of administration.

In order to process calls correctly, Cisco Unified Communications Manager needs to retrieve configuration settings for all devices. These settings are stored in a database using IBM Informix Dynamic Server (IDS). The database is the repository for information such as service parameters, features, device configurations, and the dial plan.

Cisco Unified Communications Manager Clustering

The database replicates nearly all information in a star topology (one publisher, many subscribers). However, Cisco Unified Communications Manager nodes also use a second communication method to replicate run-time data in a mesh topology (every node updates every other node). This type of communication is used for dynamic information that changes more frequently than database changes. The primary use of this replication is to communicate newly registered phones, gateways, and digital signal processor (DSP) resources, so that optimum routing of calls between members of the cluster and the associated gateways occurs.

Cisco Unified Communications Manager Hardware Requirements

This topic describes the hardware requirements for the Cisco Unified Communications Manager Release 6.0.

Cisco 7800 Series MCS

- Cisco Unified Communications Manager Release 6.0 can be installed on the Cisco 7800 MCS server platforms that are available from Cisco.
- Cisco 7800 MCS server platforms:
 - 7816 Series
 - 7825 Series
 - 7835 Series
 - 7845 Series
- Minimum hardware requirements for Cisco Unified Communications Manager Release 6.0:
 - 2 GHz processor
 - 2 GB RAM
 - 72 GB hard disk
- For detailed model information, check Cisco Unified Communications Manager Server Support Matrix
 - http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure0900aecd8062a4f9.html

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-11

These are the minimum hardware requirements for Cisco Unified Communications Manager Release 6.0:

- 2 GHz processor
- 2 GB RAM
- 72 GB hard disk

Minimum requirements remain the same as for Cisco Unified CallManager Release 5.0, but only specific Cisco MCS models are approved.

Note	Cisco Unified Communications Manager Server Support Matrix and hardware specifications can be found at the following URL: http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure0900aecd8062a4f9.html
-------------	--

Third-Party Hardware Solutions Approved by Cisco

Cisco Unified Communications Manager Release 6.0 can also be installed on third-party hardware platforms that are approved by Cisco.

Third-Party Hardware Solutions Approved by Cisco

Cisco Unified Communications Manager Release 6.0 can also be installed on the following third-party hardware platforms approved by Cisco:

- HP Server Solutions
 - http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/product_solution_overview09186a0080107d79.html
- IBM Server Solutions
 - http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure0900aecd80091615.html

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-12

Because voice networks should maintain a high uptime, Cisco Unified Communications Manager must be installed on a server that meets Cisco configuration standards. For this reason, Cisco has collaborated with two server hardware manufacturers, Hewlett-Packard and IBM, who designed these server hardware platforms specifically for Cisco voice applications.

The following URLs provide a list of the IBM and HP hardware platforms that are approved by Cisco:

IBM Server Solutions -

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure0900aecd80091615.html

HP Server Solutions -

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/product_solution_overview09186a0080107d79.html

Cisco Unified Communications Operating System

This topic describes the Cisco Unified Communications operating system.

Cisco Unified Communications Operating System

- Appliance operating system (based on Red Hat Linux)
- Operating system updates provided by Cisco (along with application updates)
- Unnecessary accounts and services disabled
- IDS as the database
- DHCP server
- Cisco Security Agent
- Cisco Unified Communications operating system is also used for these other Cisco Unified Communications applications:
 - Cisco Emergency Responder 2.0
 - Cisco Unity Connection 2.0
 - Cisco Unified Presence 6.0

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-14

Cisco Unified Communications operating system is an appliance operating system (based on Red Hat Linux). Operating system updates are provided by Cisco (along with application updates) through patches that are signed by Cisco. Unsupported software and applications (not signed by Cisco) cannot be uploaded or installed into the appliance.

Root access to the file system is not permitted, and all unnecessary accounts and services have been disabled in the appliance operating system.

IBM IDS is installed as the database for the Cisco Unified Communications applications.

Cisco Security Agent, a host intrusion-prevention system, is also built into the appliance to provide protection against known and unknown attacks.

A DHCP server is integrated into Cisco Unified Communications Manager to provide DHCP services to IP phones.

Cisco Unified Communications operating system is also used for these other Cisco Unified Communications applications:

- Cisco Emergency Responder 2.0
- Unity Connection 2.0
- Cisco Unified Presence 6.0

Cisco Unified Communications Operating System Access

Several points must be considered when attempting to access the appliance operating system.

Cisco Unified Communications Operating System Access

- Root and other common default accounts of native operating system disabled.
- No native operating system access.
 - Only Cisco CLI and GUI can be used.
 - Cisco CLI can be used to troubleshoot GUI access.
- No access to native operating system debug interfaces.
 - Traces, alarms, and counters can be enabled and monitored through Cisco CLI and GUI.
- No direct access to file system.
 - Only some files and directories accessible through Cisco CLI and GUI.
- Customer can activate remote account support for specific time for Cisco TAC access.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-15

Cisco Unified Communications operating system is a hardened operating system. The root and other common but unnecessary default accounts of the native operating system have been disabled.

There is no possibility to access the native operating system directly or to install any unsupported applications or software. Access to the platform and upgrading of patches can only be done through the Cisco CLI and GUI.

There is also no access to native operating system debug interfaces; however, traces, alarms, and performance counters can be enabled and monitored through the Cisco CLI and GUI.

There is no direct access to the file system; only some files and directories are accessible through the Cisco CLI and GUI for maintenance purposes.

To require support from Cisco, activate remote account support for a specific time for remote Cisco Technical Assistance Center (TAC) access.

Cisco Unified Communications Manager Database

This topic describes the Cisco Unified Communications Manager IDS database.

Cisco Unified Communications Database

- IBM IDS database stores
 - Static configuration data:
 - Servers and enabled services within the cluster
 - Devices (phones, gateways, and trunks)
 - Users, dial plan, etc.
 - Dynamic data utilized by user-facing features:
 - Call Forward All, MWI
 - Privacy, DND
 - Hunt group login status, etc.
- Basically a single master database model
 - R/W database access only for publisher (read-only for subscribers)
 - Exception: Subscribers do allow R/W access for user-facing features

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-17

The data in the Cisco Unified Communications Manager database is divided into two types.

Static configuration data are created or modified as part of the configuration of the Cisco Unified Communications Manager cluster. Read/write access to this data is provided for the publisher only. Subscribers will provide only read-only access to this data. If the publisher is not available, this data cannot be modified. Replication of the data is from the publisher to the subscribers.

Dynamic user-facing features data are created or modified when certain user features are modified by the user or by an application feature. Read/write access to this data is provided on all servers. This data can be modified even if the publisher is unavailable. User-facing features data can be replicated from the server where the change was initiated to all other servers within the Cisco Unified Communications Manager cluster.

Examples for user-facing features are:

- Call Forward All (CFA)
- Message Waiting Indicator (MWI)
- Privacy enable/disable
- Do Not Disturb (DND) enable/disable
- Extension Mobility (EM) login
- Hunt-group login status

Services That Rely on the Publisher

In order to understand the results of a failure of the publisher, you must identify the services that rely on the publisher.

Services That Rely On The Publisher

Component	Function	When
CCMAdmin	Provisions everything	Always
CCMUser	Provisions user settings	Always
BAT	Provisions everything	Always
TAPS	Updates device records	Always
AXL	Provisions everything	Always
AXIS-SOAP	Enables and disables services	Sometimes
CCM	Inserts phones	Autoregistration only
LDAP Sync	Updates End-user table	Always (local)
License Audit	Updates License tables	Always (local)

These services are not available in the event of a publisher failure.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-18

Services that use the publisher will be affected in the event of a publisher failure. These are mainly services that provide configuration changes to the Cisco Unified Communications Manager cluster. The replication of these data will always be initiated from the publisher to the subscribers. The figure shows the list of services that rely on the publisher.

User-Facing Features

User-facing features are independent of the publisher, as their data can be written to subscribers.

User-Facing Features

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy Enable/Disable
- Do Not Disturb Enable/Disable (DND)
- Extension Mobility Login (EM)
- Hunt Group Logout
- Device Mobility
- CTI CAPF status for end users and application users
- Credential hacking and authentication

These features do not rely on the availability of the publisher because necessary data can be written to subscribers.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-19

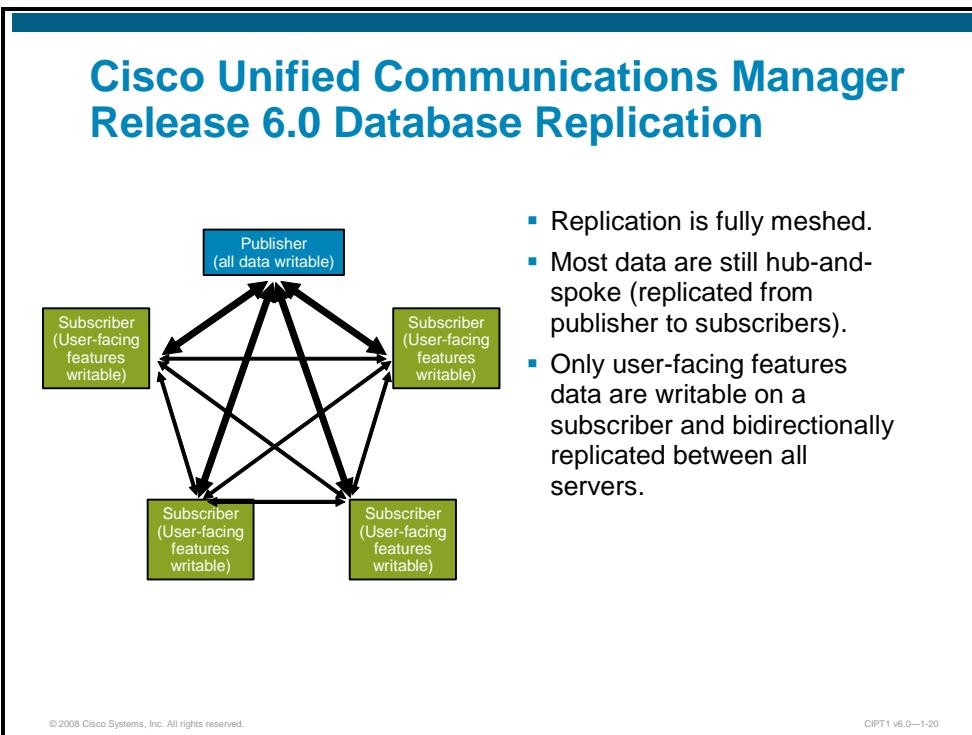
The user-facing features listed in the figure do not rely on the availability of the publisher, as these dynamic user-facing features data can be written to the subscribers to which the device is registered. These data are then replicated to all other servers within the cluster.

By allowing the data to be written to the subscriber, the user-facing features can continue to function in the event of a publisher failure. This functionality has been introduced with Cisco Unified Communications Manager Release 6.0. In all earlier versions, these user-facing features did not work during publisher failure.

Computer telephony integration (CTI) Certificate Authority Proxy Function (CAPF) status for end users and application users is one of the user-facing features.

Cisco Unified Communications Manager Release 6.0 Database Replication

This section describes the Cisco Unified Communications Manager Release 6.0 database replication.

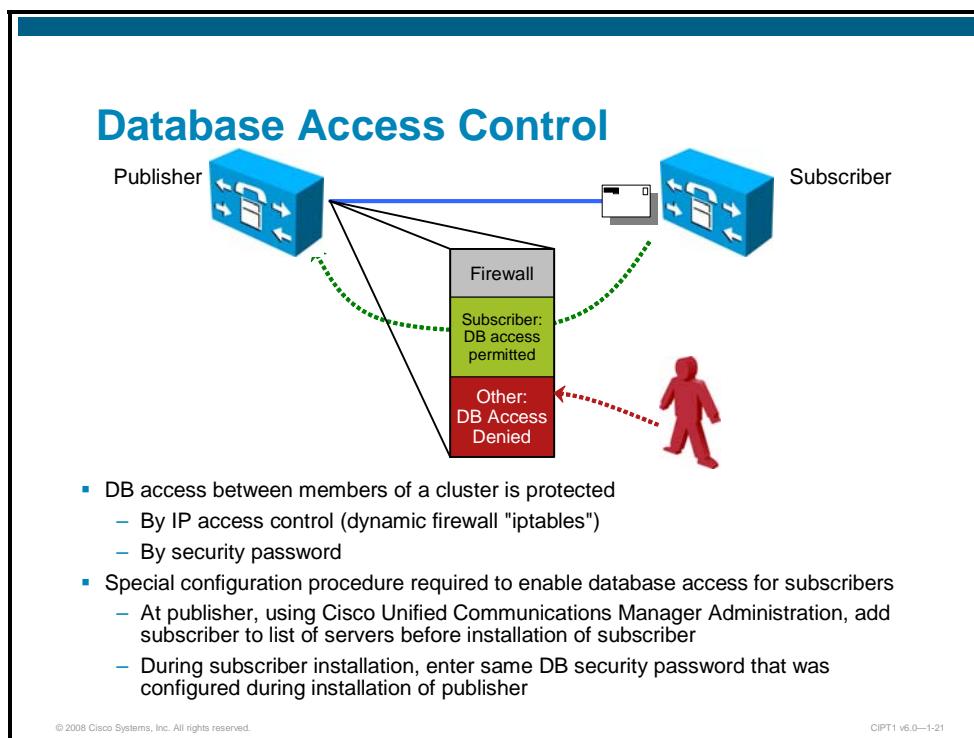


Replication is now fully meshed between all servers within a cluster. However, only user-facing features data (for example, Cisco Unified Communications Manager Extension Mobility features) are writeable on a subscriber and are replicated from an updated subscriber to all other servers. All non-user-facing features data can be written only to the publisher database and will get replicated from the publisher to all subscribers.

Therefore, most data (all non-user-facing features data) is still replicated in hub-and-spoke style (publisher to subscribers), while user-facing features data is replicated bidirectional between all servers.

Database Access Control

In Cisco Unified Communications Manager Release 6.0, access to the IBM Informix Dynamic Server (IDS) database is secured by two different methods.



The first method is IP access control using “iptables” (dynamic firewall), and the second method is the use of a database security password.

The procedure to allow new subscribers to access the database on the publisher is as follows:

- Add the subscriber to the publisher database using Cisco Unified Communications Manager Administration.
- During installation of the subscriber, enter the same database security password that was entered during installation of the publisher.

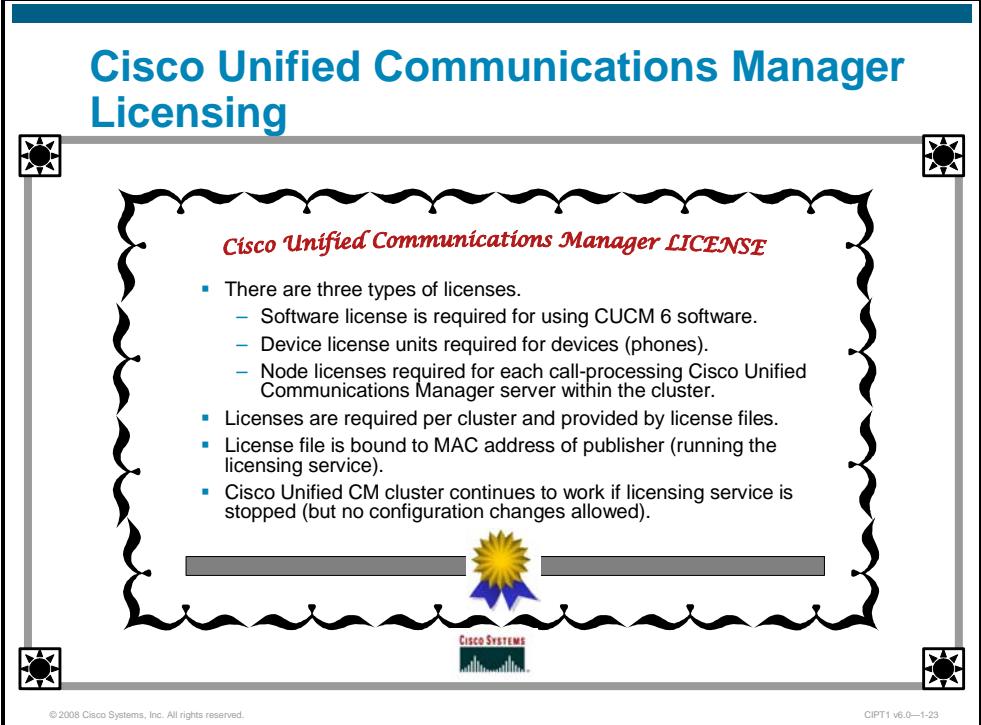
After this configuration, the following process occurs in order to replicate the database from the publisher to the newly added subscriber:

- The subscriber attempts to establish a connection to the publisher database using the database management channel.
- The publisher verifies the subscriber’s authenticity and adds the subscriber’s IP address to its dynamic firewall (iptables).
- The subscriber is allowed to access the publisher database.
- The database content is replicated from the publisher to the subscriber.

Note	Cisco Unified Communications Manager Release 6.0 TCP and UDP port usage (including ports used for database traffic) can be found at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/6_0/60plrev1.pdf .
-------------	--

Cisco Unified Communications Manager Licensing Model

This topic provides an overview of the Cisco Unified Communications Manager licensing model.



The slide has a decorative border with four sun icons at the corners and a wavy pattern along the inner edges. The title 'Cisco Unified Communications Manager Licensing' is at the top in blue. Below it is a red section header 'Cisco Unified Communications Manager LICENSE'. The main content is a bulleted list:

- There are three types of licenses.
 - Software license is required for using CUCM 6 software.
 - Device license units required for devices (phones).
 - Node licenses required for each call-processing Cisco Unified Communications Manager server within the cluster.
- Licenses are required per cluster and provided by license files.
- License file is bound to MAC address of publisher (running the licensing service).
- Cisco Unified CM cluster continues to work if licensing service is stopped (but no configuration changes allowed).

At the bottom center is the Cisco Systems logo, which includes a stylized sun icon above the text 'CISCO SYSTEMS'.

Licensing is implemented in Cisco Unified Communications Manager Administration to accurately track the number of devices that are registered to the Cisco Unified Communications Manager, including third-party SIP phones, and compare that number with the number of license units that have been purchased. License enforcement occurs at the time of phone provisioning and Cisco Unified Communications Manager service activation.

The publisher is the only licensing server. The licensing server is the logical component that keeps track of the licenses purchased and the licenses used. If the publisher fails, no new phones can register, and no configuration changes will be allowed; however, existing phones still operate.

Cisco Unified Communications Manager tracks the license compliance for devices, applications, and software.

- Device units licenses
 - The maximum number of provisioned devices in Cisco Unified Communications Manager database will be tracked and enforced.
 - Route points and CTI ports are not enforced.
- Application licenses
 - The Cisco Unified Communications Manager software will be tied to the MAC address of the publisher.
 - Application licenses are required for every call-processing server (that is, servers running the Cisco CallManager service).

- Software licenses

- Software license is tied to the major version of the software.
- Software licenses will be required for upgrade to Cisco Unified Communications Manager Release 6.0.

Licenses are created and distributed in accordance with the Cisco FlexLM process.

Device License Units

Device licenses are sold in device license units.

Device License Units

- Amount of device license units depends on device type and device capabilities.
 - Cisco phone or third-party phone
 - Number of lines
 - Video capabilities
 - Etc.
- Number of units required per device can be viewed from Cisco Unified Communications Manager Administration.

Type of Licensed Device	Units Consumed per Device
Cisco 7902	1
Cisco ATA 186	2
Cisco 7905	2
Cisco 7910	2
Cisco 7912	3
Cisco 7935	3
Cisco 7936	3
Cisco IP Communicator	3
Cisco 7920	4
Cisco 7940	4
Cisco 7941	4
Cisco 7960	4
Cisco 7961	4
Cisco 7970	5
Cisco 7971	5
Cisco 7941G-GE	4
Cisco 7961G-GE	4

Device License Units

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-24

These two types of product IDs are available:

- Cisco device license units
- Third-party device license units

The Cisco units are for Cisco devices only. The third-party units can be converted to Cisco units, but not vice versa.

Cisco Unified Communications Manager tracks the number of units required by each device, as shown in the figure. Each device type corresponds to a fixed number of units.

Amount of device license units depends on device type and device capabilities:

- Cisco phone or third-party phone
- Number of lines
- Video capabilities, and so on

Number of units required per device can be viewed from Cisco Unified Communications Manager Administration. Device license units are perpetual and device-independent.

License File Specifics

The license file contains information specific to the customer.

License File Specifics

- The license file contains the following information:
 - MAC address of the license server (publisher)
 - Version (major release) of the Cisco Unified Communications Manager software
 - Number of node licenses
 - Number of device license units
- License files are additive (multiple license files can be loaded).
- Cisco FlexLM process is used to obtain licenses.
- License file integrity is assured by a digital signature.
- Upgrade considerations
 - From Cisco Unified CallManager Release 4.x
 - An interim license file is created during upgrade.
 - No changes possible until replaced by real license file.
 - From Unified Cisco Unified CallManager Release 5.x
 - A software license has to be added (Cisco Unified CM 5.x only required node licenses and device license units).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-25

The main components of the license file are:

- MAC address of the license server (publisher)
- Version (major release) of the Cisco Unified Communications Manager software
- Number of node licenses
- Number of device license units

License files are additive (multiple license files can be loaded). The Cisco FlexLM process is used to obtain licenses, and integrity of license files is assured by a digital signature.

When upgrading from previous versions of Cisco Unified Communications Manager, you have to take the following requirements into consideration:

- From Cisco Unified CallManager Release 4.x:
 - The licenses required are calculated during the Cisco Unified Communications Manager migration process, and an intermediate Extensible Markup Language (XML) file containing these license counts is generated.
 - The number of devices and servers that are in the database at the time of migration is the basis for the amount of device license units and node licenses in the interim license file.
 - No additional phones may be added until the interim license file has been replaced by a real license file.
 - The procedure to upgrade from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager Release 6.0(1) is as follows:

- After upgrading to Cisco Unified Communications Manager Release 6.0(1), use the **View File** option on the License File Upload window to view the intermediate XML file.
 - Copy and paste the intermediate license file into the Cisco Unified Communications Manager License Upgrade window on Cisco.com to obtain the actual license file.
 - Upload the actual license file to the publisher (License Server).
- From Cisco Unified Communications Manager Release 5.x:
- A Cisco Unified Communications Manager Release 6.0 software license has to be uploaded (Cisco Unified Communications Manager Release 5.x required only node licenses and device license units).
 - Existing device and node licenses can be used.

Example License File

The figure shows an example of a license file for 1000 device license units.

Example License File

1000 Device License Units

```
INCREMENT PHONE_UNIT cisco 6.0 permanent uncounted \
VENDOR_STRING=<Count>1000</Count><OrigMacId>000BCD4EE59D</OrigMacId>
<LicFileVersion>1.0</L icFileVersion> \
HOSTID=000bcd4ee59d
NOTICE=<LicFileID>20050826140539162</LicFileID><LicLineID>2</LicLineID> \
<PAK></PAK>" SIGN="112D 17E4 A755 5EDC F616 0F2B B820 AA9C \
0313 A36F B317 F359 1E08 5E15 E524 1915 66EA BC9F A82B CBC8 \
4CAF 2930 017F D594 3E44 EBA3 04CD 01BF 38BA BF1B"
```

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—1-26

Significant fields are highlighted and described as follows:

- INCREMENT PHONE_UNIT cisco 6.0: Indicates a phone unit license file for Cisco Unified Communications Manager Release 6.0. There is no expiration date for this license, as indicated by the keyword *permanent*.

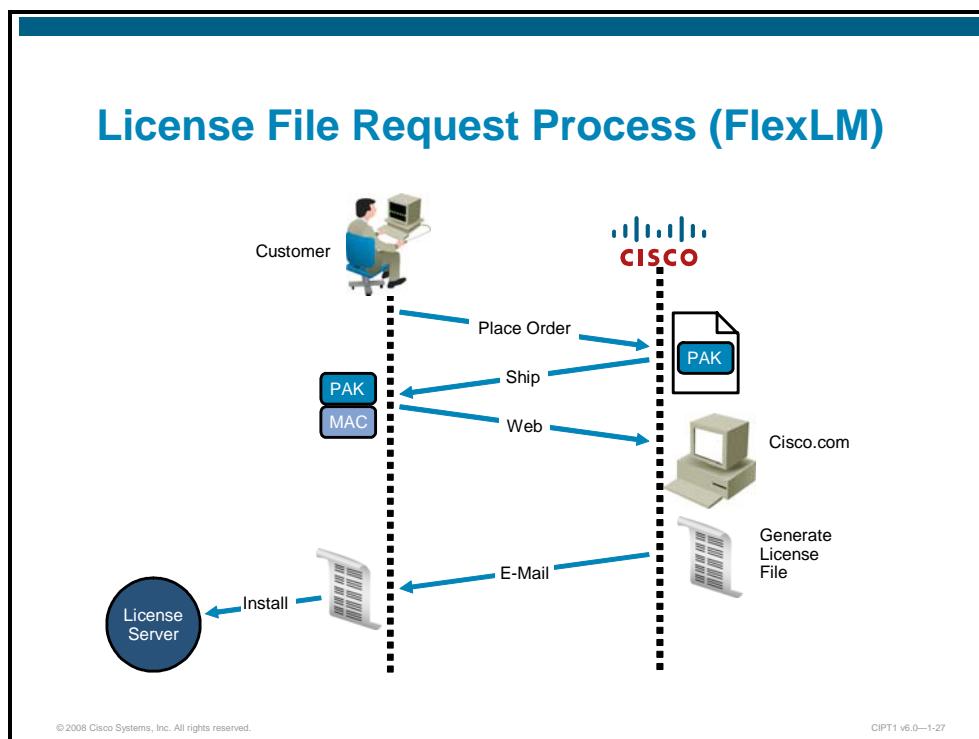
Note If this license had been a Cisco Unified Communications Manager node license, the INCREMENT type would be “CCM_NODE cisco 6.0 permanent uncounted.”

If this license had been a Cisco Unified Communications Manager software license, the INCREMENT type would be “SW_FEATURE cisco 6.0 permanent uncounted.”

- This license file includes 1000 license units.
- The MAC address of the license server is 000BCD4EE59D.

License File Request Process (FlexLM)

The figure depicts the license file request process.

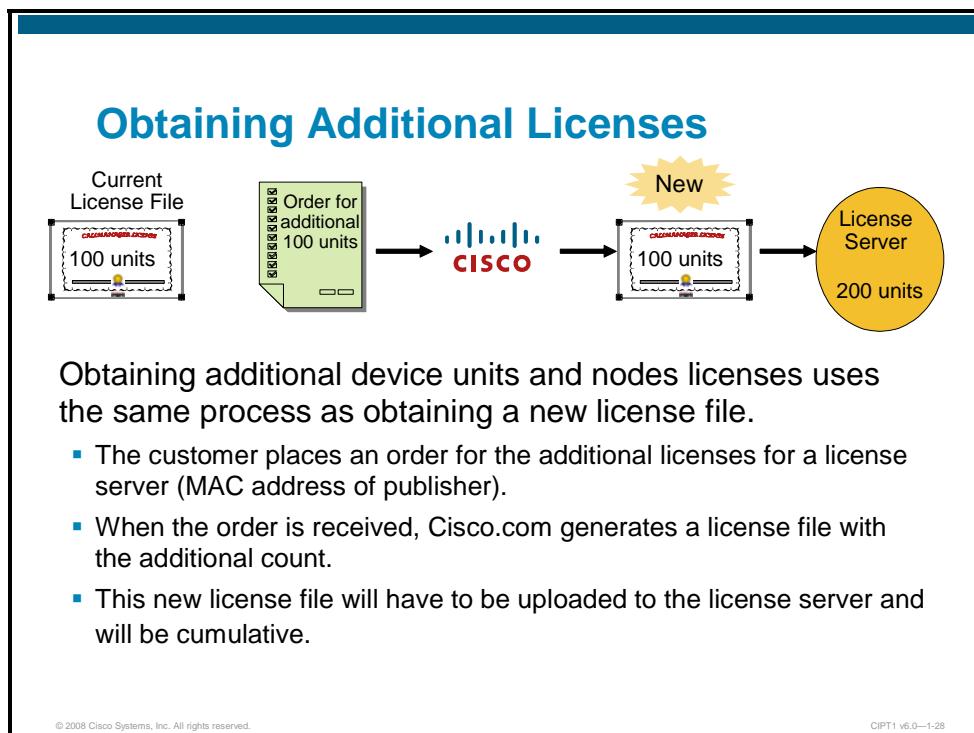


As shown in the figure, the license file request process includes these steps:

- Step 1** The customer places an order for Cisco Unified Communications Manager.
- Step 2** The manufacturing database scans the Product Authorization Key (PAK) and records it against the sales order.
- Step 3** The product (CD or paper Claim Certificate) is physically delivered to the customer.
- Step 4** The customer registers the product at Cisco.com or public web page and provides the MAC address of the publisher device that will become the license server.
- Step 5** The license fulfillment infrastructure validates the PAK, and the license key generator creates a license file.
- Step 6** The license file is delivered via e-mail to the customer. The e-mail message also contains instructions on how to install the license file.
- Step 7** The customer installs the license file on the license server (publisher).

Obtaining Additional Licenses

Additional licenses are obtained using the same process as obtaining a new license file.



The process of obtaining additional device license units and node licenses includes the following steps:

- The customer places an order for the additional licenses for a license server (publisher MAC address has to be specified).
- When the order is received, Cisco.com generates a license file with the additional count and sends it to the customer.
- The new license file has to be uploaded to the license server and will be cumulative.

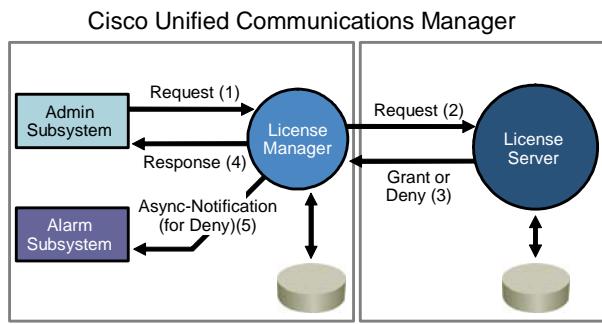
For example, if you have an existing license file uploaded to Cisco Unified Communications Manager that contains 100 device license units, and you purchase another 100 device license units, the second license file that is generated will contain only 100 device license units. When this license file is uploaded to Cisco Unified Communications Manager, the 100 device license units from the first license file are added to the devices of the second license file, resulting in a total of 200 device license units.

Cisco Unified Communications Manager Licensing Tools

This topic describes licensing tools used with Cisco Unified Communications Manager.

Licensing Functional Diagram

- License Server:
Keeps track of licenses purchased and used.
- License Manager:
Cisco Unified Communications Manager service acts as a broker between Cisco Unified CM applications that use licensing information and the license server.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-30

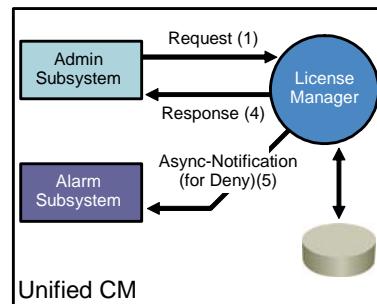
The key licensing components of the Cisco Unified Communications Manager licensing are the license server and the license manager.

License server: The license server is a service that runs on the publisher in a Cisco Unified Communications Manager cluster. The publisher takes on the functionality of the license server and is responsible for keeping track of the licenses purchased and the licenses used. When you request a license file, the MAC address of the publisher is required to generate the license file. Once generated, the license file has to be loaded to the publisher, which has to have the corresponding MAC address.

License Manager: Another service, the licenseMgr, is implemented on Cisco Unified Communications Manager. This logical component acts as a broker between Cisco Unified Communications Manager applications that use licensing information and the license server. When the License Manager receives a request from the Cisco Unified Communications Manager application, it forwards the request to the license server and responds back to the application after the request has been processed by the license server.

Licensing Functional Diagram (Cont.)

- Administration subsystem
 - Keeps information about the license units required for each phone type
 - Provides license unit calculator
 - Displays the total license capacity and the number of licenses in use
- Alarm subsystem provides alarms for following conditions:
 - Overdraft
 - License server down
 - Insufficient licenses
 - License file version mismatch



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-31

An administration subsystem and alarm subsystem complete the functional diagram. Details of these two subsystems are as follows:

- The administration subsystem provides these capabilities:
 - Keeps information about the license units required for each phone type. The customer can view this information using a GUI.
 - Supports a GUI tool that calculates the required number of phone unit licenses. The customer inputs phone types and the number of phones of each type that the customer wants to purchase. The output is the total number of licenses that the customer would need for the given configuration.
 - Supports a GUI tool that displays the total license capacity and the number of licenses in use and the license files details. The tool can also report the number of available licenses.
- The alarm subsystem generates alarms that are routed to event logs or sent to a management station as Simple Network Management Protocol (SNMP) traps to notify the administrator of these conditions:
 - **Overdraft:** Occurs when an overdraft condition exists. An overdraft condition occurs when more licenses are used than available, but the amount of exceeding licenses is in an acceptable range (five percent overdraft is permitted).
 - **License server down:** Occurs when the license manager cannot reach the license server.
 - **Insufficient licenses:** Occurs when the license server detects the fact that there are not sufficient licenses to fulfill the request and raises an alarm to notify the administrator.

- **Issues with license file:** Occurs when there is a version mismatch between the license file and the Cisco Unified Communications Manager (license file version mismatch alarm), or when the number of licenses in the license file is less than the number of phones provisioned (license file insufficient licenses alarm). Another cause of this condition is an invalid MAC address (for instance, after a network interface card [NIC] change).

Calculating License Units

Cisco Unified Communications Manager includes a tool to calculate the device license units required for a given number of phones.

Calculating License Units

CCM Node License Feature					
Type of Licensed Device	Units Consumed per Device	Current Number of Devices	Number of Units Consumed		Number of Devices
CCM Node	1	0	0		<input type="text" value="0"/>
Total CCM Node License Units Used:				Total CCM Node License Units Needed:	<input type="text" value="0"/>

Phone License Feature					
Type of Licensed Device	Units Consumed per Device	Current Number of Devices	Number of Units Consumed		Number of Devices
Analog Phone	0	0	0		<input type="text" value="0"/>
CTI Port	0	0	0		<input type="text" value="0"/>
Cisco 12 S	2	0	0		<input type="text" value="0"/>
Cisco 12 SP	2	0	0		<input type="text" value="0"/>
Cisco 12 SP+	2	0	0		<input type="text" value="0"/>
Cisco 30 SP+	2	0	0		<input type="text" value="0"/>
Cisco 30 VIP	2	0	0		<input type="text" value="0"/>

Cisco Unified Communications Manager Administration includes a license calculator that displays the amount of units consumed per device and calculates the total amount of required units for a given number of devices.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—1-32

Use this procedure to calculate the number of phone licenses required when the number of phone types and the total number of phones per phone type is entered:

- Step 1** Choose **System > License > License Unit Calculator**. The License Unit Calculator window displays. The number of license units consumed per device and the current number of devices is displayed.
- Step 2** In the Number of Devices column, enter the desired number of devices, corresponding to each node or phone.
- Step 3** Click **Calculate**. The total number of Cisco Unified Communications Manager node license units and device license units required for specified configuration is displayed.

Generating License Unit Report

Another tool, the License Unit Report tool, generates a report about the utilization of license units.

The screenshot shows the 'License Unit Report' window with three main sections:

- Phone License Feature:**

License Server	Units Authorized	Units Used	Units Remaining
CUCM1-1	50	0	50
Total Units for Feature	50	0	50
- CCM Node License Feature:**

License Server	Units Authorized	Units Used	Units Remaining
CUCM1-1	2	0	2
Total Units for Feature	2	0	2
- Software License Version:**

License Server	SW Version
CUCM1-1	6.0

At the bottom of the window, there are copyright and version information:

© 2008 Cisco Systems, Inc. All rights reserved.
CIPT1 v6.0—1-33

Use this procedure to generate a license unit report:

- Step 1** Choose **System > License > License Unit Report**.
- Step 2** The License Unit Report window displays the number of phone licenses and number of node licenses, in these categories:
 - Units Authorized
 - Units Used
 - Units Remaining

Uploading License File

To upload a license file, use Cisco Unified Communications Manager Administration.

The screenshot shows the Cisco Unified CM Administration interface. The main title is "Uploading License File". Below it, a section titled "License file upload steps" contains the following list:

1. Ensure that you have downloaded the license file to a local PC.
2. From the PC, log in to Cisco Unified Communications Manager Administration.
3. Go to **System > Licensing > License File Upload**.

The background of the interface shows a sidebar with various system settings like Server, Cisco Unified CM, and Device Pool, and a central panel with a blue header labeled "Administration". A copyright notice at the bottom left reads "© 2008 Cisco Systems, Inc. All rights reserved." and a page number "CIPT1 v6.0—1-34" at the bottom right.

Follow this procedure to upload a license file to the publisher server:

- Step 1** Ensure that the license file is downloaded to a local PC.
- Step 2** From the PC using a supported browser, log in to Cisco Unified Communications Manager Administration.
- Step 3** Choose **System > License > License File Upload**. The License File Upload window displays.

Uploading License File (Cont.)

4. Click **Upload License File**.
5. Click **Browse** to choose the license file from local directory.
6. Click **Upload**.

The screenshot shows the 'License File Upload' page. At the top, there's a 'Status' section with a blue information icon and the text 'Status: Ready'. Below it is a 'License File Information' section containing a note: 'Note: Cisco Unified Communications Manager service should be restarted after uploading software version license file.' Underneath are two buttons: 'Upload License File' (highlighted with a red box) and 'Upload File'. The 'Upload File' section contains a 'File:' input field with a 'Browse...' button to its right, and an 'Upload' button at the bottom, also highlighted with a red box. The bottom of the page includes copyright and version information: '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—1-35'.

Step 4 Click **Upload License File**.

Step 5 Click **Browse** to choose the license file from the local directory.

Step 6 Click **Upload**.

Uploading License File (Cont.)

7. Click **Continue** after the file is validated.



- Step 7** After the upload process is complete, the Upload Result file displays. Click the **Continue** prompt when it appears. The content of the newly uploaded license file will be displayed.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco Unified Communications is a comprehensive communications system of voice, video, data, and mobility products and applications over a single network infrastructure using standards-based Internet Protocol.
- Cisco Unified Communications Manager functions include call processing, signaling and device control, dial plan administration, phone feature administration, directory services, and a programming interface.
- Cisco Unified Communications Manager must be installed on a supported Cisco MCS platform or third-party server hardware approved by Cisco.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-37

Summary (Cont.)

- Access to the system is only allowed through the use of Cisco CLI and GUI tools.
- Cisco Unified Communications Manager uses an Informix Dynamic Server (IDS) database, and configuration information in the database is replicated from the first node to all subsequent nodes within a cluster.
- Three type of licenses are required: devices, applications, and software.
- License files are uploaded using Cisco Unified Communications Manager Administration GUI.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-38

References

For additional information, refer to these resources:

- Cisco Unified Communications (IP Communications/VoIP)
http://www.cisco.com/en/US/partner/netsol/ns641/networking_solutions_packages_list.htm
- Cisco Unified Communications Manager (CallManager)
<http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/index.html>

Lesson 2

Understanding Cisco Unified Communications Manager Deployment and Redundancy Options

Overview

To ensure that the Cisco Unified Communications network provides a high availability at or above that which a traditional voice network provides, it is important to understand the deployment and redundancy options of Cisco Unified Communications Manager and to follow the recommended design and deployment practices.

Objectives

Upon completing this lesson, you will be able to understand the Cisco Unified Communications Manager deployment and redundancy options. This ability includes being able to meet these objectives:

- List the supported Cisco Unified Communications Manager deployment options
- Describe the characteristics of a Cisco Unified Communications Manager single-site deployment and list the reasons for choosing this deployment option
- Describe the characteristics of a Cisco Unified Communications Manager multisite deployment with centralized call processing and list the reasons for choosing this deployment option
- Describe the characteristics of a Cisco Unified Communications Manager multisite deployment with distributed call processing and list the reasons for choosing this deployment option
- Describe the characteristics of a Cisco Unified Communications Manager multisite deployment with clustering over the WAN and list the reasons for choosing this deployment option
- Explain how call-processing redundancy is provided in a Cisco Unified Communications Manager cluster and identify the requirements for different redundancy scenarios

Cisco Unified Communications Manager Deployment Options

This topic provides an overview of the supported Cisco Unified Communications Manager deployment options.

Cisco Unified Communications Manager Deployment Options

Supported IP telephony deployment models

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

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—1-4

Cisco IP telephony supports these deployment models:

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

Selection of the type of deployment model is based on several factors, including:

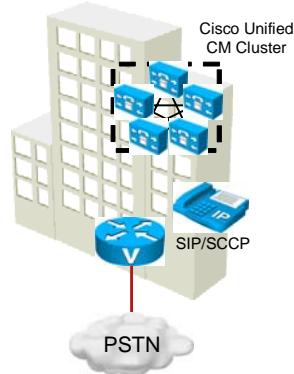
- **Size:** Number of IP phones, Cisco Unified Communications Manager servers, and other resources, such as gateways or media resources (conference bridges, music on hold [MOH] servers, and so on)
- **Geographical distribution:** Number and location of sites
- **Network characteristics:** Bandwidth and delay of network links, type of traffic that is carried over the network

Cisco Unified Communications Manager Single-Site Deployment

This topic describes the characteristics of a Cisco Unified Communications Manager single-site deployment and lists the reasons for choosing this deployment option.

Single-Site Deployment

- Cisco Unified Communications Manager servers, applications, and DSP resources are at the same physical location.
- IP WAN (if one) is used for data traffic only; PSTN is used for all external calls.
- Supports approximately 30,000 IP phones per cluster.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-6

The single-site model for Cisco Unified Communications consists of a Cisco Unified Communications Manager cluster located at a single site, or campus, with no telephony services provided over an IP WAN. All Cisco Unified Communications Manager servers, applications, and digital signal processor (DSP) resources are located in the same physical location.

An enterprise would typically deploy the single-site model over a LAN or metropolitan-area network (MAN), which carries the voice traffic within the site. In this model, calls beyond the LAN or MAN use the public switched telephone network (PSTN).

In a single-site deployment model, all Cisco Unified Communications Manager servers, applications, and DSP resources are located in the same physical location.

Each cluster supports a maximum of 30,000 IP phones. If there is a need to deploy more than 30,000 IP phones in a single-site configuration, multiple clusters inside a LAN or within a MAN can be implemented and interconnected through intercluster trunks.

Gateway trunks that connect directly to the PSTN handle external calls. If an IP WAN exists between sites, it is used to carry data traffic only; no telephony services are provided over the WAN.

Single Site: Design Guidelines

Single-site deployment requires that, for future scalability, best practices specific to the distributed and centralized call-processing model are recommended.

Single-Site: Design Guidelines

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

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-7

Current calling patterns within the enterprise must be understood. How and where are users making calls? How many calls are intersite versus intrasite? If calling patterns dictate that most calls are intrasite, using the single-site model will simplify dial plans and avoid having to provision additional dedicated bandwidth for voice across the IP WAN.

Since VoIP calls are within the LAN or campus network, it is assumed that bandwidth is not a concern. Using G.711 codecs for all endpoints will eliminate the requirement of DSP resources for transcoding, and those resources can be allocated to other functions such as conferencing and Media Termination Points (MTPs).

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 of Media Gateway Control Protocol (MGCP) gateways for the PSTN gateway is recommended if H.323 functionality is not required. When deploying multiple clusters, choose a uniform gateway and centralize the gateway functions using H.323 gatekeepers rather than using MGCP gateways.

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

Do not oversubscribe Cisco Unified Communications Manager to scale larger installations. Single-site deployment does not always equate to a single cluster. If the site has more than 30,000 IP phones, install multiple clusters and configure intercluster trunks (ICTs) between the clusters.

Single Site: Benefits

A single infrastructure for a converged network solution provides significant cost benefits and enables Cisco Unified Communications to take advantage of the many IP-based applications in the enterprise.

Single-Site: Benefits

- Ease of deployment
- A common infrastructure for a converged solution
- Simplified dial plan
- No transcoding resources required, due to the use of only a single high-bandwidth codec

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-8

Single-site deployment allows each site to be completely self-contained. Calls between sites will be routed over the PSTN. Additional provisioning of WAN bandwidth is not needed. Dial plans are also easier to provision. There is no dependency for service in the event of an IP WAN failure or insufficient bandwidth, and there is no loss of call-processing service or functionality.

In summary, the main benefits of the single-site model are:

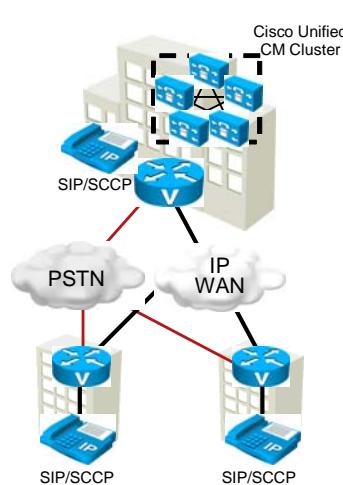
- Ease of deployment
- A common infrastructure for a converged solution
- Simplified dial plan
- No transcoding resources required, due to the use of only a single codec

Cisco Unified Communications Manager Multisite Deployment with Centralized Call Processing

This topic describes the characteristics of a Cisco Unified Communications Manager multisite deployment with centralized call processing and lists the reasons for choosing this deployment option.

Multisite WAN with Centralized Call Processing

- Cisco Unified Communications Manager at central site; applications and DSP resources centralized or distributed.
- IP WAN carries voice traffic and call control signaling.
- Supports approximately 30,000 IP phones per cluster.
- Call admission control (limit number of calls per site).
- SRST for remote branches.
- AAR used if WAN bandwidth is exceeded.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-10

The multisite WAN with centralized call-processing model consists of a centralized Cisco Unified Communications Manager cluster that provides services for many sites and uses the IP WAN to transport IP telephony traffic between the sites.

The IP WAN also carries call-control signaling between the Cisco Unified Communications Manager cluster at the central site and the IP phones at the remote sites.

The figure illustrates a typical centralized call-processing deployment, with a Cisco Unified Communications Manager cluster at the central site and an IP WAN with QoS enabled to connect all the sites. The remote sites rely on the centralized Cisco Unified Communications Manager cluster to handle their call processing. Applications such as voice mail and interactive voice response (IVR) systems are typically centralized, as well, to reduce the overall costs of administration and maintenance.

The Cisco Unified Survivable Remote Site Telephony (SRST) feature available in Cisco IOS gateways provides call-processing services to remote IP phones during WAN outage. When the IP WAN is down, the IP phones at the remote branch office can register to the SRST router. The SRST router can process calls between registered IP phones and can send calls to other sites through the PSTN.

To avoid oversubscribing the WAN links with voice traffic, causing deterioration of the quality of established calls, Call Admission Control (CAC) is used to limit the number of calls between the sites.

Centralized call-processing models can take advantage of automated alternate routing (AAR) features. AAR allows Cisco Unified Communications Manager to dynamically reroute a call over the PSTN if the call is denied because of CAC.

Multisite WAN with Centralized Call Processing: Design Guidelines

These best-practice guidelines should be followed when deploying a centralized call-processing model.

Multisite WAN with Centralized Call Processing: Design Guidelines

- Maximum of 1000 locations per Cisco Unified Communications Manager cluster.
- Maximum of 1100 H.323 devices (gateways, MCUs, trunks, and clients) or 1100 MGCP gateways per Cisco Unified Communications Manager cluster.
- Minimize delay between Cisco Unified Communications Manager and remote locations to reduce voice cut-through delays.
- Use the locations mechanism in Cisco Unified Communications Manager to provide call admission control into and out of remote branches.
- SRST on the branch router limits remote offices to a maximum of 720 Cisco IP phones when using a Cisco 3845 Series router.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-11

When implementing the multisite WAN model with centralized call processing, the following guidelines are to be considered:

- Maximum of 1000 locations per Cisco Unified Communications Manager cluster.
- Maximum of 1100 H.323 devices (gateways, multipoint control units (MCU), trunks, and clients) or 1100 MGCP gateways per Unified Cisco Unified Communications Manager cluster.
- Minimize delay between Cisco Unified Communications Manager and remote locations to reduce voice cut-through delays.
- Use the locations mechanism in Cisco Unified Communications Manager to provide CAC into and out of remote branches. The locations can support a maximum of 30,000 IP phones per cluster when Cisco Unified Communications Manager runs on the largest supported server. Since Cisco Unified Communications Manager Release 5.0, you can use Resource Reservation Protocol (RSVP)-based CAC between locations.
- There is no limit to the number of IP phones at each individual remote branch. However, the capability that is provided by the SRST feature in the branch router limits remote branches to a maximum of 720 Cisco IP phones on a Cisco 3845 series router during a WAN outage or failover to SRST. Other platforms have different limits.

If a distributed call-processing model is more suitable for the business needs of a customer, the choices include installing a Cisco Unified Communications Manager cluster at the remote branch or running Cisco Unified Communications Manager Express on the branch router.

Multisite WAN with Centralized Call Processing: Benefits

This section describes the benefits of a multisite WAN deployment with centralized call processing.

Multisite WAN with Centralized Call Processing: Benefits

- A common infrastructure for a converged solution.
- PSTN call cost savings when using the IP WAN for calls between sites.
- Use of the IP WAN to bypass toll charges by routing calls through remote site gateways, closer to the PSTN number dialed. This practice is known as tail-end hop-off (TEHO).
- Maximum utilization of available bandwidth by allowing voice traffic to share the IP WAN with other types of traffic.
- Use of Extension Mobility features between sites.
- Use of AAR in the case of insufficient bandwidth.
- Centralized administration.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-12

Multisite WAN with centralized call processing saves PSTN costs for intersite calls by using the IP WAN instead of the PSTN. IP WAN can also be used to bypass toll charges by routing calls through remote site gateways, closer to the PSTN number dialed. This practice is known as tailend hop-off (TEHO). TEHO is disallowed in some countries, and local regulations should be verified before implementing TEHO.

This deployment model maximizes the utilization of available bandwidth by allowing voice traffic to share the IP WAN with other types of traffic. Voice quality is ensured by deploying QoS and CAC. AAR reroutes calls over the PSTN if CAC denies the calls due to oversubscription.

Cisco Unified Extension Mobility can be used within the Cisco Unified Communications Manager cluster, allowing roaming users to use their directory numbers at remote phones as if they would be at their home phones.

When using the multisite WAN with centralized call-processing deployment model, Cisco Unified Communications Manager administration centralized and therefore simpler compared to a multisite with distributed call-processing model where multiple clusters have to be separately administered.

Cisco Unified Communications Manager Multisite Deployment with Distributed Call Processing

This topic describes the characteristics of a Cisco Unified Communications Manager multisite deployment with distributed call processing and lists the reasons for choosing this deployment option.

Multisite WAN with Distributed Call Processing

- Cisco Unified Communications Manager and applications are located at each site.
- IP WAN does not carry intrasite call control signaling.
- Gatekeepers can be used for scalability.
- Transparent use of the PSTN if the IP WAN is unavailable.

The diagram illustrates a multisite WAN deployment with distributed call processing. It shows three separate Cisco Unified CM Clusters, each consisting of a stack of servers and a pool of phones. Each cluster has a central 'V' icon representing a VoIP gateway. A 'GK' icon represents a Gatekeeper. The clusters are connected to a central 'IP WAN' cloud. Each cluster also connects to a 'PSTN' (Public Switched Telephone Network) via its own 'V' icon. The 'IP WAN' cloud contains a 'GK' icon, indicating it handles intersite call control signaling. The entire diagram is enclosed in a blue border with the title 'Multisite WAN with Distributed Call Processing' at the top.

The model for a multisite WAN deployment with distributed call processing consists of multiple independent sites, each with its own Cisco Unified Communications Manager cluster, connected to an IP WAN that carries voice traffic between the distributed sites.

Cisco Unified Communications Manager, applications, and DSP resources may be located at each site. IP WAN carries only signaling traffic for intersite calls, but signaling traffic for calls within a site remains local to the site. This way, the amount of signaling traffic between sites is reduced compared to a centralized call-processing model.

With the use of gatekeepers, a distributed call-processing model can scale to hundreds of sites. It also provides transparent use of the PSTN in the event that the IP WAN is unavailable.

Multisite Distributed Call Processing: Design Guidelines

This section describes the design guidelines for a multisite with distributed call-processing deployment model.

Multisite Distributed Call Processing: Design Guidelines

- Deploy a single WAN codec
- Gatekeeper networks scale to hundreds of sites
 - Implement a logical hub-and-spoke topology for the gatekeeper
 - Use gatekeeper redundancy

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-15

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

When using gatekeepers to control the intercluster communication, this deployment model scales to hundreds of sites. A gatekeeper is an H.323 device that provides CAC and E.164 dial plan resolution. Additional gatekeeper guidelines include the following:

- Gatekeeper networks can scale to hundreds of sites. Use a logical hub-and-spoke topology for the gatekeeper. A gatekeeper can manage the bandwidth into and out of a site or between zones within a site, but it is not aware of the topology.
- It is recommended to use gatekeeper redundancy support to provide a gatekeeper solution with high availability. It is also recommended to use multiple gatekeepers to provide spatial redundancy within the network.
- It is recommended to use a single WAN codec because the H.323 specification does not allow for Layer 2, IP, User Datagram Protocol (UDP), or Real-Time Transport Protocol (RTP) header overhead in the bandwidth request (header overhead is allowed only in the payload or encoded voice part of the packet). Using one type of codec on the WAN simplifies capacity planning by eliminating the need to over-provision the IP WAN to allow for the worst-case scenario.

Multisite WAN with Distributed Call Processing: Benefits

Multisite WAN with distributed call-processing model is a superset of both single-site and multisite WAN with centralized call processing.

Multisite WAN with Distributed Call Processing: Benefits

- PSTN call cost savings when using the IP WAN for calls between sites.
- Use of the IP WAN to bypass toll charges by routing calls through remote site gateways, closer to the PSTN number dialed, that is, TEHO.
- Maximum utilization of available bandwidth by allowing voice traffic to share the IP WAN with other types of traffic.
- No loss of functionality during IP WAN failure, because there is a call-processing agent at each site.

© 2008 Cisco Systems, Inc. All rights reserved.

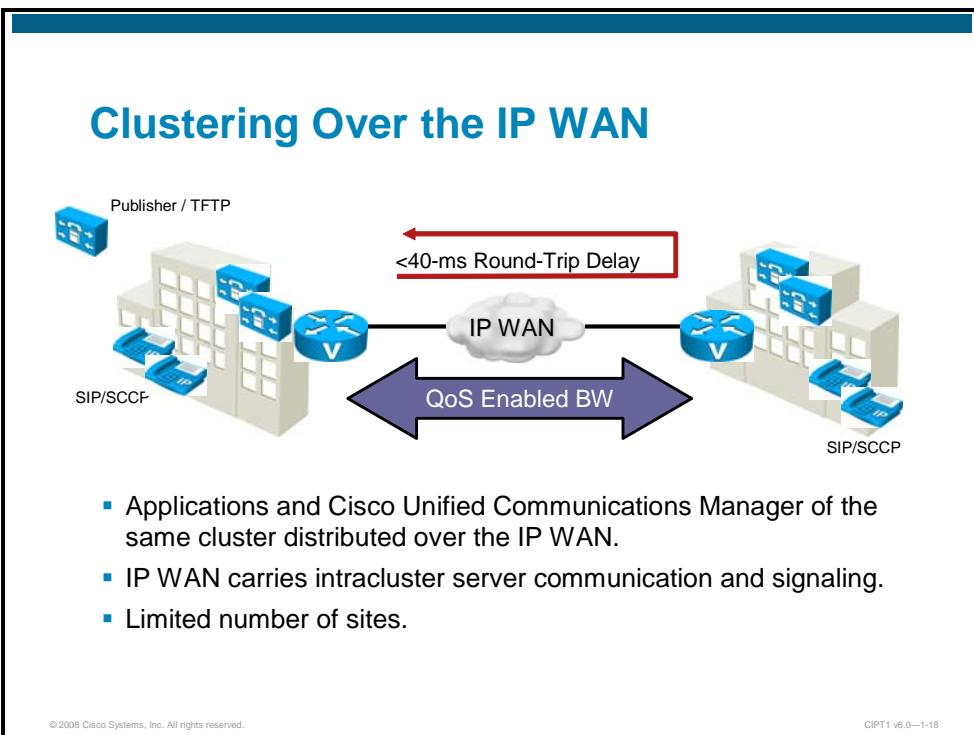
CIPT1 v6.0—1-16

The multisite WAN model with distributed call processing provides the following benefits:

- PSTN call cost savings when using the IP WAN for calls between sites
- Use of the IP WAN to bypass toll charges by routing calls through remote site gateways, closer to the PSTN number dialed, that is, TEHO
- Maximum utilization of available bandwidth by allowing voice traffic to share the IP WAN with other types of traffic
- No loss of functionality during IP WAN failure because there is a call-processing agent at each site

Cisco Unified Communications Manager Multisite Deployment with Clustering Over the WAN

This topic describes the characteristics of a Cisco Unified Communications Manager multisite deployment with clustering over the WAN and lists the reasons for choosing this deployment option.



Cisco supports Cisco Unified Communications Manager clusters over a WAN. Some of the characteristics include:

- Applications and Cisco Unified Communications Manager of the same cluster distributed over the IP WAN
- IP WAN carries intracluster server communication and signaling
- Limited number of sites:
 - Two to four sites for local failover (two Cisco Unified Communications Manager servers per site)
 - Up to eight sites for remote failover across the IP WAN (one Cisco Unified Communications Manager server per site)

The cluster design is useful for customers who require more functionality than the limited feature set offered by SRST. This network design also allows remote offices to support more IP phones than SRST in the event that the connection to the primary Cisco Unified Communications Manager is lost.

Clustering Over the IP WAN: Design Guidelines

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

Clustering Over the IP WAN: Design Guidelines

- 40-ms maximum round-trip delay between *any* two Cisco Unified Communications Manager servers in the cluster
- Minimum 1.544 Mb/s and 900 kb/s for every 10,000 BHCA within the cluster
- Up to eight small sites using the remote failover deployment model
- Failover across WAN supported (more bandwidth)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-19

The design guidelines for clustering over the IP WAN are as follows:

- Two Cisco Unified Communications Manager servers in a cluster must have a maximum round-trip delay of 40 ms between them. In comparison, high-quality voice guidelines dictate that one-way, end-to-end delay should not exceed 150 ms. Because of this strict guideline, this design can be used only between closely connected, high-speed locations.
- For every 10,000 busy hour call attempts (BHCA) within the cluster, an additional 900 kb/s of WAN bandwidth for intracluster run-time communication must be supported. The BHCA represents the number of call attempts made during the busiest hour of the day.
- Up to eight small sites are supported using the remote failover deployment model. Remote failover allows you to deploy one server per location (maximum of eight call-processing servers are supported in a cluster). In the event of Cisco Unified Communications Manager failure, IP phones will register to another server over the WAN. Therefore, SRST is not required in this deployment model (although supported). The remote failover design may require significant additional bandwidth, depending on the number of telephones at each location.

Note	In prior versions of Cisco Unified Communications Manager, subscriber servers in the cluster use the publisher's database for read/write access, and they use their local database for read-only access when the publisher's database cannot be reached. With Cisco Unified Communications Manager Release 6.x, subscriber servers in the cluster read their local database. Even database modifications can occur in the local database (for special applications such as user-facing features). Informix Dynamic Server (IDS) database replication is used to synchronize the databases on the various servers in the cluster. Therefore, when recovering from failure conditions such as the loss of WAN connectivity for an extended period of time, the Cisco Unified Communications Manager databases must be synchronized with any changes that might have been made during the outage. This process happens automatically when database connectivity is restored and can take longer over low bandwidth links. In rare scenarios, manual reset or repair of the database replication between servers in the cluster might be required, which is performed by using the commands such as utils dbreplication repair all or utils dbreplication reset all at the command-line interface (CLI). Repair or reset of database replication using the CLI on remote subscribers over the WAN causes all Cisco Unified Communications Manager databases in the cluster to be resynchronized, in which case additional bandwidth above 1.544 Mb/s might be required. Lower bandwidths can take longer for database replication repair or reset to complete.
-------------	--

Clustering Over the IP WAN: Benefits

Clustering over the IP WAN provides a combination of the benefits of the two deployment models to satisfy specific site requirements.

Clustering Over the IP WAN: Benefits

- PSTN call cost savings when using the IP WAN for calls between sites.
- Use of the IP WAN to bypass toll charges by routing calls through remote site gateways, closer to the PSTN number dialed, that is, TEHO.
- Maximum utilization of available bandwidth by allowing voice traffic to share the IP WAN with other types of traffic.
- Failover across WAN is supported.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-20

Although there are stringent requirements, clustering over the IP WAN design offers these advantages:

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

The clustering over IP WAN design is useful for customers who want to combine these advantages with the benefits provided by a local call-processing agent at each site (intrasite signaling is kept local, independent of WAN failures) and requires more functionality at the remote sites than provided by SRST. This network design also allows remote offices to support more Cisco IP phones than SRST (720 IP phones using Cisco 3845 ISR routers) in the event of WAN failure.

These features make clustering across the IP WAN ideal as a disaster-recovery plan for business continuance sites or as a single solution for up to eight small or medium sites.

Cisco Unified Communications Manager Call-Processing Redundancy

This topic explains how call-processing redundancy is provided in a Cisco Unified Communications Manager cluster and identifies the requirements for different redundancy scenarios.

Cisco Unified Communications Manager Redundancy

- Maximum of eight call-processing servers in a cluster.
- Redundancy is provided by Cisco Unified Communications Manager groups.
 - Prioritized list of call-processing servers (one or more).
 - Multiple Cisco Unified Communications Manager groups can exist in the same cluster.
 - Each call-processing server can be assigned to more than one Cisco Unified Communications Manager group.
 - Each device has a Cisco Unified Communications Manager group assigned determines the primary and backup server to which it will register.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-22

A Cisco Unified Communications Manager cluster is a group of physical servers working as a single IP PBX system. With Cisco Unified Communications Manager Release 6.0, a cluster may contain up to 20 servers, of which a maximum of 8 servers may run the Cisco CallManager service performing call processing in a cluster. Other servers can be used as TFTP servers or provide media resources such as software conference bridges or music on hold (MOH).

Cisco Unified Communications Manager call-processing redundancy is implemented by grouping servers running the Cisco CallManager service into Cisco Unified CM groups. A Cisco Unified CM group is a prioritized list of (one or more) call-processing servers.

The following rules apply for the Cisco Unified CM groups:

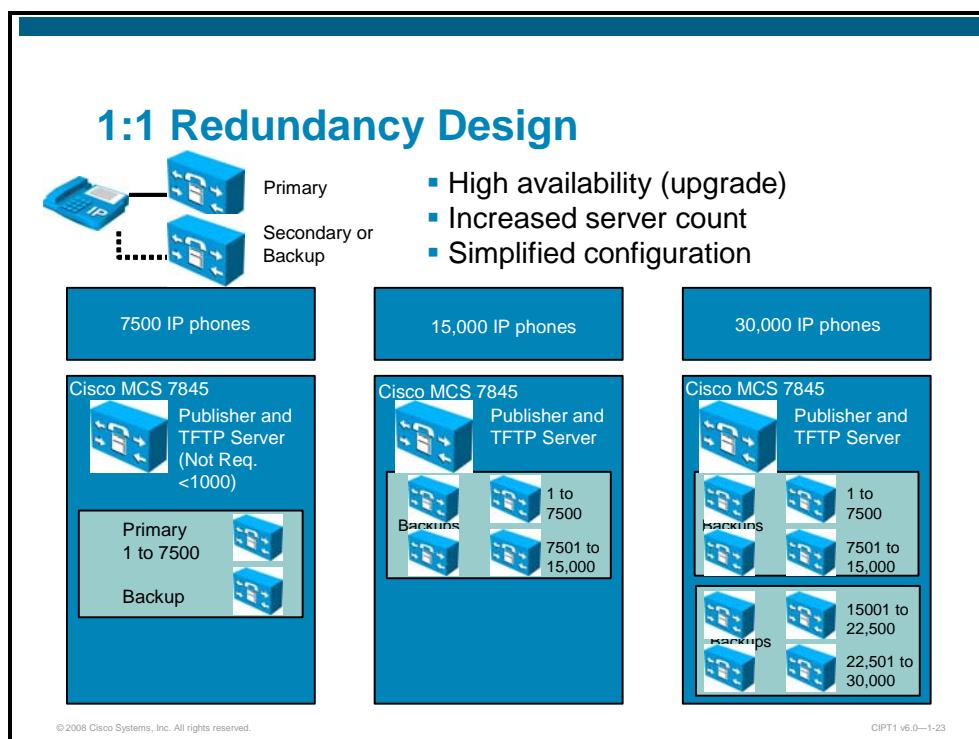
- Multiple Cisco Unified CM groups can exist in the same cluster.
- Each call-processing server can be assigned to more than one Cisco Unified CM group.
- Each device has to have a Cisco Unified CM group assigned, which will determine the primary and backup servers to which it can register.

Cisco IP phones register with their primary server. When idle, the IP phones and Cisco Unified Communications Manager exchange the signaling application keepalives. In addition, Cisco IP phones establish a TCP session with their secondary server and exchange TCP keepalives. When the connection to the primary server is lost (no keepalives received), the IP phone registers to the secondary server. The IP phone will continuously try to re-establish a

connection with the primary server; if successful, the IP phone will re-register with the primary server.

1:1 Redundancy Design

In a 1:1 Cisco Unified Communications Manager redundancy deployment design, there is a dedicated backup server for every primary server.



A 1:1 Cisco Unified Communications Manager call-processing redundancy deployment design guarantees that Cisco IP phone registrations will never overwhelm the backup servers, even if multiple primary servers fail concurrently. However, the 1:1 has an increased server count compared to other redundancy designs and may not be cost-effective.

The other services (dedicated database publisher, dedicated TFTP server, or MOH servers) and media-streaming applications (conference bridge or MTP) may also be enabled on a separate server that registers with the cluster.

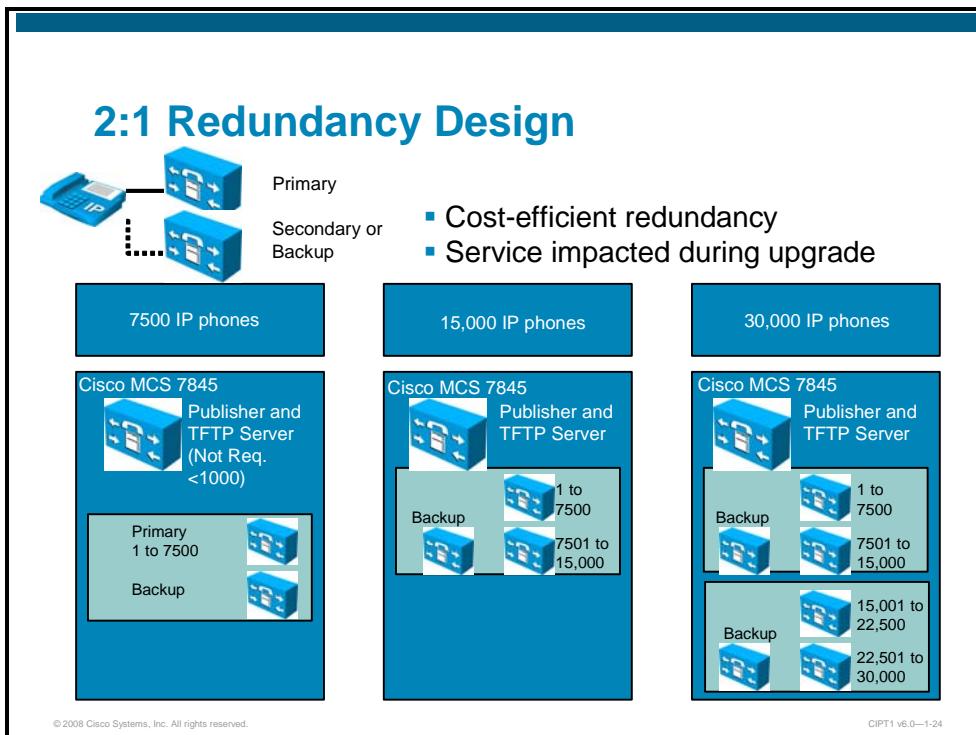
Each cluster must also provide a TFTP service. The TFTP service is responsible for delivering IP phone configuration files to telephones, along with streamed media files, such as MOH and ring files; therefore, the server running the TFTP service can experience a considerable network and processor load. Depending on the number of devices that a server is supporting, you can run the TFTP service on a dedicated server, on the database publisher server, or on any other server in the cluster.

In this example, a Cisco 7845 Media Convergence Server (MCS) is used as the dedicated database publisher and TFTP server. In addition, there are two call-processing servers supporting a maximum of 7500 Cisco IP phones (on the Cisco 7845 MCS platform). One of these two servers is the primary server; the other one is a dedicated backup server. The function of the database publisher and the TFTP server can be provided by the primary or secondary call-processing server in a smaller IP telephony deployment (fewer than 1000 IP phones). In this case, only two servers are needed in total.

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

2:1 Redundancy Design

In a 2:1 Cisco Unified Communications Manager redundancy deployment design, a dedicated backup server is in place for every two primary servers.



Although the 2:1 redundancy design offers some redundancy, there is the risk of overwhelming the backup server if multiple primary servers fail. In addition, upgrading the Cisco Unified Communications Manager servers can cause a temporary loss of service because a reboot of the Cisco Unified Communications Manager servers is needed after the upgrade is complete.

Network engineers use this 2:1 redundancy model in most IP telephony deployments because of the reduced server costs. If a Cisco MCS 7845 is used (shown in the figure), that server is equipped with redundant, hot-swappable power supplies and hard drives. When these servers are properly connected and configured, 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.

As shown in the first scenario, when using no more than 7500 IP phones, there are no savings in the 2:1 redundancy design compared to the 1:1 redundancy design, simply because there is only a single primary server.

In the scenario with up to 15,000 IP phones, there are two primary servers (each serving 7500 IP phones) and one secondary server. As long as only one primary server fails, the backup server can provide full support. If both primary servers failed, the backup server would only be able to serve half of the IP phones.

The third scenario shows a deployment with 30,000 IP phones. Four primary servers are required to facilitate this amount of IP phones. For each pair of primary servers, there is one backup server. As long as no more than two servers fail, the backup servers can provide full support, and all IP phones will operate normally.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Supported Cisco Unified Communications Manager deployment models are single-site, multisite with centralized call processing, multisite with distributed call processing, and clustering over the IP WAN.
- In the single-site deployment model, the Cisco Unified Communications Manager, applications, and DSP resources are at the same physical location; all off-site calls are handled by the PSTN.
- The multisite with centralized call-processing model has a single Cisco Unified Communications Manager cluster; applications and DSP resources can be centralized or distributed; the IP WAN carries call control signaling traffic even for calls within a remote site.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-25

Summary (Cont.)

- The multisite with distributed call-processing model has multiple independent sites, each with a Cisco Unified Communications Manager cluster; the IP WAN carries traffic only for intersite calls.
- Clustering over the WAN provides centralized administration, a unified dial plan, feature extension to all offices, and support for more remote phones during failover. But it also places strict delay and bandwidth requirements on the WAN.
- Clusters provide redundancy. A 1:1 redundancy design offers the highest availability but requires the most resources and is not as cost-effective as 1:2 redundancy.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-26

References

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html

Lesson 3

Installing and Upgrading Cisco Unified Communications Manager

Overview

Installing or upgrading software is a fundamental task that you need to perform to support the deployment of Cisco Unified Communications Manager Release 6.0. This lesson covers the Cisco Unified Communications Manager Release 6.0 installation framework, installation requirements, and the procedures to perform an installation or an upgrade.

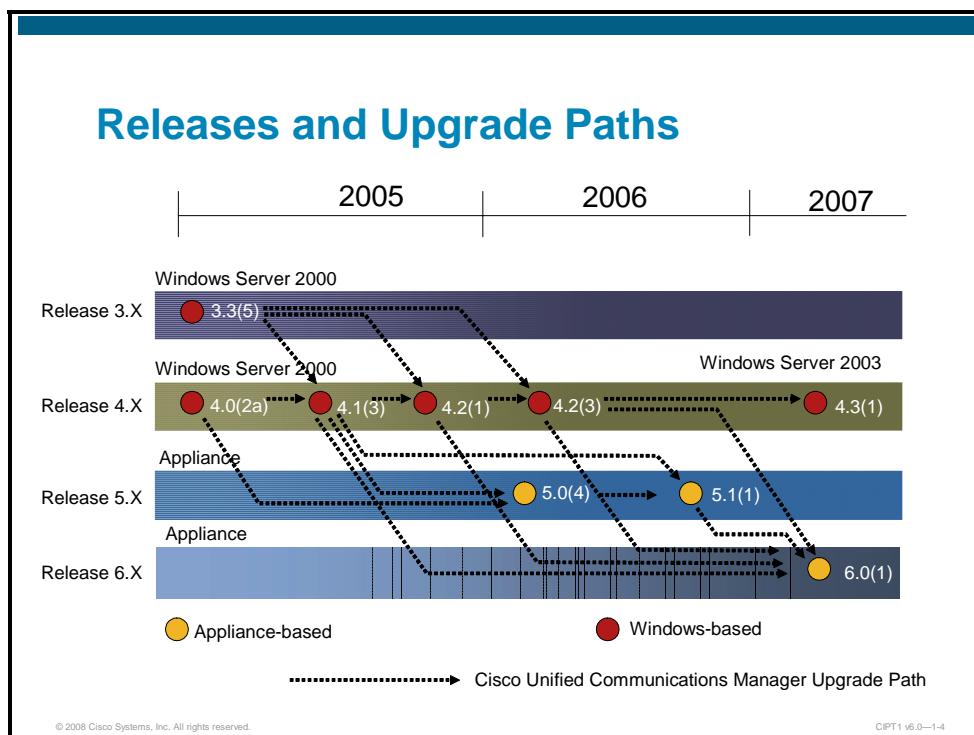
Objectives

Upon completing this lesson, you will be able to describe the Cisco Unified Communications Manager Release 6.0 installation framework, installation and upgrade procedures, and requirements. This ability includes being able to meet these objectives:

- Identify the Cisco Unified Communications Manager installation and upgrade options
- Describe how to perform a new installation of Cisco Unified Communications Manager
- Describe how to perform an upgrade during a new installation of Cisco Unified Communications Manager
- Describe how to upgrade to Cisco Unified Communications Manager Release 6.0 from Cisco Unified CallManager Release 4.x
- Describe how to upgrade from Cisco Unified CallManager Release 5.0 or higher

Cisco Unified Communications Manager Installation and Upgrade Overview

This topic describes the upgrade paths for the previous releases of Cisco Unified Communications Manager to Cisco Unified Communications Manager Release 6.0(1).



Cisco Unified Communications Manager can be upgraded from the various previous releases of Windows server-based Cisco Unified Communications Manager or appliance-based Cisco Unified Communications Manager.

Cisco CallManager Releases 3.x and earlier for Windows server have to be upgraded to Release 4.1(3) or higher before upgrade to Cisco Unified Communications Manager Release 6.0(1) is possible.

Appliance-based Cisco Unified Communications Manager versions earlier than Release 5.1(1) have to be upgraded to Release 5.1(1) before upgrade to Release 6.0(1) is possible.

Cisco Unified Communications Manager Installation and Upgrade Options

There are four different options for installation and upgrade of the Cisco Unified Communications Manager Release 6.0.

Cisco Unified Communications Manager Installation and Upgrade Options

Option	Description
Basic install	Install operating system and Cisco Unified Communications Manager application software from bootable DVD.
Upgrade during install	Basic install from bootable DVD; upgrade patches are installed from FTP, SFTP, or local DVD.
Windows upgrade	Upgrade from supported 4.x release. Existing database is dumped to file server using the Data Migration Assistant tool. Cisco Unified CM Release 6.x is installed from bootable DVD, and data previously exported by DMA are imported into Cisco Unified CM Release 6.x database.
5.x or higher upgrade	Upgrade from 5.1(x) release or higher can be done from the platform administration page using FTP or local DVD. Cisco Unified CM software is updated; no installation from bootable DVD is required.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-5

Of the four options, only the first three options are available when booting up from the DVD. These options are available when Cisco Unified Communications Manager has been chosen in the product deployment selection screen.

An upgrade from Release 5.1 (or higher) does not require (and is not supported) when booting from the installation DVD but is presented here as one of the upgrade options.

Cisco Unified Communications Manager Release 6.0(x) uses an installation framework similar to Cisco Unified Communications Manager Release 5.x. The installation process allows performing a basic installation, upgrade to a newer service release during the installation, and upgrade from Cisco Unified CallManager Release 4.1(3) or higher to Cisco Unified Communications Manager Release 6.0(1).

The installation and upgrade options work in the following way:

- **Basic install:** This option represents the basic installation and does not use any imported data. This type of installation generally starts by booting a system from an installation DVD or powering up a new system from the factory (with preinstalled software).
- **Upgrade during install:** This option performs a basic installation on a system and also allows the system to be upgraded to a specific service release patch level before the completion of the basic installation. Selection of “Upgrade During Install” for a full installation will effectively perform a basic installation before prompting the installer for additional upgrade information.

Note	It has to be ensured that the patches are available on DVD or SFTP/FTP during this installation option.
-------------	---

- **Windows upgrade:** This option upgrades a Windows-based Cisco Unified Communications Manager system to an appliance-based system and migrates data from an existing Windows server-based Cisco Unified Communications Manager system. This installation method can be done on the same machine or a different machine from the Windows server-based Cisco Unified Communications Manager machine. The Windows migration file can be saved to a variety of locations, including a remote hard drive or tape system. The Cisco Unified Communications Manager then uploads the file from one of these locations during the upgrade process.

Note	During upgrade from a Windows-based release, new software licenses and configuration files generated with the Data Migration Assistant (DMA) tool are needed.
-------------	---

- **Release 5.x or higher upgrade:** If you are upgrading from Cisco Unified Communications Manager Release 5.x, the upgrade file name has the following format:

cisco-ipt-k9-patchX.X.X-X.tar.gz.sgn

Here, X.X.X-X represents the release and build number. An upgrade from Release 5.x or higher is performed from the Cisco Unified Communications Operating System Administration.

Software Sources

Two methods exist for installing Cisco Unified Communications Manager Release 6.0 and its operating system.

Software Sources

- **From DVD**

- The operating system and Cisco Unified Communications Manager application are copied from the Installation DVD. Configuration information is prompted immediately before the operating system and application installation.

- **Pre-Installed**

- The operating system and Cisco Unified Communications Manager application are preloaded at the Cisco factory and shipped. Configuration information is prompted when the system is powered on.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-6

The first method is a full installation from the beginning, where the customer inserts a DVD and loads the operating system and Cisco Unified Communications Manager Release 6.0 application. This method is primarily for customers who have an existing Cisco Media Convergence Server (MCS), or when users purchase servers from a third-party vendor approved by Cisco.

The second method is a factory preinstallation, in which the customer orders a Cisco MCS server platform, and the operating system and Cisco Unified Communications Manager Release 6.0 application are preloaded to the server at the factory and then shipped to the customer. This method is primarily for customers who order a new Cisco MCS platform. A preinstallation without any configuration can also be done from the installation DVD by selecting “Skip” during the Platform Installation Wizard prompt. In this case, only the software will be installed, and no configuration will be applied. When the server is booted the next time, the configuration wizard will start automatically (such as on a factory-preinstalled system).

Caution Installation on an existing server formats the hard drive; all existing data on the drive is lost.

Installation Disc

The installation disc allows you to perform a basic installation, upgrade from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager Release 6.0(1), and upgrade to a newer service release during the installation.

Installation Disc

One installation DVD includes:

- Operating system
- Three products or product suites
 - Cisco Unified Communications Manager
 - Cisco Unity Connection
 - Cisco Unified Communications Manager, Business Edition
- Hardware configuration is part of install process

Note: All other discussion following this point assumes that the first option "Cisco Unified Communications Manager" is selected.



© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—1-7

The installation disc allows you to install the operating system and Cisco Unified Communications Manager from the same DVD. The installation disc will perform a hardware check to verify hardware requirements for the release. If any unsupported component is found, an applicable error message will be displayed, and the installation will be halted.

The disc can be used for full installation or for recovery if you have a backup of the data.

A separate recovery disc is available for use for system recovery if you want to recover the operating system and application files without a backup of the data.

Cisco Unity Connection and Cisco Unified Communications Manager Business Edition can also be installed from the same DVD; therefore, you have to first select the product that you want to install. This lesson describes the installation and upgrade of Cisco Unified Communications Manager.

Note Only the products that are supported on your server appear in the list.

Hardware Configuration

Hardware configuration is integrated with the Cisco Unified Communications Manager installation process.

Hardware Configuration

Hardware configuration is integrated with the Cisco Unified Communications Manager installation process.

- The installation process checks for correct hardware configuration, unsupported platforms, and minimum hardware requirements.
- The installation disc automatically configures the correct BIOS and RAID settings.

```
Checking for 2 disks for size 72 GB
physicaldrive 2:0 (port 2:id 0, 72.8 GB): OK
physicaldrive 2:1 (port 2:id 1, 72.8 GB): OK

Machine passed harddisk checks
configuring 7835H-3866 machine
checking HP machine's BIOS version
forcing current BIOS version from 06/23/2004 to 09/15/2004
#####
System Rebooting #####
System is going to reboot for new BIOS firmware to upload
press any key to continue
#####
```

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-8

The hardware configuration includes the following steps:

- The installation process checks for correct hardware configuration, supported platforms, and minimum hardware requirements.
- The installation disc automatically configures the correct BIOS and RAID settings on the supported platforms as part of the installation.

Cisco Unified Communications Manager Basic Installation

This topic describes the process for performing a basic installation of the operating system and Cisco Unified Communications Manager Release 6.0 application on the first node, the publisher.



In both the Apply Additional Release window and the Import Windows Data window, choose **No** in order to select the Basic Install option.

Important Configuration Information

Important configuration information requested during Cisco Unified Communications Manager setup is listed below.

Important Configuration Information	
Field	Description
DHCP	Static or dynamic configuration of Server IP, hostname etc. Options: Yes/No. If "No," the hostname, IP address, IP mask, and gateway have to be defined manually.
DNS Enabled	If DNS server exists in your network, enter Yes . When DNS is not enabled, only IP addresses have to be used to reach all network devices in your Cisco Unified Communications network.
First Node	If "Yes," the first Cisco Unified Communications Manager node in the cluster is configured.
NTP	When enabled, this server will act as a NTP server and provide time updates to the subsequent nodes in the cluster.
Security Password	Servers in the cluster use the security password to communicate with one another. The password must contain at least six alphanumeric characters.
SMTP	This field specifies the name of the SMTP host that is used for outbound e-mail. You must fill in this field if you plan to use electronic notification.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-11

The following table shows information about all configuration data.

Field	Description	Usage
Administrator ID	This field specifies the name that you want to assign to this account.	Ensure that the name is unique; it can contain lowercase, alphanumeric characters, hyphens, and underscores. It must start with a lowercase alphanumeric character. For this mandatory field, you should record the name for use when logging into the command-line interface (CLI) or into Cisco Unified Operating System Administration.
Administrator Password	This field specifies the password that you use for logging into the CLI on the platform and for logging into Cisco Unified Operating System Administration.	Ensure that the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscores. For this mandatory field, you should record the password for use when logging into the CLI or into Cisco Unified Operating System Administration.
DHCP	Dynamic Host Configuration Protocol	Choose Yes if you want to use DHCP to automatically configure the network settings on your server. If you choose No , you must enter a hostname, IP address, IP mask, and gateway.

Field	Description	Usage
DNS Enabled	A Domain Name System (DNS) server represents a device that resolves a hostname into an IP address or an IP address into a hostname.	If you do not have a DNS server, enter No . When DNS is not enabled, you should enter only IP addresses (not hostnames) for all network devices in your Cisco Unified Communications network. If you have a DNS server, Cisco recommends that you enter Yes to enable DNS. Disabling DNS limits the system ability to resolve some domain names.
DNS Primary	The server contacts this DNS server first when it attempts to resolve hostnames.	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd, where ddd can have a value between 0 and 255 (except 0.0.0.0). Consider this field mandatory if DNS is set to "Yes."
DNS Secondary	When a primary DNS server fails, the server will attempt to connect to the secondary DNS server.	In this optional field, enter the IP address of the secondary DNS. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd, where ddd can have a value between 0 and 255 (except 0.0.0.0).
Domain	This field represents the name of the domain in which this machine is located.	Consider this field mandatory if DNS is set to "Yes."
First Cisco Unified Communications Manager Node	This field specifies the first Cisco Unified Communications Manager node that contains the database. Subsequent nodes connect to the first node to access database content. The first node also synchronizes with an external Network Time Protocol (NTP) server and provides time to the other nodes.	Choose Yes if you are configuring the first Cisco Unified Communications Manager node in the cluster.
Hostname	A hostname represents an alias that is assigned to an IP address to identify it.	Enter a hostname that is unique to your network. The hostname can comprise up to 64 characters and can contain alphanumeric characters and hyphens. If DHCP is set to No, consider this field mandatory.
IP Address	This field specifies the IP address of this machine. It will uniquely identify the server on this network. Ensure another machine in this network does not use this IP address.	Enter the IP address in the form ddd.ddd.ddd.ddd, where ddd can have a value between 0 and 255 (except 0.0.0.0). If DHCP is set to No, consider this field mandatory.

Field	Description	Usage
IP Mask	This field specifies the IP subnet mask of this machine. The subnet mask, together with the IP address, defines the network address and the host address.	<p>Enter the IP mask in the form ddd.ddd.ddd.ddd, where ddd can have a value between 0 and 255 (except 0.0.0.0).</p> <p>A valid mask should have contiguous '1' bits on the left side and contiguous '0' bits on the right side.</p> <p>For example, a valid mask follows: 255.255.240.0 (11111111.11111111.1110000.00000000)</p> <p>An invalid mask follows: 255.255.240.240 (11111111.11111111.11110000.11110000)</p>
NIC Speed	This field specifies the speed of the server network interface card (NIC) in megabits per second.	The possible speeds include 10 or 100.
NIC Duplex	This field specifies the duplex setting of the server NIC.	The possible settings include Half and Full.
NTP Server	This field identifies the NTP servers with which you want to synchronize.	<p>Enter the hostname or IP address of one or more NTP server(s).</p> <p>Note You can add additional NTP servers or make changes to the NTP server list at a later time.</p>
NTP Server Enable	When enabled, this server will act as a NTP server and provide time updates to the subsequent nodes in the cluster.	<p>Choose Yes if you want to enable this machine to be an NTP server.</p> <p>This option is available only on the first node in a cluster.</p>
Security Password	<p>Servers in the cluster use the security password to communicate with one another.</p> <p>You will be asked to enter the same security password for each subsequent node in the cluster.</p>	<p>Enter the security password.</p> <p>Enter the same password in the Confirm Password field.</p> <p>The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.</p> <p>Caution All nodes in the cluster must have the same password.</p>

Field	Description	Usage
Set Hardware Clock	This field specifies the date and local time for the machine.	<p>Choose Yes if you want to set the date and local time for the time zone that you chose. Enter the hours based on a 24-hour format.</p> <hr/> <p>Note If you configure an external NTP server, the hardware clock gets set automatically.</p> <hr/> <p>Note If you set the hardware clock manually, the node does not use an external NTP server for time synchronization</p>
SMTP	This field specifies the name of the Simple Mail Transfer Protocol (SMTP) host that is used for outbound e-mail.	<p>Enter the hostname or dotted IP address for the SMTP server. For a host, it can contain alphanumeric characters, hyphens, or periods. For a hostname, it must start with an alphanumeric character.</p> <p>You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.</p>
Subnet IP Address	By entering a subnet address, you can specify a range of IP addresses that will be granted access to query this NTP server.	<p>Enter an IP subnet that will be granted access to the NTP server During installation, you can enter only two subnets.</p>
Subnet Mask	This field specifies the subnet mask for the subnet address.	Enter the subnet mask for the IP subnet.
Time Zone	This field specifies the local time zone and offset from Greenwich Mean Time (GMT).	<p>Choose Yes if you want to change the time zone. Choose the time zone that most closely matches the location of your machine.</p>

Installation Procedures for Basic Install (Using Installation DVD)

Cisco Unified Communications Manager Release 6.0 has to be installed on the publisher before installing it on any subscriber nodes. Installation starts the same way for all three installation options: Insert the installation disc in the DVD drive and reboot the server. The DVD Found window displays after the server completes the boot sequence.

Installation Procedures for Basic Install (Using Installation DVD)

- Starting the installation.
 - Boot the server with the installation DVD.
 - Verify the integrity of the DVD if installing from this DVD for the first time.
 - Select **Cisco Unified Communications Manager**.
 - Choose to overwrite the hard disk (otherwise installation will abort).
- Platform Installation Wizard.
 - Select **No** at the Apply Additional Releases window.
 - Select **No** at the Import Windows Data window.
- Continue with Entering the Basic Install Information window.
 - Time Zone, NIC, Network Settings, Certificates, Logins and Passwords, etc. as prompted.
- Operating system and application will be installed after all installation information has been entered.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-12

To perform the media check, choose **Yes**. To skip the media check, choose **No**. If “Yes” was selected, the installation process performs a media check of the image on the DVD to ensure that the image is error-free before installation. If the disc is OK, the installation continues.

A hardware check is then performed to determine if the correct hardware is installed, and then the Redundant Array of Independent Disks (RAID) and BIOS settings are configured.

After the hardware checks complete, the Product Deployment Selection window displays. In the Product Deployment Selection window, you can choose from the following options:

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified Communications Manager Business Edition (includes Cisco Unified Communications Manager and Cisco Unity Connection)

Note Only the products that are supported on your server appear in the list.

Select the first option (Cisco Unified Communications Manager) to install only Cisco Unified Communications Manager.

The Overwrite Hard Drive window will then indicate the current software version on your hard drive and the version on the DVD. Choosing “No” here halts the installation. Choosing “Yes” overwrites the hard drive.

Next, choose the desired type of installation by performing the following steps.

In both the Apply Additional Release window and the Import Windows Data window, choose **No** in order to select the Basic Install” option. After clicking “Continue,” the Platform Installation Wizard guides you through the installation process and gathers the required information. Review this window to familiarize yourself with navigating within the Platform Installation Wizard, and follow these guidelines:

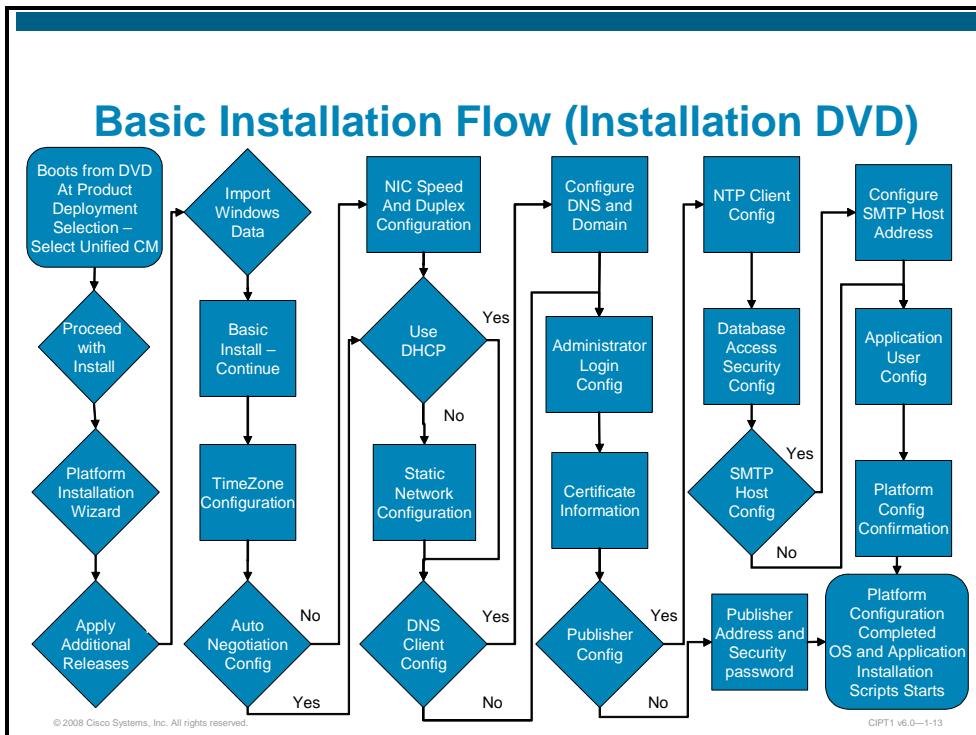
- If “Proceed” is selected, the Product Installation Configuration window displays immediately before any software is copied or installed.
- If “Skip” is selected, the software is first transferred to the hard drive, then the system shuts down. At the next boot, the system will display the Installation Configuration window. This is the same state as on a factory-installed system, in which the software is preloaded but no configuration has been done. When the preloaded system boots up, the configuration dialog is skipped if a Universal Serial Bus (USB) drive with a configuration file that includes all configuration parameters is found. Such a configuration file can be prepared using the Answer File Generator.

Note For more information regarding the Answer File Generator, refer to Using the Cisco Unified Communications Answer File Generator at
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/install/6_0_1/install/cmims601.html#wp123429

The tool itself can be accessed at http://www.cisco.com/web/cuc_afg/index.html

Basic Installation Flow (Installation DVD)

The figure shows the flow of a Basic Installation using the installation DVD.



Installation Procedures for Basic Install (Preinstalled)

This section describes the basic installation procedure when the software was preinstalled.

Installation Procedures for Basic Install (Preinstalled)

- Boots up from the hard disk (with operating system and application pre-installed).
- Enter Pre-existing configuration information.
 - Insert USB key with configuration file.
- Platform Installation Wizard (if no USB configuration file is present).
 - Select **No** at the Apply Additional Releases window.
 - Select **No** at the Import Windows Data window.
- Continue entering the Basic Install information (if no USB configuration file).
 - Time zone, NIC, network settings, certificates, logins, passwords, etc.
- Configuration scripts will run after the configuration information has been collected, and network services will be restarted.

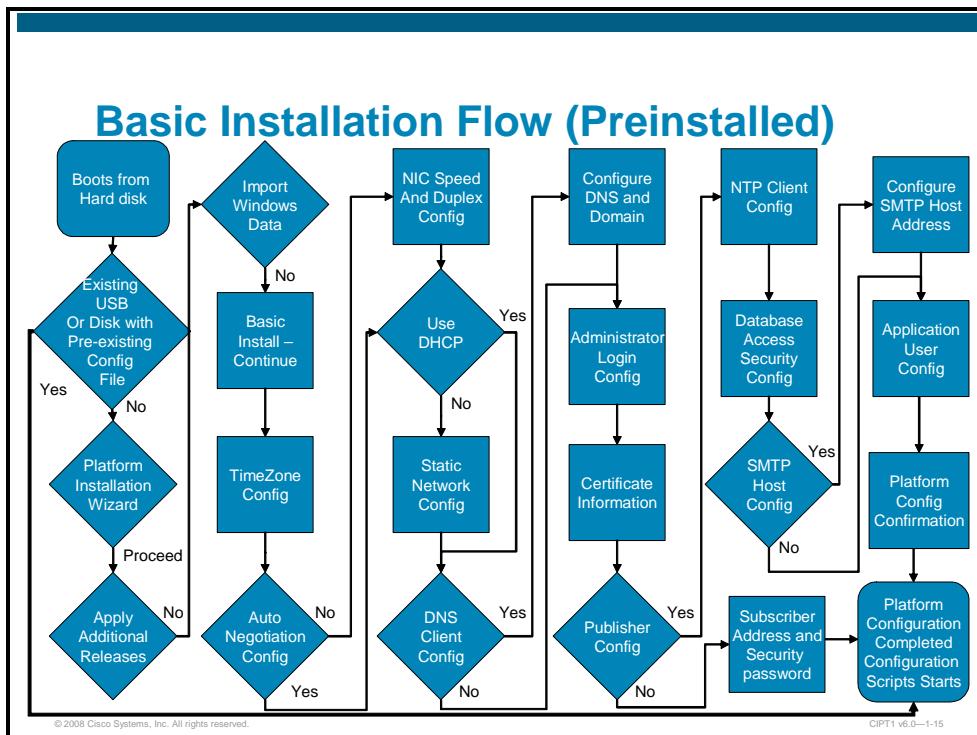
© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-14

After the boot of the system, the Pre-existing Installation Configuration window displays. If pre-existing configuration information generated by the Answer File Generator and stored on a floppy disc or a USB key exists, the disc or the USB key has to be inserted and “Continue” has to be chosen. In this case, the installation wizard will read the configuration information from the USB key. If no configuration file on a USB key is provided, the installation wizard prompts for configuration data.

Basic Installation Flow (Preinstalled)

The following figure shows the flow of a basic installation procedure when the software was preinstalled.



The only difference in a basic installation executed from the installation DVD is the ability to skip the configuration portion by providing a configuration file on a USB key.

Cisco Unified Communications Manager Upgrade During Installation

This topic describes the procedure to include upgrades in the installation process.

Apply Additional Release

Upgrade During Install option

- Is selected when you select **Yes** at the Apply Additional Release window
- Performs a basic install and allows the system to be upgraded to a specific patch level
- Obtains upgrade patch from a remote source or local DVD source
- Installs multiple patches if desired



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-17

This option is chosen by selecting “Yes” at the Apply Additional Release window. Using this mechanism saves a considerable amount of installation time, as the installation of the software stored on the DVD, and the installation of a service release, engineering special, or security update are combined into a single installation process. The additional release has to be downloaded and prepared on a DVD or FTP/Secure FTP (SFTP) server before starting the installation.

Installation Procedures for Upgrade During Installation

This section describes the procedure of an upgrade during installation.

Installation Procedures for Upgrade During Installation

- Starting the installation.
 - Boot the server with the installation DVD.
 - Verify the checksum for the DVD.
 - Choose to overwrite the hard disk.
- Platform Installation Wizard.
 - Select **Yes** at the Apply Additional Releases window.
- Installation of operating system and application will start.
 - When installation has completed, appliance will reboot.
- After reboot, choose **Upgrade Retrieval Mechanism**.
 - Local: Specified path and file name.
 - FTP/SFTP: Configure Network Settings and enter the location and login information for the remote file server.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-18

The installation starts when the server is booted from the installation DVD. The checksum for the DVD should be verified and “Overwrite Hard Disk” has to be selected.

In the Platform Installation Wizard, “Yes” needs to be selected at the Apply Additional Releases window. Then the installation of operating system and application will start, and when finished, the system will reboot.

After reboot, the Upgrade Retrieval mechanism has to be chosen:

- Local: Specify path and file name on the local DVD
- FTP/SFTP: Configure Network Settings and enter the location and login information for the remote file server

Caution The Overwrite Hard Drive window indicates the software version on your hard drive (if a previous installation) and the DVD. All existing data on your hard drive gets overwritten and destroyed.

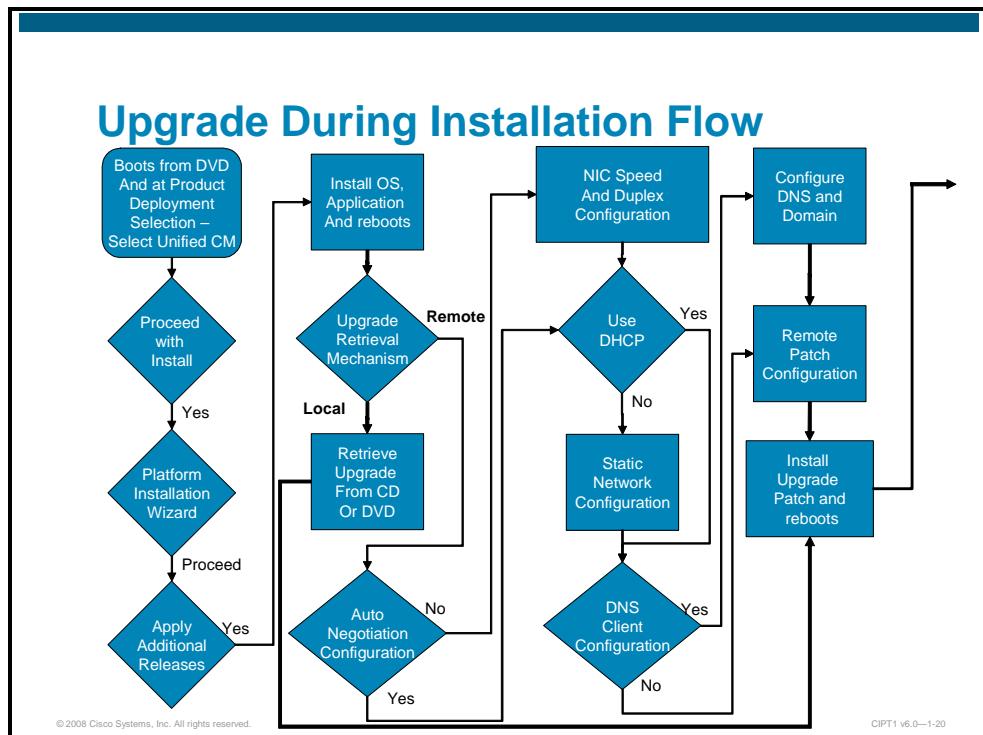
Installation Procedures for Upgrade During Installation (Cont.)

- Upgrade will start.
 - When upgrade has completed, appliance will reboot.
- After reboot, at the Entering Pre-existing Configuration Information dialog box, insert USB or disc if you have pre-existing configuration information.
- Platform Installation Wizard.
 - Select **No** at the Apply Additional Releases window.
 - Select **No** at the Import Windows Data window (if you have no existing Windows DMA data).
- Continue entering the Basic Install information if no USB or disc with pre-existing configuration information has been inserted.
 - Time zone, NIC, network settings, certificates, logins, passwords, etc.
- Configuration scripts will run after the configuration information has been collected, and network services will be restarted.

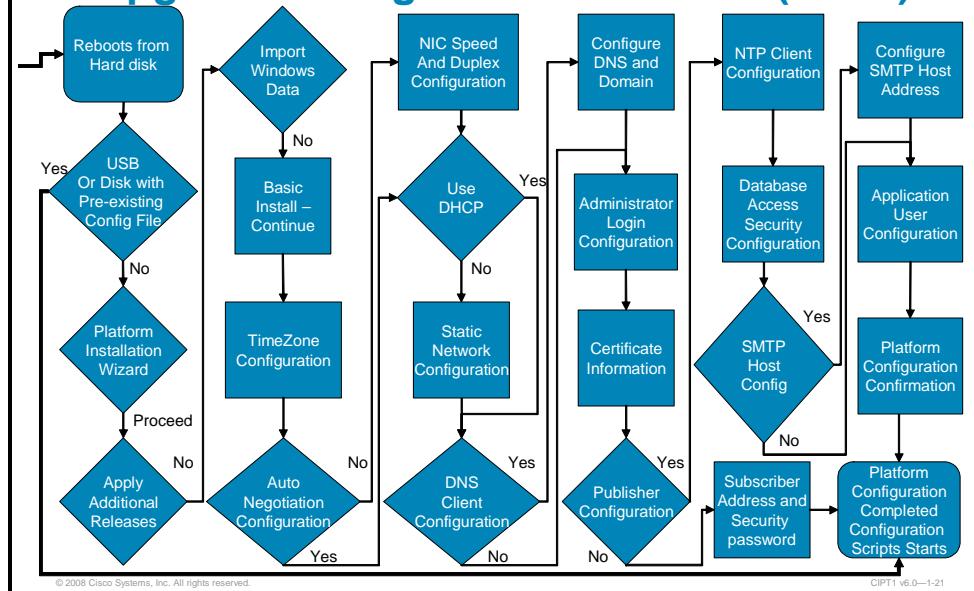
After entering the source of the additional release, the upgrade will start. When the upgrade has completed, the system reboots. The rest of the installation will be exactly the same, such as on a preinstalled system after the first boot.

Upgrade During Installation Flow

The figure shows the flow of a basic installation procedure when the Apply Additional Releases option was selected during installation of the system.



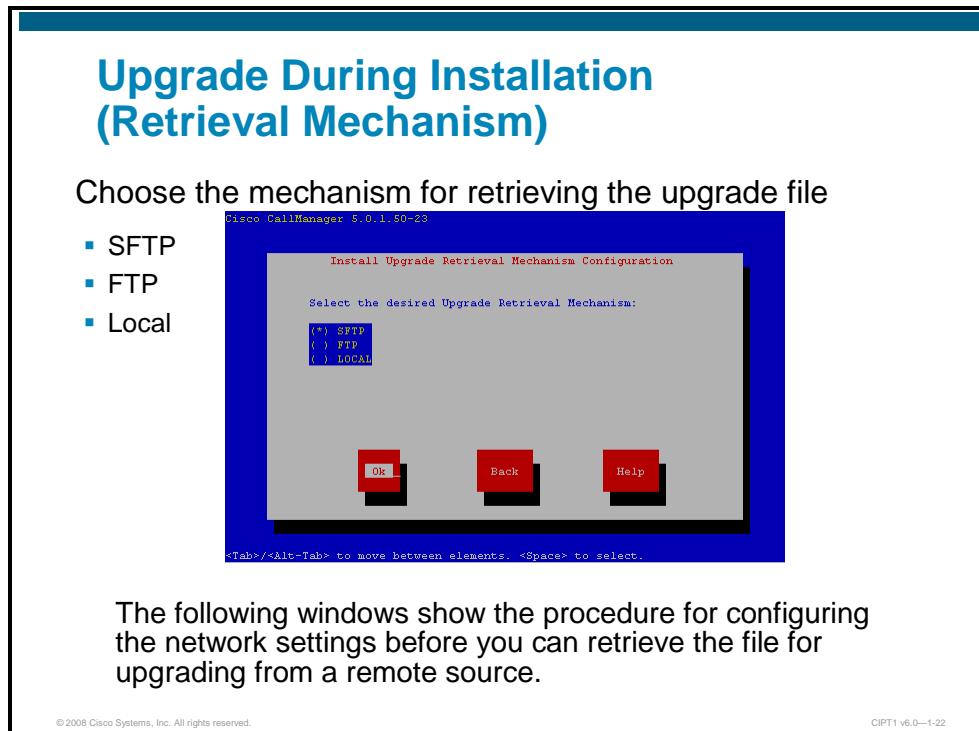
Upgrade During Installation Flow (Cont.)



This part equals the installation process of a preinstalled system.

Upgrade During Installation (Retrieval Mechanism)

The figure shows the Retrieval Mechanism dialog.

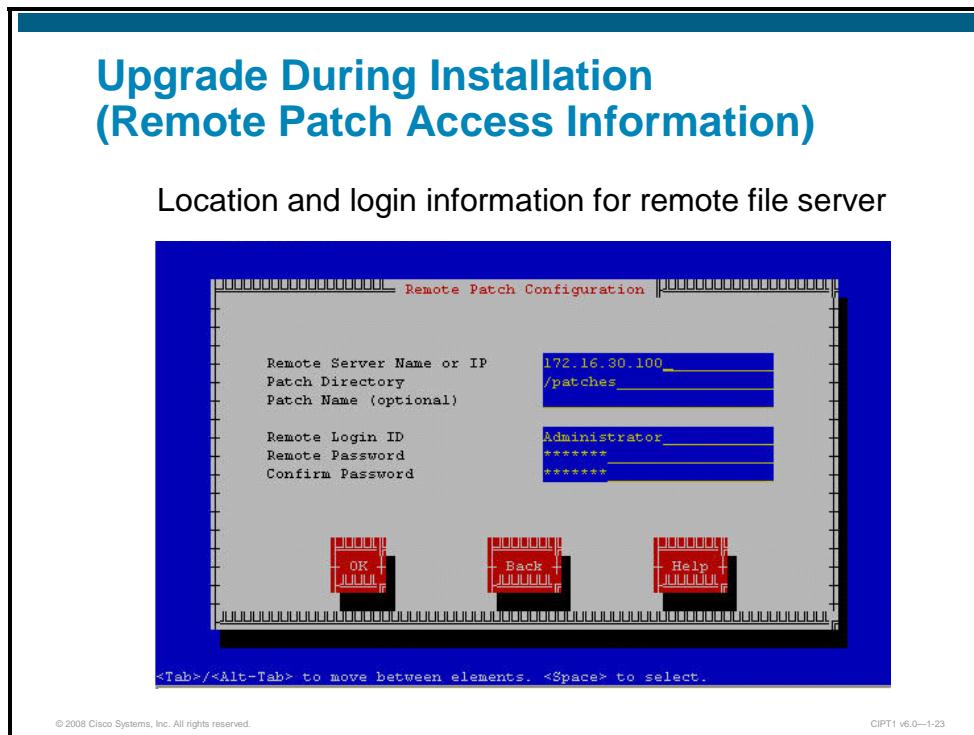


This table contains the field descriptions.

Field	Description
LOCAL	Retrieves the upgrade file from a local CD or DVD
FTP	Retrieves the upgrade file from a remote server by using FTP
SFTP	Retrieves the upgrade file from a remote server by using the SFTP

Upgrade During Installation (Remote Patch Access Information)

The figure shows the Remote Patch Configuration dialog used by the FTP/SFTP retrieval methods.

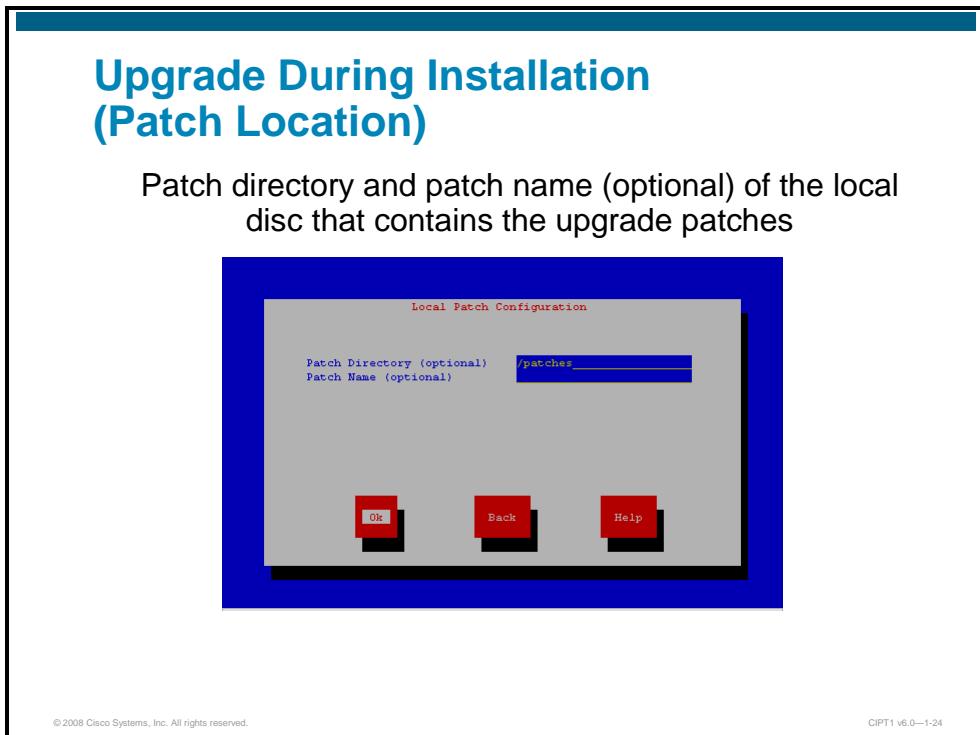


This table contains the field descriptions.

Field	Description
Remote Server Name or IP	IP address of the FTP or TFTP server. If using hostname, you need to ensure that the DNS is configured and that the hostname can be resolved to a valid IP address.
Patch Directory	Specifies the directory path for the patch.
Remote Login ID	Login ID for the FTP or SFTP server.
Remote Password	Remote passwords for the FTP or SFTP server.
SFTP	Specifies the file name for the patch.

Upgrade During Installation (Patch Location)

The figure shows the Local Patch Configuration dialog used by the local retrieval methods.



The patch directory and file name refer to the root of the DVD.

Cisco Unified Communications Manager Windows Upgrade

This topic describes upgrade procedures from Cisco Unified CallManager Releases 4.x on Windows-based platforms. Upgrade from these platforms involves the Cisco DMA tool.

Installation Procedures for Windows Upgrade

- The Cisco Unified CallManager Release 4.x has to be backed up using Cisco BARS.
- The Cisco Data Migration Assistant (DMA) is used to export the database content to a file server.
- Installation of Cisco Unified Communications Manager Release 6.x.
 - Server is booted with the installation DVD.
 - The system hard disk needs to be overwritten.
- Platform Installation Wizard has to import Windows data.
- Installation of operating system and application will start.
- After completed installation, the Cisco DMA retrieval mechanism loads the exported 4.x data file from these devices:
 - A local path by file name.
 - A FTP/SFTP server with given network settings, location, and login.

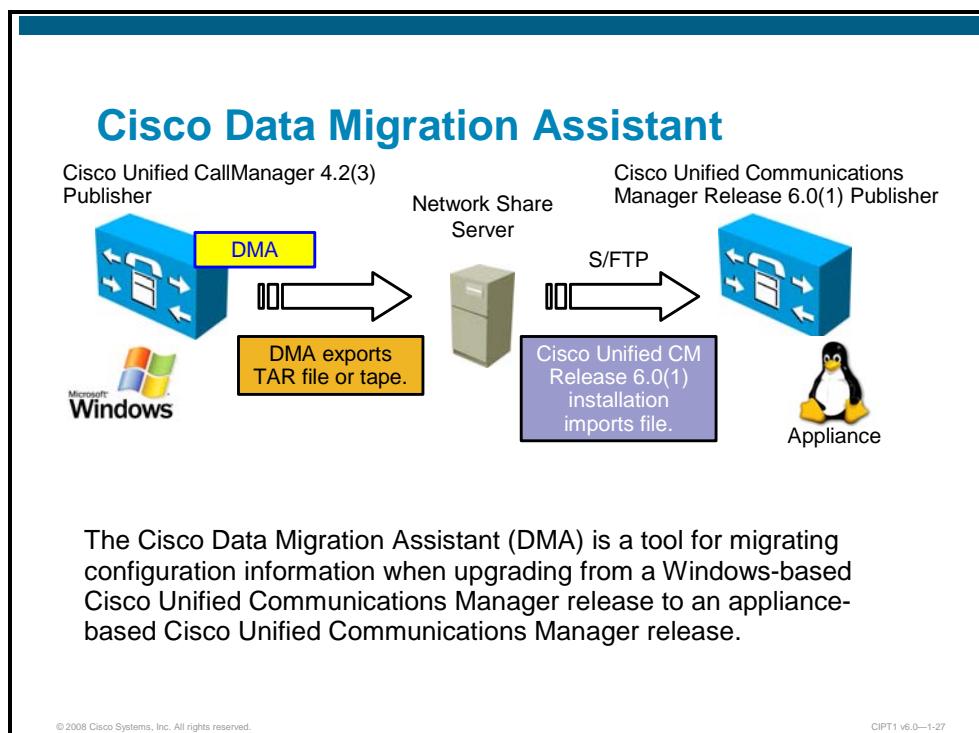
© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-26

When upgrading from Windows-based Cisco Unified CallManager Release 4.x to the appliance-based Cisco Unified Communications Manager Releases 5.x or 6.x, all of the configuration and runtime data have to be exported from the Microsoft SQL database and transformed to the new format of the Informix database. These tasks are performed by the Cisco DMA tool.

Cisco DMA

This figure shows the functions of the Cisco DMA.



The Cisco DMA needs to be installed and run on the Cisco Unified CallManager Release 4.x publisher server. The backup file created by Cisco DMA must be saved to a tape drive or to a network location.

The Cisco Unified Communications Manager Release 6.0(1) publisher installation procedure then retrieves the DMA backup file via SFTP, FTP, or from the tape and sends Cisco Unified CallManager Release 4.x data into Cisco Unified Communications Manager Release 6.0(1).

Installation of Cisco Unified Communications Manager subscribers follows the publisher installation. Subscribers will pull data from the publisher database; therefore, no DMA files are loaded during the installation of a subscriber.

Data Not Exported by Cisco DMA

This section provides information about data not migrated by the Cisco DMA.

Data Not Exported by Cisco DMA

- Custom MOH files
 - User must reinstall on all servers after upgrade to Release 6.0(1).
- Custom TFTP phone load files and custom background images.
 - User must reapply after upgrade to Release 6.0(1).
- Files on Cisco Unified Communications Manager subscriber servers.
 - Subsequent nodes obtain required information from the first node as part of the Cisco Unified Communications Manager upgrade process.
- **Cisco Unified Communications Manager Administrator user ID needs to be set during installation.**
 - There is no longer a default CCMAdministrator user ID in Cisco Unified CM Release 6.x.
- User names are migrated, but passwords and pins are not.
 - You will define a standard password or pin for all usernames during the upgrade and ask users to change from CCMUser pages.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-28

Customized music on hold (MOH) files have to be backed up manually to be reinstalled on all Cisco Unified Communications Manager servers after upgrade to Release 6.0(1).

Special phone load files and background images stored on the TFTP server will also be lost; these files have to be backed up and can be uploaded to the newly installed TFTP server after upgrade.

All files on Cisco Unified Communications Manager subscriber servers will not be backed up, because the Cisco DMA only runs on the publisher server.

The default user ID for the Cisco Unified Communications Manager administrator needs to be set during the Cisco Unified Communications Manager Release 6.0(1) installation, as a default user ID “CCMAdministrator” is no longer mandatory.

All usernames are migrated, but the passwords and pins will be reset to a default defined during installation procedure. After upgrade, the users are able to change their passwords and pins on the Cisco Unified Communications Manager UserOptions web pages.

Windows Upgrade Installation Option

This section shows the activation of the Windows upgrade installation option.

Windows Upgrade Installation Option

Windows Upgrade option

- Is selected at the Import Windows Data window
- Installs Cisco Unified Communications Manager Release 6.x and imports data from a Cisco Unified CallManager Release 4.x
- Obtains Data Migration Assistant (DMA) data file from a remote source or local DVD
- Requires install and run DMA on a Cisco Unified CallManager 4.x



The screenshot shows a dialog box titled "Cisco Unified Communications Manager 6.0.1.1000-7" with the sub-section "Import Windows Data". The text inside the box reads:
"Would you like to import data from a Windows version of the Cisco Unified Communications Manager?
This option allows you to import data from an existing Windows system as a data file created by the Data Migration Assistant (DMA). It asks for information necessary to retrieve the data file, installs the software from the PBD and then imports the configuration into the system."
At the bottom are three red buttons labeled "Yes", "No", and "Back".
(Tab)>/Alt-Tab> to move between elements. <Space> to select.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-29

To perform the windows upgrade installation option, select **Yes** at the Import Windows Data window. After the installation of Cisco Unified Communications Manager Release 6.0, the configuration data will be retrieved from tape or an FTP or SFTP source. This installation option requires Cisco DMA to run on the Windows-based Cisco Unified Communications Manager Release 4.x version prior to upgrade start.

Cisco Unified Communications Manager Upgrade

This topic describes upgrade procedures from Cisco Unified Communications Manager Releases 5.x or 6.x. Upgrades on these platforms are done using the Cisco Unified Operating System Administration.

Cisco Unified Communications Manager Release 5.x and 6.x Upgrades

- Upgrades from Release 5.x or higher is done from the Cisco Unified Operating System Administration page.
- Cisco Unified Communications Manager provides dual partitions.
 - Holds two copies of the Cisco Unified Communications Manager software and database (active and inactive partitions).
- Upgrade Process.
 - Perform a backup using Disaster Recovery System (DRS).
 - Start the installation of the new version (performed in the background while current version is operating).
 - After new version has been installed to inactive partition, reboot, switching to new version.
 - Cisco Unified Communications Manager will boot from partition where new version has been installed.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-31

Updates from appliance-based Cisco Unified Communications Manager Release 5.x or higher are performed from the Cisco Unified Operating System Administration web page.

Note	Cisco Unified CallManager Release 5.0 requires an upgrade to Cisco Unified Communications Manager Release 5.1(1) before it can be upgraded to Cisco Unified Communications Manager Release 6.0.
-------------	---

The system does not have to be rebooted, as the current operating system and application are not overwritten by the new version. Instead, they are installed to a second (inactive partition).

The upgrade procedure includes the following steps:

- Perform a backup using Cisco Unified Communications Manager Disaster Recovery System (DRS).
- Start the installation of the new version from Cisco Unified Operating System Administration.
- The installation of the new version will be performed in the background, while the server continues to operate using the current version.
- At any time after the new version has been installed, reboot the system with the option to switch versions (swap active and inactive partitions).
- Cisco Unified Communications Manager will boot from the partition where the new version has been installed.

Dual Partitions

This section provides information about the Cisco Unified Communications Manager Dual Partitions mechanism.

Dual Partitions

- Dual partitions each have Unified Communications Manager software and database.
- Enables continued operation when you upgrade software.
- Upgrade software installs on the inactive partition.
- Activates the upgraded software by “switching versions” during reboot.
- Current active partition becomes inactive and retains current “old” software until next upgrade.
- If versions are switched before next upgrade, you revert to previous version.
- System maintains two versions of software (does not apply to Release 4.x upgrades).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-32

Since Release 5.x, Cisco Unified Communications Manager supports dual partitions, which simplify software updates:

- Each partition keeps one version of Cisco Unified Communications Manager software and database.
- Operation continues during upgrades.
- Upgrade installs to the inactive partition.
- During reboot, versions (active and inactive partitions) can be swapped. The previously active partition becomes inactive and retains the “old” software and database until the next upgrade.
- If versions are switched again before the next upgrade, you revert to the previous version (downgrade).
- The system always maintains two versions of software (does not apply to upgrade from Cisco Unified CallManager Release 4.x).

Installation Procedures for Cisco Unified Communications Manager Upgrade

This section provides information about the upgrade procedure of an existing appliance-based Cisco Unified Communications Manager.

Installation Procedures for Cisco Unified Communications Manager Upgrade

- Back up the existing Cisco Unified Communications Manager Release 5.1(1) system using the Cisco Unified Communications Manager Disaster Recovery System (DRS).
- Ensure that SFTP/FTP server is available to perform the upgrade remotely or that an upgrade image is available on DVD to perform the upgrade locally.
- Log in to the Cisco Unified Operating System Administration page and start the upgrade.
- Cisco Unified Communications Manager upgrades can be done without affecting call processing, and server can be rebooted later during a service window after the upgrade.
- Install updated license file (if required).
- Reboot and switch version on publisher and wait until it is initialized and fully operational.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-33

The upgrade procedure includes the following steps:

- Back up the existing Cisco Unified Communications Manager Release 5.1(1) system using the Cisco Unified Communications Manager DRS.
- Ensure that an SFTP or FTP server is available to perform the upgrade remotely, or that an upgrade image is available on DVD to perform the upgrade locally.
- Log in to the Cisco Unified Operating System Administration page and start the upgrade.
- Cisco Unified Communications Manager upgrades can be done without affecting call processing, and the server can be rebooted later during a service window after the upgrade.
- Install the updated license file (required when upgrading from Cisco Unified Communications Manager Release 5.x to Release 6.0).
- Reboot and switch versions on the publisher, and wait until it is initialized and fully operational.

Upgrade Process on Cisco Unified Communications Manager Releases 5.x and 6.x

The Cisco Unified Operating System Administration allows upgrades from local sources and FTP or SFTP servers.

Upgrade Process on Cisco Unified Communications Manager Platforms 5.x and 6.x

Cisco Unified Operating System Administration > Software Upgrades > Install/Upgrade

Software Location

Source*	Remote Filesystem
Directory*	/upgrade/
Server*	172.47.1.102
User Name*	cisco
User Password*	*****
Transfer Protocol*	FTP

Cisco Unified Operating System Administration allows upgrades from local sources and FTP or SFTP servers.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-34

Log in to the Cisco Unified Operating System Administration. Select the Software Upgrades menu, and select “Install/Upgrade” to define the source of the upgrade file.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Upgrades from versions 3.x, 4.0(2), 5.0(x) to 6.x are not supported.
- Cisco Unified Communications Manager basic installation can be performed from bootable DVD or factory pre-installed systems.
- Using the Upgrade During Install option saves time when applying service release updates.
- The Cisco Unified Communications Manager administrators user ID can be freely chosen. The account CCMAdministrator is no longer mandatory.
- Upgrades from version 5.1x to 6.x can be done via Cisco Unified Operating System Administration Software Upgrade.

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Installation Documentation
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/docguide/6_0_1/dg601.html#wp1028219
- Installing Cisco Unified Communications Manager 6.0(1)
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/install/6_0_1/install/cmins601.html#wp61456

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- Cisco Unified Communications Manager is the central component of the Cisco Unified Communications solution, which covers the whole range of IP communication.
- There are four call-processing deployment models. They differ based on the call-processing type (central versus distributed) and the number of sites (single versus multi-site).
- First-time installation of Cisco Unified Communications Manager Release 6.x and upgrades from Cisco Unified CallManager Release 4.x (Microsoft Windows based) are performed from a bootable DVD.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—1-1

This module describes main characteristics of Cisco Unified Communications Manager. The module describes the role that Cisco Unified Communications Manager plays in the overall Cisco Unified Communications solution, and in the Cisco Unified Communications Manager hardware and software requirements. Also, the module describes the four call-processing deployment models and how Cisco Unified Communications Manager clusters provide redundancy and failover. Finally, the module describes the Cisco Unified Communications Manager installation and upgrade processes.

References

For additional information, refer to these resources:

- Unified Communications (IP Communications/VoIP)
http://www.cisco.com/en/US/partner/netsol/ns641/networking_solutions_packages_list.html
- Cisco Unified Communications Manager (CallManager)
<http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/index.html>
- Cisco Unified Communications Solution Reference Network Design (SRND) Document Based on Cisco Unified Communications Manager Release 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager Installation Documentation
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/docguide/6_0_1/dg601.html#wp1028219
- Installing Cisco Unified Communications Manager Release 6.0(1)
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/install/6_0_1/install/cmins601.html#wp61456

Module Self-Check

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

- Q1) Which two of the following options are not parts of the Cisco Unified Communications Architecture? (Choose two.) (Source: Understanding Cisco Unified Communications Manager Architecture)

- A) IP telephony
- B) customer contact center
- C) firewalls
- D) video telephony
- E) rich-media conferencing
- F) LAN switches
- G) third-party applications

- Q2) Which three of the following options are Cisco Unified Communications Manager functions? (Choose three.) (Source: Understanding Cisco Unified Communications Manager Architecture)

- A) packet routing
- B) signaling and device control
- C) dial plan administration
- D) phone feature administration
- E) storing voice mails
- F) providing call center functionality
- G) filtering IP packets

- Q3) List the minimum hardware requirements for Cisco MCS platforms required by Cisco Unified Communications Manager Release 6.0. (Source: Understanding Cisco Unified Communications Manager Architecture)
-

- Q4) Which database is used by Cisco Unified Communications Manager Release 6.0? (Source: Understanding Cisco Unified Communications Manager Architecture)

- A) Informix Dynamic Server
- B) Microsoft SQL 7
- C) Microsoft SQL 2000
- D) Oracle
- E) MSJET DB

- Q5) Which two of the following features rely on the publisher? (Choose two.) (Source: Understanding Cisco Unified Communications Manager Architecture)

- A) Call Forward All
- B) Message Waiting Indicator
- C) Cisco Unified Communications Manager Bulk Administration Tool
- D) Do Not Disturb Enable/Disable
- E) Cisco Unified Communications Manager Administration
- F) Extension Mobility Login

Q6) What is a licensing overdraft, and by what percentage is it allowed? (Source: Understanding Cisco Unified Communications Manager Architecture)

Q7) Which of the following options is not a Cisco Unified Communications Manager licensing tool? (Source: Understanding Cisco Unified Communications Manager Architecture)

- A) License Unit Report
- B) License File Generator
- C) License Unit Calculator
- D) License File Upload

Q8) Which three of the following options are supported Cisco Unified Communications Manager deployment models? (Choose three.) (Source: Understanding Cisco Unified Communications Manager Deployment and Redundancy Options)

- A) a single-site with one call-processing agent
- B) two clusters in active-backup mode
- C) multisites with centralized call processing
- D) two load-balancing clusters
- E) multisites, each with its own call-processing agent
- F) a single-cluster with distributed call processing
- G) two or more clusters with bidirectional trust relationships

Q9) Which codec is recommended in a single-site Cisco Unified Communications Manager deployment? (Source: Understanding Cisco Unified Communications Manager Deployment and Redundancy Options)

- A) G.721
- B) G.711
- C) G.723
- D) G.729

Q10) Which statement is true about a multisite WAN with centralized call-processing Cisco Unified Communications Manager deployment? (Source: Understanding Cisco Unified Communications Manager Deployment and Redundancy Options)

- A) IP WAN carries voice traffic but no call control signaling
- B) IP WAN is used for data only
- C) IP WAN carries voice traffic and call control signaling
- D) IP WAN carries no call control signaling for intrasite calls

Q11) Which Cisco Unified Communications Manager deployment model offers the highest scalability? (Source: Understanding Cisco Unified Communications Manager Deployment and Redundancy Options)

- A) multisite WAN with centralized call processing
- B) multisite WAN with distributed call processing
- C) single-site with one call-processing agent
- D) single-cluster with distributed call processing

- Q12) Which two of the following options are features of Cisco Unified Communications Manager clustering over the WAN? (Choose two.) (Source: Understanding Cisco Unified Communications Manager Deployment and Redundancy Options)
- A) feature extension to offices
 - B) robustness in high-delay environments
 - C) distributed administration
 - D) unified dial plan
 - E) highest scalability
- Q13) What is the maximum number of Cisco Unified Communications Manager nodes in a cluster, and how many servers can act as call-processing nodes? (Source: Understanding Cisco Unified Communications Manager Deployment and Redundancy Options)
- A) 18 nodes, 6 of them used for call processing
 - B) 18 nodes, 8 of them used for call processing
 - C) 20 nodes, 6 of them used for call processing
 - D) 20 nodes, 8 of them used for call processing
- Q14) Which of the following options is not an installation option of Cisco Unified Communications Manager Release 6.0? (Source: Installing and Upgrading Cisco Unified Communications Manager)
- A) basic install
 - B) Windows upgrade
 - C) network installation
 - D) upgrade during install
- Q15) Which of the following passwords is not set when doing a basic install on the first node? (Source: Installing and Upgrading Cisco Unified Communications Manager)
- A) Administrator password
 - B) Database Access Security password
 - C) Application User password
 - D) CAR Administrator password
- Q16) Which three of the following options can be used to retrieve an upgrade file when performing an upgrade during install? (Choose three.) (Source: Installing and Upgrading Cisco Unified Communications Manager)
- A) SFTP
 - B) HTTP
 - C) SMTP
 - D) TFTP
 - E) Local
 - F) FTP
 - G) XML

- Q17) Which of the following tools is used to export the data required for an upgrade from Cisco Unified CallManager Release 4.0 to Cisco Unified Communications Manager Release 6.0? (Source: Installing and Upgrading Cisco Unified Communications Manager)
- A) DMA
 - B) BARS
 - C) TAPS
 - D) DRS
- Q18) After upgrading from Cisco Unified CallManager Release 5.0 or higher, you have to _____ in order for the upgrade to become effective. (Source: Installing and Upgrading Cisco Unified Communications Manager)
- A) activate changes
 - B) enable upgrade
 - C) restart the server
 - D) restart the Cisco Unified Communications Manager service
 - E) switch versions

Module Self-Check Answer Key

- Q1) C, F
- Q2) B, C, D
- Q3) 2 GHz processor, 2 GB RAM and 72 GB hard disk
- Q4) A
- Q5) C, E
- Q6) An overdraft is a condition where more devices register to Cisco Unified Communications Manager than license units purchased. Cisco Unified Communications Manager allows a five percent overdraft.
- Q7) B
- Q8) A, C, E
- Q9) B
- Q10) C
- Q11) B
- Q12) A, D
- Q13) C
- Q14) C
- Q15) D
- Q16) A, E, F
- Q17) A
- Q18) E

Module 2

Administration of Cisco Unified Communications Manager

Overview

Performing system administration by configuring initial basic settings is the first important task when deploying Cisco Unified Communications Manager. In order to be able to administer Cisco Unified Communications Manager, it is important to know which user interfaces exist and when to use which one. Another important step of Cisco Unified Communications Manager administration is user management, optionally by integrating with Lightweight Directory Access Protocol (LDAP).

This module describes the different administration methods and features, provides information about how to access them, discusses the configuration of initial settings, and explains how to manage users in Cisco Unified Communications Manager.

Module Objectives

Upon completing this module, you will be able to perform Cisco Unified Communications Manager platform and general administration, initial configuration, and user management. This ability includes being able to meet these objectives:

- Describe the purpose and basic functionality of all Cisco Unified Communications Manager administrative options and be able to access and navigate between them
- Activate required Cisco Unified Communications Manager services, configure initial settings, and remove Domain Name System (DNS) reliance
- Manage user accounts, including integrating Cisco Unified Communications Manager with a corporate LDAP directory and enabling multiple levels of user privileges

Lesson 1

Understanding Cisco Unified Communications Manager Administration Options

Overview

Cisco Unified Communications Manager provides several interfaces, such as GUIs and command-line interface (CLI), to administer the Cisco Unified Communications Manager operating system and application. It also provides GUI access to user web pages. This lesson describes the available Cisco Unified Communications Manager administration and user interfaces.

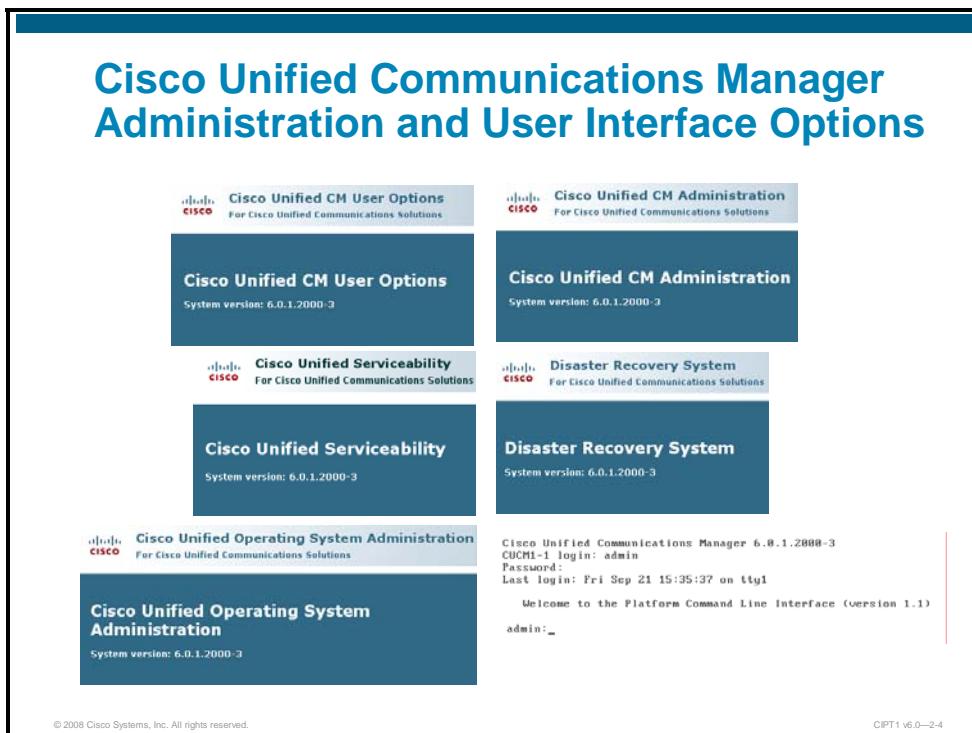
Objectives

Upon completing this lesson, you will be able to describe the purpose and basic functionality of all Cisco Unified Communications Manager administrative and user interfaces and be able to access and navigate between them. This ability includes being able to meet these objectives:

- Describe Cisco Unified Communications Manager administration and user interface options
- Describe how to access the Cisco Unified Communications Manager user web interface and which features it provides
- Describe how to access the Cisco Unified Communications Manager administration web interface and which features it provides
- Describe how to access the Cisco Unified Communications Manager serviceability web interface and which features it provides
- Describe how to access the Cisco Unified Communications Manager disaster recovery web interface and which features it provides
- Describe how to access the Cisco Unified Communications Manager operating system web interface and which features it provides
- Describe how to access the Cisco Unified Communications Manager CLI and which features it provides

Cisco Unified Communications Manager Administration and User Interfaces

This topic provides an overview about Cisco Unified Communications Manager administration and user interface options.



Since Release 5.0, Cisco Unified Communications Manager (formerly Cisco Unified CallManager) has been an appliance in which access to the system is only possible through Cisco Unified Communications Manager GUIs and the Cisco Unified Communications Manager CLI. The available interfaces are shown in the figure.

Cisco Unified Communications Manager Administration and User Interface Functions

The table describes the functions of Cisco Unified Communications Manager administration and user interfaces.

Cisco Unified Communications Manager Administration and User Interface Functions	
User Web Interface	Allows end users to customize their own IP phone settings, configuration, and features
Administration Web Interface	Allows Cisco Unified CM administrators to provision the system and to configure call routing, voice mail, devices, applications, end users, etc.
Serviceability Web Interface	Allows Cisco Unified CM administrators to control feature and network services, configure alarms, trace information, etc.
Disaster Recovery Web Interface	Allows platform administrators to perform or schedule Cisco Unified CM backup and restore tasks
Operating System Web Interface	Allows platform administrators to manage the Cisco Unified CM operating system
Administration CLI	Allows platform administrators to manage the Cisco Unified CM operating system via a CLI

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-5

There are five web interfaces:

User web interface: Allows end users to customize their own IP phone settings, configuration, and features.

Administration web interface: Allows Cisco Unified Communications Manager administrators to provision the system and to configure call routing, voice mail, devices, applications, end users, and so on.

Serviceability web interface: Allows Cisco Unified Communications Manager administrators to control feature and network services, to configure alarms and trace information, and so on.

Disaster Recovery web interface: Allows platform administrators to perform or schedule Cisco Unified Communications Manager backup and restore tasks.

Operating System web interface: Allows platform administrators to manage the Cisco Unified Communications Manager operating system.

In addition to these GUIs, there is also a CLI:

Administration CLI: Allows platform administrators to manage the Cisco Unified Communications Manager operating system via a CLI.

Cisco Unified Communications Manager User Web Interface

This topic describes the Cisco Unified Communications Manager user web interface.

User Web Interface Functions

Allows users to configure their IP phone to:

- Forward all calls to a different number
- Configure speed-dial numbers
- Subscribe to IP phone services
- Configure personal address book and fast dials
- Change message waiting lamp policy
- Change locale, password, and PIN

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-7

Cisco Unified Communications Manager allows the configuration of end-user accounts where each of them can be associated with one or more IP phones, which, in turn, allows end users to configure personal features for their IP phone(s). Such features include:

- **Forward all calls to a different number.**
- **Configure speed-dial numbers:** Most Cisco IP phone models have buttons that can be configured as speed dials. When the user hits such a button, the configured number is dialed. End users can freely configure the numbers assigned to the speed-dial buttons using the Cisco Unified Communications Manager user web interface.
- **Subscribe to IP phone services:** Most Cisco IP phone models can be used to access Extensible Markup Language (XML)-based web applications by so-called IP phone services. End users can freely subscribe (or unsubscribe) to IP phone services.
- **Configure personal address book and fast dials.**
- **Change message waiting lamp policy.**
- **Change locale, password, and PIN.**

Accessing the User Web Interface

The Cisco Unified Communications Manager user web interface is accessed by browsing to the URL shown in the figure.

Accessing the User Web Interface

- <https://server-address/ccmuser>
- Log in using the personal user account created by Cisco Unified Communications Manager Administrator



When accessing the Cisco Unified Communications Manager User web interface, the user has to log in with username and password. The end-user accounts are created by the Cisco Unified Communications Manager administrator.

Cisco Unified Communications Manager User Main Page

The figure shows the main page of the Cisco Unified Communications Manager user web interface.

The screenshot displays the Cisco Unified CM User Main Page. At the top, there's a header bar with the Cisco logo, the text "Cisco Unified CM User Options For Cisco Unified Communications Solutions", and navigation links for "User1", "About", and "Logout". A dropdown menu labeled "User Options" is open. Below the header is a main content area titled "Cisco Unified CM User Options" with the subtitle "System version: 6.0.1.2000-3". To the right of the title is a small image of a server room. The footer contains copyright information, a note about cryptographic features, and a link to U.S. export laws. At the very bottom, there are copyright and versioning details.

Cisco Unified CM User Options
For Cisco Unified Communications Solutions

User1 | About | Logout

User Options ▾

Cisco Unified CM User Options
System version: 6.0.1.2000-3

Copyright © 1999 - 2006 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wl/export/crypto/tool/starg.html>.
If you require further assistance please contact us by sending email to export@cisco.com.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-9

Cisco Unified Communications Manager Administration Web Interface

This topic describes the Cisco Unified Communications Manager Administration web interface.

Cisco Unified Communications Manager Administration Web Interface Functions

- **System configuration:** Cisco Unified Communications Manager groups, presence groups, device-mobility groups, device pools, regions, locations, phone security profile, etc.
- **Call routing configuration:** Dial rules, route patterns, call hunting, time-of-day routing, partitioning and CSS, intercom, call park, call pickup, etc.
- **Media Resource configuration:** Conference bridges, transcoders, MOH, MTPs, etc.
- **Voice-mail configuration**
- **Device configuration:** Gateways, gatekeepers, trunks, IP phones, etc.
- **Application configuration:** Manager, assistant, attendant console)
- **User management:** End users, application users, groups, and role configuration)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-11

The Cisco Unified Communications Manager Administration web interface provides the following functions:

- **System configuration:** Cisco Unified Communications Manager groups, presence groups, device-mobility groups, device pools, regions, locations, phone security profile, and so on
- **Call routing configuration:** Dial rules, route patterns, call hunting, time-of-day routing, partitioning and Calling Search Space (CSS), intercom, call park, call pickup, and so on
- **Media Resource configuration:** Conference bridges, transcoders, music on hold (MOH), Media Termination Points (MTPs), and so on
- **Voice-mail configuration**
- **Device configuration:** Gateways, gatekeepers, trunks, IP phones, and so on
- **Application configuration:** Manager, assistant, attendant console, and so on
- **User management:** End users, application users, groups, and role configuration

Accessing the Administration Web Interface

The Cisco Unified Communications Manager Administration web interface is accessed by browsing to the URL shown in the figure.

Accessing the Administration Web Interface

- <https://server-address/ccmadmin>
- Log in using Cisco Unified Communications Manager administrator account (created during installation)



© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-12

When accessing the Cisco Unified Communications Manager Administration web interface, the administrator has to log in with username and password. The initial administrator account is created during installation. Additional administrator accounts can be created from the Cisco Unified Communications Manager Administration web interface.

Cisco Unified Communications Manager Administration Main Page

The figure shows the main page of the Cisco Unified Communications Manager Administration web interface.

The screenshot displays the main page of the Cisco Unified Communications Manager Administration web interface. At the top, a blue header bar contains the text "Cisco Unified CM Administration Main Page". Below this, a navigation bar includes the Cisco logo, the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions", and links for "Navigation", "Cisco Unified CM Administration", "Go", "ccmadministrator", "About", and "Logout". A secondary navigation menu below the main one lists categories: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area features a dark blue banner with the text "Cisco Unified CM Administration" and "System version: 6.0.1.2000-3". To the right of the banner is a photograph of a server room. Below the banner, a copyright notice states: "Copyright © 1999 - 2006 Cisco Systems, Inc. All rights reserved." It also includes a legal disclaimer about cryptographic features and U.S. export laws, a link to the U.S. laws governing Cisco cryptographic products, and contact information for further assistance. At the bottom of the page, there are footer links for "Cisco Systems, Inc. All rights reserved." and "CIPT1 v6.0—2-13".

Cisco Unified Communications Manager Serviceability Web Interface

This topic describes the Cisco Unified Communications Manager Serviceability web interface.

Cisco Unified Communications Manager Serviceability Web Interface Functions

Allows Cisco Unified Communications Manager administrators to complete these tasks:

- Configure alarms and logs
- Configure traces
- Configure CDR disk storage and external billing servers
- Activate, deactivate, start, stop, and restart network and feature services
- Configure SNMP settings
- Configure serviceability reports

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-15

The Cisco Unified Communications Manager Serviceability web interface provides the following functions:

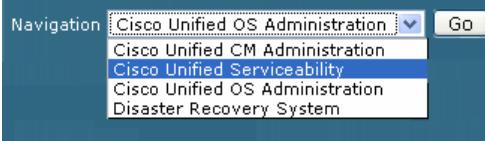
- **Configure alarms, logs, and traces:** For monitoring and troubleshooting Cisco Unified Communications Manager.
- **Configure Call Detail Records (CDRs) disk storage and external billing servers:** Cisco Unified Communications Manager has the ability to create CDRs and Call Management Records (CMRs) providing detailed information about call activities and voice quality. Using Cisco Unified Communications Manager Serviceability, an administrator can limit the disk space used for these records and configure Cisco Unified Communications Manager to copy or move these files containing CDRs and CMRs to external billing servers using the Secure FTP (SFTP).
- **Activate, Deactivate, start, stop, and restart network and feature services.**
- **Configure Simple Network Management Protocol (SNMP) settings.**
- **Configure serviceability reports:** These reports are automatically created nightly and allow system (including trend) analysis based on monitored objects. A Cisco Unified Communications Manager administrator can obtain the generated reports from Cisco Unified Communications Manager Serviceability web pages.

Accessing the Serviceability Web Interface

The Cisco Unified Communications Manager Serviceability web interface is accessed by browsing to the URL shown in the figure.

Accessing the Serviceability Web Interface

- <https://server-address/ccmService>
- or access from the navigation shortcut:



- Log in using Cisco Unified Communications Manager administrator account (created during installation)



When accessing the Cisco Unified Communications Manager serviceability web interface, the administrator has to log in with username and password. The initial administrator account (created during installation) or any administrator account (created from Cisco Unified Communications Manager Administration web interface) can be used.

Note

All administrative Cisco Unified Communications Manager GUIs include a Navigation shortcut on the top right corner of the screen. The drop-down list can be used to access the desired GUI directly instead of entering the corresponding URL.

Cisco Unified Communications Manager Serviceability Main Page

The figure shows the main page of the Cisco Unified Communications Manager Serviceability web interface.

The screenshot displays the main interface of the Cisco Unified Communications Manager Serviceability. At the top, a blue header bar features the title "Cisco Unified Communications Manager Serviceability Main Page". Below the header, a navigation menu includes links for "Navigation", "Cisco Unified Serviceability", "Go", "ccmadministrator", "About", and "Logout". A secondary navigation bar at the top has dropdown menus for "Alarm", "Trace", "Logs", "Snmp", and "Help", with "Logs" currently selected. The main content area is titled "Cisco Unified Serviceability" and displays the system version "System version: 6.0.1.2000-3". To the right of the text is a small thumbnail image of a server room. At the bottom of the page, there is a copyright notice: "Copyright © 1999 - 2006 Cisco Systems, Inc. All rights reserved." and a legal disclaimer about cryptographic features. The footer contains the text "© 2008 Cisco Systems, Inc. All rights reserved." and "CIPT1 v6.0-2-17".

Cisco Unified Communications Manager Disaster Recovery Web Interface

This topic describes the Cisco Unified Communications Manager Disaster Recovery web interface.

Cisco Unified CM Disaster Recovery Web Interface Functions

- Provide a user interface for backup and restore tasks
- Write backups to a physical tape drive or remote SFTP server
- Support full cluster backups
- Support ad-hoc backup and restore jobs
- Support scheduled backups

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-19

The Cisco Unified Communications Manager Disaster Recovery web interface provides access to the Cisco Unified Communications Manager Disaster Recovery System (DRS), which offers the following functions:

- Writes backups to a physical tape drive or remote SFTP server
- Supports full cluster backups
- Supports ad-hoc backup and restore jobs
- Supports scheduled backups

Note More information about DRS is provided in the *Troubleshooting Cisco Unified Communications Systems* (TUC) course.

Accessing the Disaster Recovery Web Interface

The Cisco Unified Communications Manager DRS is accessed by browsing to the URL shown in the figure.

Accessing the Disaster Recovery Web Interface

- <https://server-address/drif>
- or access from the navigation shortcut:



- Log in using platform administrator account (created during installation)



When accessing the Cisco Unified Communications Manager DRS web interface, the platform administrator has to log in with username and password. The initial platform administrator account is created during installation. Additional platform administrator accounts can be created from the Cisco Unified Communications Manager CLI.

Note	From an authorization perspective, Cisco Unified Communications Manager administration is split into two parts by default: The Cisco Unified Communications Manager administrator account is used to access Cisco Unified Communications Manager Administration and Cisco Unified Communications Manager Serviceability web pages, whereas the Cisco Unified Communications Manager platform administrator account is used to access Cisco Unified Communications Manager DRS and Cisco Unified Communications Manager Operating System web pages and the Cisco Unified Communications Manager CLI.
-------------	---

Cisco Unified Communications Manager Disaster Recovery Main Page

The figure shows the main page of the Cisco Unified Communications Manager DRS web interface.

The screenshot displays the main page of the Cisco Unified Communications Manager Disaster Recovery System. At the top, a blue header bar contains the title "Cisco Unified CM Disaster Recovery Main Page". Below the header is a navigation bar with links for "Navigation", "Disaster Recovery System", "admin", "About", and "Logout". A yellow menu bar at the top left includes "Backup", "Restore", and "Help". The main content area has a dark blue background. It features the "Disaster Recovery System" logo and the text "System version: 6.0.1.2000-3". To the right of the text is a photograph of a server room. At the bottom of the page, there is a copyright notice, a legal disclaimer about cryptographic features, and a summary of U.S. laws governing Cisco cryptographic products. The footer contains the text "© 2008 Cisco Systems, Inc. All rights reserved." and "CIPT1 v6.0—2-21".

Cisco Unified Communications Manager Operating System Web Interface

This topic describes the Cisco Unified Communications Manager Operating System web interface.

Cisco Unified CM Operating System Web Interface Functions

Allows platform administrators to configure and manage the Cisco Unified Communications Manager operating system. Here are examples of operating system administration tasks:

- Check software and hardware status
- Upgrade system software and install or upgrade options
- View or update IP addresses
- Manage NTP servers
- Manage server security, including IPsec and certificates
- Ping other network devices
- Manage remote support (TAC) accounts

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-23

The Cisco Unified Communications Manager Operating System web interface allows platform administrators to configure and manage the Cisco Unified Communications Manager Operating System. Examples of operating system administration tasks include the following:

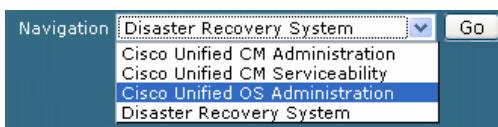
- Check software and hardware status
- Upgrade system software and install or upgrade options
- View or update IP addresses
- Manage Network Time Protocol (NTP) servers
- Manage server security, including IP Security (IPsec) configuration and certificates
- Ping other network devices
- Manage remote support (Cisco Technical Assistance Center [TAC]) accounts

Accessing the Cisco Unified Communications Manager Operating System Web Interface

The Cisco Unified Communications Manager Operating System web interface is accessed by browsing to the URL shown in the figure.

Accessing the Operating System Web Interface

- <https://server-address/cmplatform>
- or access from the navigation shortcut:



- Log in using platform administrator account (created during installation)



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-24

When accessing the Cisco Unified Communications Manager Operating System web interface, the platform administrator has to log in with username and password. The initial platform administrator account (created during installation) or any platform administrator account (created from the Cisco Unified Communications Manager CLI) can be used.

Cisco Unified Communications Manager Operating System Main Page

The figure shows the main page of the Cisco Unified Communications Manager Operating System Administration web interface.

The screenshot displays the main page of the Cisco Unified Communications Manager Operating System Administration web interface. At the top, a blue header bar contains the text "Cisco Unified CM Operating System Main Page". Below the header, a navigation bar includes links for "Cisco Unified Operating System Administration", "Navigation", "Cisco Unified OS Administration", "Go", "admin", "About", and "Logout". A secondary navigation menu below the main one has items: Show ▾, Settings ▾, Security ▾, Software Upgrades ▾, Services ▾, and Help ▾. The main content area features a dark blue banner with the text "Cisco Unified Operating System Administration" and "System version: 6.0.1.2000-3". To the right of the banner is a photograph of a server room. At the bottom of the page, there is a copyright notice: "Copyright © 1999 - 2006 Cisco Systems, Inc. All rights reserved." and a legal disclaimer about cryptographic features. The footer also includes the text "CIPT1 v6.0—2-25".

Cisco Unified Communications Manager Administration CLI

This topic describes the Cisco Unified Communications Manager CLI.

Cisco Unified Communications Manager Administration CLI Functions

Allows platform administrators to complete these tasks:

- Display platform information such as, product version, CPU, memory, disk usage, platform hardware, serial number, etc.
- Display network, process, and load information
- Configure additional platform administrator accounts
- Change platform administrator account and security passwords
- Perform disaster recovery tasks
- Use tools such as ping, traceroute, and packet capture
- Change network configuration settings
- Start, stop, and restart services
- Perform system restarts, shutdowns, and switch versions

© 2008 Cisco Systems, Inc. All rights reserved.

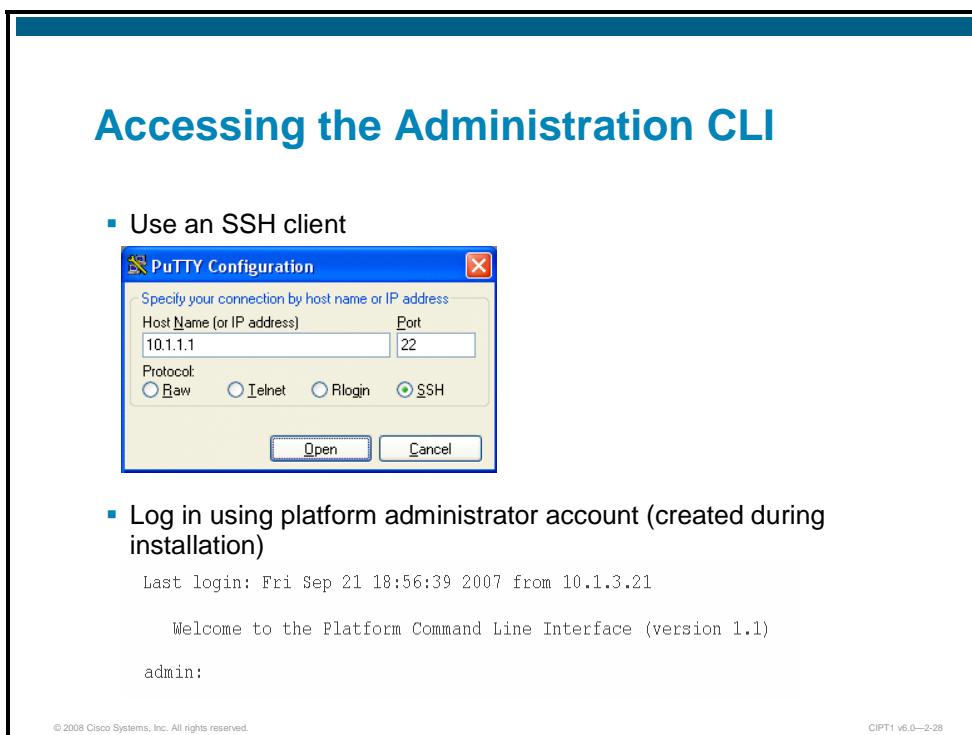
CIPT1 v6.0—2-27

The Cisco Unified Communications Manager CLI provides similar features to those that platform administrators can find in the Cisco Unified Communications Manager operating system and Cisco Unified Communications Manager DRS GUI; it also includes some additional functions:

- Displays platform information, such as product version, CPU, memory, disk usage, platform hardware, serial number, and so on
- Displays network, process, and load information
- Configures additional platform administrator accounts
- Changes platform administrator account password and security passwords
- Performs disaster recovery tasks
- Uses tools such as ping, traceroute, and packet capture
- Changes network configuration settings
- Offers start, stop, and restart services
- Performs system restarts, shutdowns, and switch versions

Accessing the Administration CLI

The Cisco Unified Communications Manager CLI is accessed from a Secure Shell (SSH) client or from the physical console of the system.



When accessing the Cisco Unified Communications Manager CLI, the platform administrator has to log in with username and password. The initial platform administrator account (created during installation) or any platform administrator account (created from the Cisco Unified Communications Manager CLI) can be used.

Note	When accessing the CLI over the network, an SSH client has to be used, because Telnet is not supported.
-------------	---

Cisco Unified Communications Manager Administration CLI Main Page

The figure shows some top-level commands of the Cisco Unified Communications Manager CLI.

Cisco Unified Communications Manager Administration CLI Main Page

```
admin:?
    help
    quit
    show*
    set*
    delete*
    unset*
    file*
    utils*
    run*

admin:show ?
    show status
    show logins
    show hardware
    show workingdir
    show web-security
    show smtp
    show myself
    show account
    show registry
    show trace
    show ups*
    show environment*
    show memory*
    show open*
    show timezone*
    show cert*
    show ipsec*
    show version*
    show packages*
```

```
admin:?
    help
    quit
    show*
    set*
    delete*
    unset*
    file*
    utils*
    run*

admin:show ?
    show status
    show logins
    show hardware
    show workingdir
    show web-security
    show smtp
    show myself
    show account
    show registry
    show trace
    show ups*
    show environment*
    show memory*
    show open*
    show timezone*
    show cert*
    show ipsec*
    show version*
    show packages*
```

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-29

When using the Cisco Unified Communications Manager CLI the ? can be used to see the available commands or command options. In the first example shown in the figure, the ? is used at the top level, and as a result, all top-level commands have been displayed. In the second example, the command **show ?** is entered, and therefore, all available show commands have been displayed. Finally, all utility commands have been displayed because of the entered **utils ?** command.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- The User web interface allows end users to customize their own IP phone settings, configuration, and features.
- The Administration web interface allows Cisco Unified CM administrators to provision the system and to configure call routing, voice mail, devices, applications, end users, etc.
- The Serviceability web interface allows Cisco Unified CM administrators to control the feature and network services, to configure alarms and traces, etc.
- The Disaster Recovery web interface allows Cisco Unified CM platform administrators to perform or schedule Cisco Unified CM backup and restore tasks.
- The Operating System web interface allows Cisco Unified CM platform administrators to manage the Cisco Unified CM operating system.
- The Administration CLI allows Cisco Unified CM platform administrators to manage the Cisco Unified CM operating system and to perform backup and restore tasks from a CLI.

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager – Maintain and Operate Guides
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Lesson 2

Managing Services and Initial Configuration of Cisco Unified Communications Manager

Overview

Cisco Unified Communications Manager configuration includes basic settings plus specific settings that depend on the features and services used. This lesson describes how basic settings on Cisco Unified Communications Manager are configured in order to enable the system and prepare Cisco Unified Communications Manager for endpoint deployment.

Objectives

Upon completing this lesson, you will be able to activate required Cisco Unified Communications Manager services and settings to enable features and remove Domain Name System (DNS) reliance. This ability includes being able to meet these objectives:

- List elements used for general, initial configuration
- List network configuration options of Cisco Unified Communications Manager
- List the reasons for using Network Time Protocol (NTP) servers and enabling DHCP services in Cisco Unified Communications Manager
- Describe the reliance on DNS by IP phones when server names are used instead of server IP addresses
- Describe the difference between network and feature services and explain how they can be managed using Cisco Unified Communications Manager serviceability
- Describe the purpose of enterprise parameters and explain key parameters
- Describe the purpose of service parameters and explain key parameters

Cisco Unified Communications Manager Initial Configuration

This topic provides an overview about Cisco Unified Communications Manager initial configuration.

Cisco Unified Communications Manager Initial Configuration

Configure network settings	NTP servers, DHCP services, remove DNS reliance
Verify network and Feature services	Activate the necessary feature services and check network services
Configure enterprise parameters	Modify enterprise parameters as required
Configure service parameters	Modify service parameters as required

© 2008 Cisco Systems, Inc. All rights reserved.

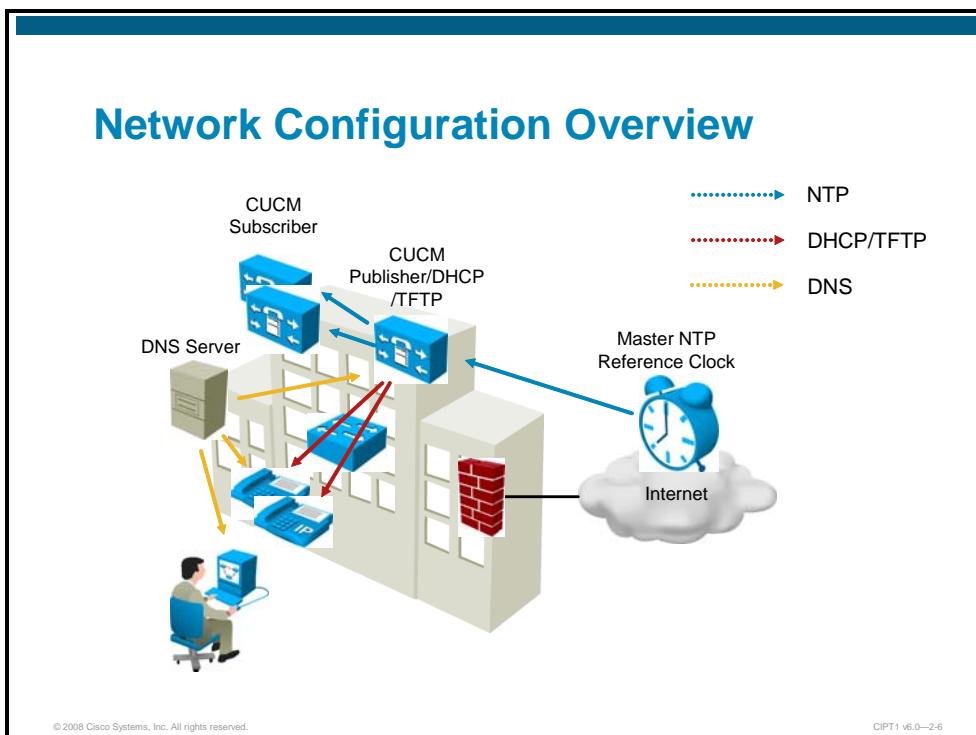
CIPT1 v6.0—2-4

After installing Cisco Unified Communications Manager, some initial configuration has to be done before starting to deploy endpoints. This initial configuration includes:

- **Configure network settings:** Basic network settings have already been configured during installation. However, some of them should be revisited (for example, use of external NTP and DNS servers), and network settings that are not configurable during installation (for example, enabling DHCP services on Cisco Unified Communications Manager) have to be addressed before endpoint deployment.
- **Verify network and feature services:** Cisco Unified Communications Manager servers run network services (automatically activated) and feature services (activated by the administrator). After installation, network services should be checked, and desired feature services have to be activated.
- **Configure enterprise parameters:** Cisco Unified Communications Manager has cluster-wide configuration settings called enterprise parameters. After installation, enterprise parameter default values should be verified and modified, if required.
- **Configure service parameters:** Cisco Unified Communications Manager services have configurable parameters that can usually be set per Cisco Unified Communications Manager server. After installation and service activation, service parameter default values should be verified and modified, if required.

Cisco Unified Communications Manager Network Configuration Options

This topic describes network configuration options that should be evaluated after installation and before endpoint deployment.



Cisco Unified Communications Manager network configuration options include the use of external NTP and DNS servers and the ability to provide DHCP and TFTP services to endpoints.

Network Components

This section describes the function of network components used or provided by Cisco Unified Communications Manager.

Network Components	
Master NTP reference clock	NTP stratum 1 server, directly connected to radio receivers or atomic clocks. Alternatively, a Cisco router can be configured as a master NTP server. The Cisco Unified Communications Manager. Publisher is the NTP client.
DHCP and TFTP server	DHCP server provides IP address configuration and TFTP server location to the IP phones. TFTP server provides device configuration files, ringer files, and firmware upgrades to the IP phones. A Cisco Unified CM server (typically publisher) can provide both the DHCP and TFTP services.
DNS server	Provides hostname to IP address resolution to the IP phones and user PCs.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-7

The NTP is a protocol for synchronizing the clocks of computer systems over IP networks. It has a hierarchical organization by the use of clock strata. Stratum 0 is an extremely precise clock source, such as an atomic clock or radio clock. A stratum 1 server is directly connected to a stratum 0 clock and can provide time information to other (stratum 2) devices, which themselves can serve stratum 3 devices.

Cisco Unified Communications Manager can use NTP to obtain time information from a time server (typically stratum 1). Only the publisher will send NTP requests to the external NTP server(s); subscribers will synchronize their time with the publisher. The configuration of an external NTP server is not required; if no NTP server is configured, the publisher will rely on its own system time.

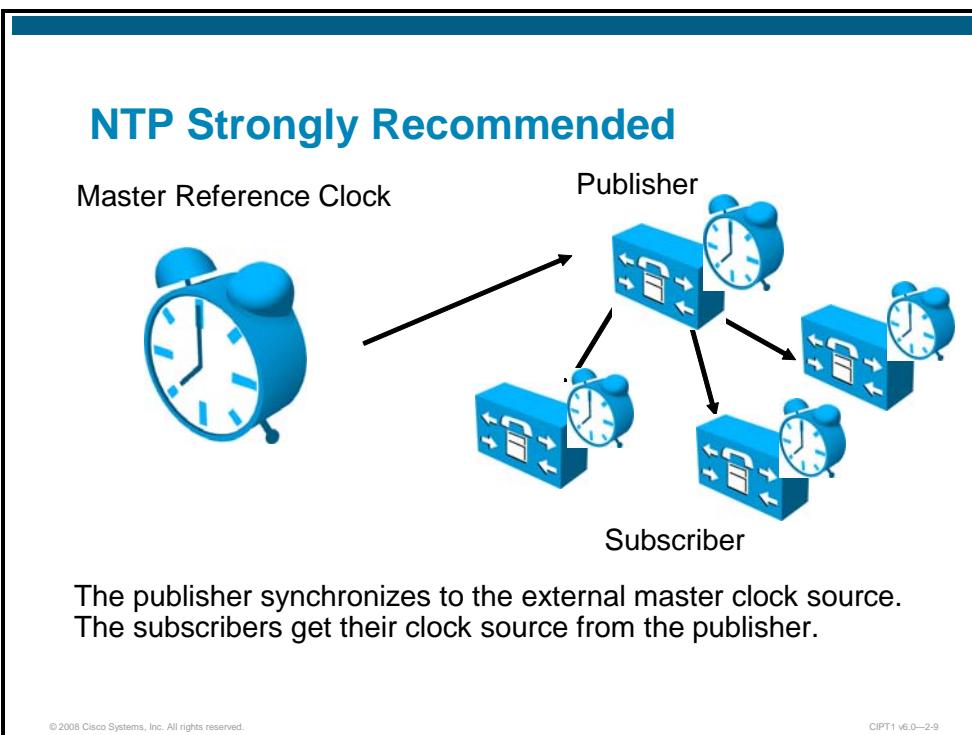
DHCP is a protocol that allows IP endpoints to obtain their IP settings from a server. The most important settings are IP address, subnet mask, and default gateway. In addition, the DNS server address and special functions, such as the TFTP server address used by Cisco IP phones, can be assigned to the client. Cisco Unified Communications Manager features a DHCP server, designed to serve Cisco IP phones only.

TFTP is a simple file transfer protocol and is used by Cisco IP phones to obtain configuration files and their software. A Cisco Unified Communications Manager cluster has to run the TFTP service at least on one server to be able to support Cisco IP phones.

DNS is a name resolution protocol that allows IP applications to refer to other systems by logical names instead of IP addresses. A Cisco Unified Communications Manager cluster can be configured to use either DNS or IP addresses.

Cisco Unified Communications Manager NTP and DHCP Considerations

This topic describes how to change NTP configuration in Cisco Unified Communications Manager.



NTP can be enabled and configured during installation. However, sometimes the decision to use or to not use external NTP servers is not considered properly during that time, and therefore should be reconsidered before deploying endpoints.

It is extremely important that all network devices have accurate time information, as the system time of Cisco Unified Communications Manager is relevant in the following situations:

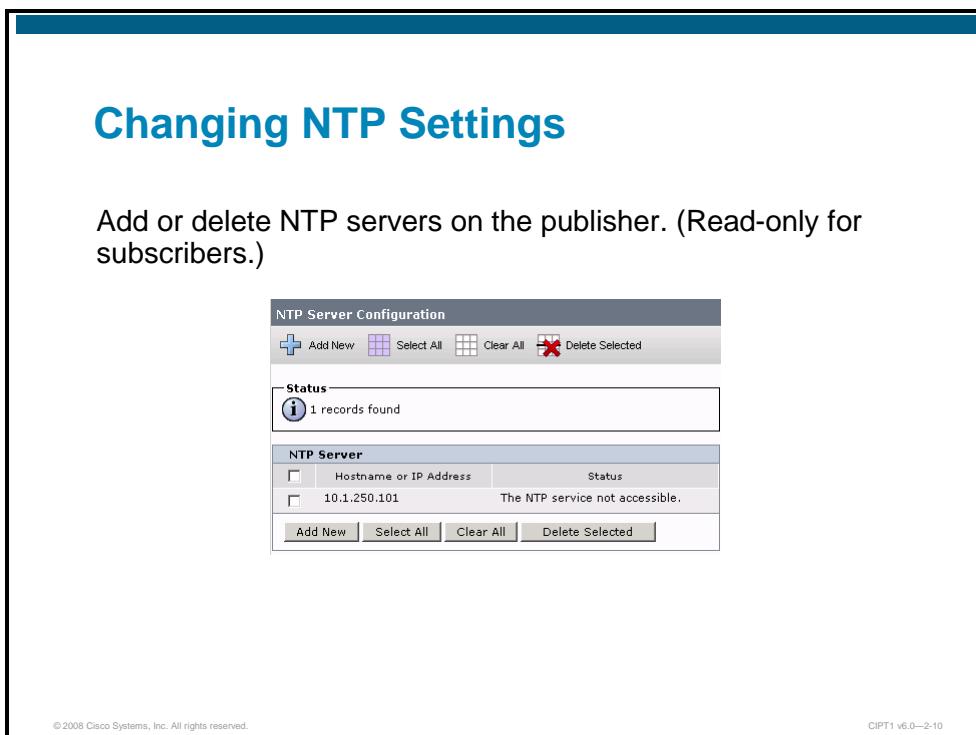
- Cisco IP phones display date and time information; this information is obtained from Cisco Unified Communications Manager.
- Call Detail Records (CDR) and Call Management Record (CMR), which are used for call reporting, analysis, and billing, include date and time information.
- Alarms and events in log files, as well as trace information in trace files include time information. Troubleshooting a problem requires correlation of information created by different system components (Cisco Unified Communications Manager, Cisco IOS gateway, and so on). This problem-solving is only possible if all devices in the network have the same correct time information.
- Some Cisco Unified Communications Manager features are date- or time-based, and therefore rely on correct date and time. These features include time-of-day routing and certificate-based security features.

Note	Certificates include a validity period. If a system that receives a certificate has an invalid (future) date, it may consider the received certificate to be invalid (expired).
-------------	---

To ensure that all network devices have correct date and time, it is recommended that all network devices (including Cisco Unified Communications Manager) use NTP for time synchronization. The master reference clock should be a stratum 1 NTP server.

Changing NTP Settings

This section describes how to change NTP configuration in Cisco Unified Communications Manager.



The screenshot shows the 'NTP Server Configuration' page. At the top, there are buttons for 'Add New', 'Select All', 'Clear All', and 'Delete Selected'. Below this is a status message: 'Status' with '1 records found'. A table follows, with columns 'Hostname or IP Address' and 'Status'. It contains one row with the IP '10.1.250.101' and the status 'The NTP service not accessible.' At the bottom are buttons for 'Add New', 'Select All', 'Clear All', and 'Delete Selected'.

To modify NTP configuration in Cisco Unified Communications Manager, use Cisco Unified Operating System Administration web pages and go to **Settings > NTP Servers**. There you can add, delete, and modify NTP servers.

DHCP Server Feature Support

This section describes DHCP server support in Cisco Unified Communications Manager.

DHCP Server Feature Support

- DHCP server in Cisco Unified CM is designed to serve IP phones.
 - Provides a subset of Windows 2000 Server DHCP functionality.
 - Sufficient for IP phone purposes.
 - Not designed to serve other network devices (PCs, etc.).
 - Only for smaller deployments (up to 1000 IP phones).
- Only one DHCP server per Cisco Unified Communications Manager cluster.
 - DHCP server is a standalone server.
 - No backup server exists.
- Multiple subnets can be configured for each server.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-11

The Cisco Unified Communications Manager DHCP server is designed to serve IP phones in small deployments (maximum of 1000 devices). It provides a subset of Windows 2000 Server DHCP functionality that is sufficient for IP phones, but it should not be used for other network devices (such as PCs, and so on).

Note	The DHCP server of Cisco Unified Communications Manager must not be used with deployments of more than 1000 registered devices. Even if there are fewer devices, the CPU load of the services has to be watched closely, and if high CPU load is experienced, the DHCP service should be provided by other devices (for example, dedicated DHCP server, switch, router, and so on).
-------------	---

Only one DHCP server can be configured per Cisco Unified Communications Manager cluster; no backup configuration is possible.

The Cisco Unified Communications Manager DHCP server can be configured with multiple subnets. In non-attached subnets, DHCP relay must be enabled so that the DHCP requests that were sent out by the clients are forwarded to the DHCP server.

Steps to Configure DHCP Phone Support

This slide shows the configuration procedure to enable DHCP services in Cisco Unified Communications Manager.

Steps to Configure DHCP Phone Support

1. Activate DHCP Monitor Service.
2. Add and configure the DHCP server.
3. Configure the DHCP subnets.

Step 1: Activate DHCP Monitor Service

The DHCP server function is enabled by activating the DHCP Monitor Service.

Service Name	Activation
Cisco CallManager	Activated
Cisco Tftp	Activated
Cisco Messaging Interface	Deactivated
Cisco Unified Mobile Voice Access Service	Activated
Cisco IP Voice Media Streaming App	Activated
Cisco CTIManager	Activated
Cisco Extension Mobility	Activated
Cisco Extended Functions	Activated
Cisco Dialed Number Analyzer	Activated
Cisco DHCP Monitor Service	Activated

Activate the DHCP Monitor Service from **Cisco Unified Communications Manager Serviceability > Tools > Service Activation**.

Step 2: Configure the DHCP Server

Global DHCP server configuration is done from **Cisco Unified Communications Manager Administration > System > DHCP Server Configuration**.

Step 2: Configure the DHCP Server

DHCP Server Configuration

Status: Status: Ready

DHCP Server Information

Host Server*	10.96.128.200
Primary DNS IP Address	
Secondary DNS IP Address	
Primary TFTP Server IP Address(Option 150)	10.96.128.200
Secondary TFTP Server IP Address(Option 150)	
Bootstrap Server IP Address	
Domain Name	
TFTP Server Name(Option 66)	
ARP Cache Timeout(sec)*	0
IP Address Lease Time(sec)*	0
Renewal(T1) Time(sec)*	0
Rebinding(T2) Time(sec)*	0

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-14

DHCP server configuration includes the selection of the Cisco Unified Communications Manager cluster member that should run the DHCP service (drop-down list) and general (default) parameters, such as DNS and TFTP server addresses.

Step 3: Configure the DHCP Subnet

DHCP scopes (that is, IP address ranges for a certain subnet) are configured from **Cisco Unified Communications Manager Administration > System > DHCP Subnet Information**.

The screenshot shows the 'Step 3: Configure the DHCP Subnet' page. On the left, three callout boxes point to specific configuration fields:

- A box labeled "Choose the DHCP server." points to the "DHCP Server*" field, which is set to "10.96.128.200".
- A box labeled "Configure subnet number and primary address range to be provided to the phones." points to the "Subnet IP Address*", "Primary Start IP Address*", and "Primary End IP Address*" fields, all set to "10.96.128.0", "10.96.128.11", and "10.96.128.99" respectively.
- A box labeled "Configure secondary address range as necessary (useful if you have a block of reserved addresses to exclude between primary and secondary range)." points to the "Secondary Start IP Address", "Secondary End IP Address", and "Subnet Mask*" fields, all set to blank, and the "Domain Name", "Primary DNS IP Address", and "Secondary DNS IP Address" fields, all set to blank.

On the right, there are additional configuration fields for TFTP, Bootstrap, and lease times, all set to their default values (0 or blank). At the bottom of the page, copyright and version information are present.

Cisco Unified Communications Manager DHCP Subnet Information configuration includes the selection of the DHCP server, the network ID of the subnet, up to two continuous IP address ranges (to allow excluded ranges in-between), subnet mask, default gateway, and all parameters for which the defaults have been set under **Cisco Unified Communications Manager Administration > System > DHCP Server Configuration**.

DHCP Migration Considerations

This section provides information to be considered when upgrading from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager Release 5.x or Release 6.x.

DHCP Migration Considerations

When upgrading from Cisco Unified CM Release 4.x to 6.0:

- No migration provided from Windows 2000-based DHCP configuration to appliance-based DHCP configuration
- Reprovisioning of the DHCP service required
 - Using Cisco Unified Communications Manager Release 6.0 server
 - Using the DHCP Server feature on the Cisco IOS router or switch
 - Use third-party DHCP servers

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-16

In Cisco Unified CallManager Release 4.x, DHCP services were able to be provided by the Windows-based operating system of Cisco Unified CallManager. If the Windows DHCP server was used with Cisco Unified CallManager Release 4.x, and the system is upgraded to Cisco Unified Communications Manager Release 5.x or Release 6.x, all DHCP configuration is lost. Cisco Data Migration Assistant (DMA) does not transfer Windows DHCP configuration, but only configuration related to Cisco Unified Communications Manager. Therefore, in such a scenario, reprovisioning of the DHCP service is required. It can be configured on a Cisco Unified Communications Manager Release 5.x or Release 6.x server (assuming that there are no more than 1000 devices registering to Cisco Unified Communications Manager) or deployed on network devices (such as switches or routers) or on dedicated DHCP servers.

DNS Reliance of IP Phones

This topic describes the advantages and disadvantages of using IP addresses versus DNS.

IP vs. DNS Considerations

Cisco Unified Communications Manager Release 6.0 can use DNS names (default) or IP addresses for system addressing.

Advantages of using IP addresses	Advantages of using DNS
Does not require a DNS server	Simplifies management because of the use of names instead of numbers
Prevents the IP telephony network from failing if the IP phones lose connection to the DNS server	Easier IP address changes because of name-based IP paths
Decreases the amount of time required when a device attempts to contact the Cisco Unified CM server	Server to IP phone NAT possible
Simplifies troubleshooting	

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-18

Cisco Unified Communications Manager can either use IP addresses or names to refer to other IP devices in application settings. When names are used, they need to be resolved to IP addresses by DNS.

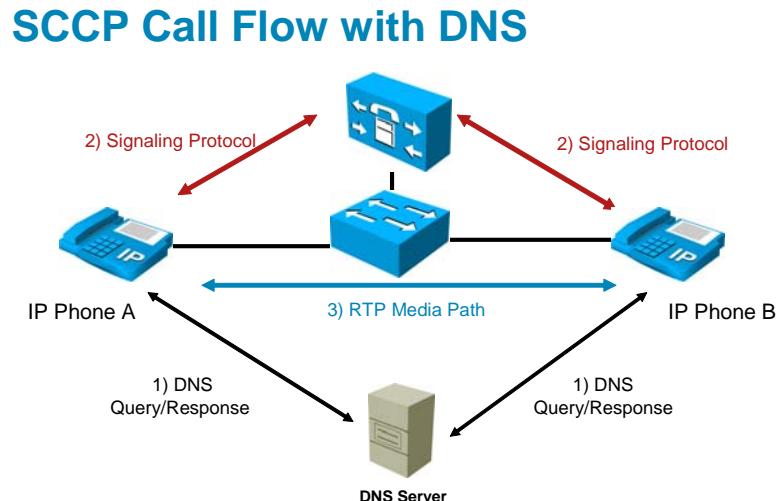
Both methods have some advantages:

- **Using IP addresses:** The system does not depend on a DNS server, which prevents loss of service when the DNS server cannot be reached. When a device initiates a connection, the time required to establish the connection is shorter because no name resolution (DNS lookup sent to the DNS server, and DNS reply sent back from the server) is required. By eliminating the need of DNS, there is no danger of errors caused by DNS misconfiguration. Troubleshooting is simplified because there is no need to verify proper name resolution.
- **Using DNS:** Management is simplified because logical names are simpler to handle than 32-bit addresses. If IP addresses change, there is no need to modify the application settings as they can still use the same names; only the DNS server configuration has to be modified in this case. IP addresses of Cisco Unified Communications Manager servers can be translated towards IP phones, as the IP phone configuration files do not include the original server IP address (which should appear differently to the IP phone) but server names. As long as these names are resolved to the correct (translated) address when DNS requests have been sent out by IP phones, the Network Address Translation (NAT) is no problem.

In general, due to the additional point of failure caused by configuration errors or because of unavailability of the service, the recommendation is not to use DNS with Cisco Unified Communications Manager.

SCCP Call Flow with DNS

The figure illustrates a call between IP phones where DNS is used.



Before sending packets, IP phones will query the DNS server to resolve the IP address of the Cisco Unified CM server.

© 2008 Cisco Systems, Inc. All rights reserved.

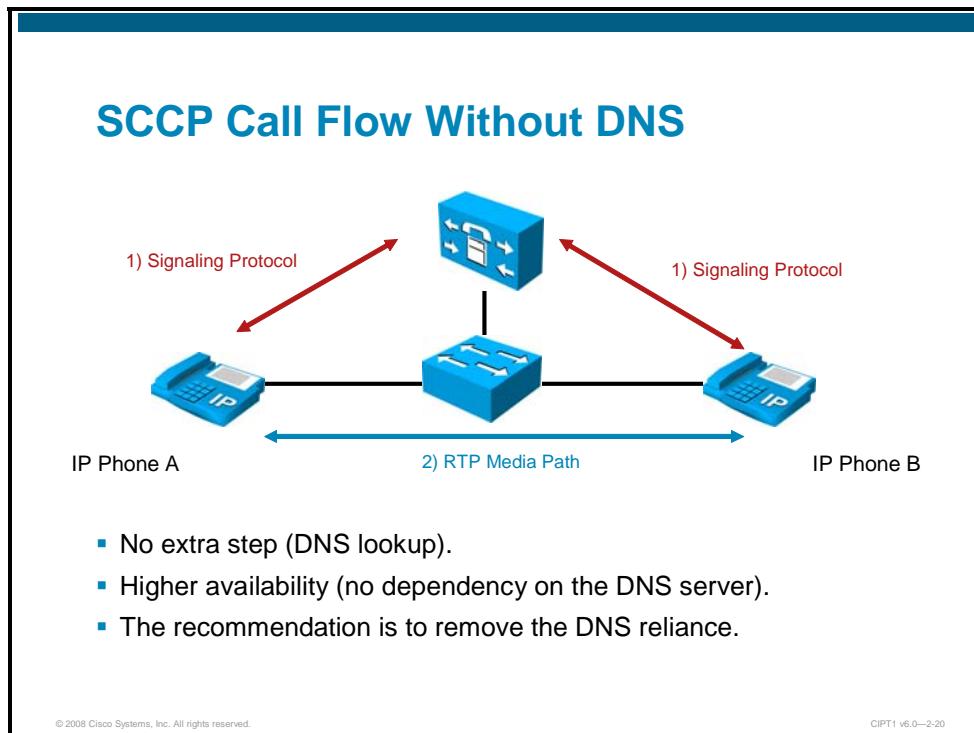
CIPT1 v6.0—2-19

Before the IP phone can communicate with Cisco Unified Communications Manager, it has to resolve the name of the server (obtained from the configuration file which was downloaded from a TFTP server). Only then can signaling messages be exchanged between the IP phone and Cisco Unified Communications Manager.

Note SCCP = Skinny Client Control Protocol

SCCP Call Flow Without DNS

The figure illustrates a call between IP phones where DNS is not used.



When IP addresses are used instead of DNS names for the Cisco Unified Communications Manager servers, the need for the extra step of DNS resolution is eliminated. The signaling session can be set up immediately, and calls can be processed even if the DNS service is not available. Therefore, the recommendation is to remove DNS reliance.

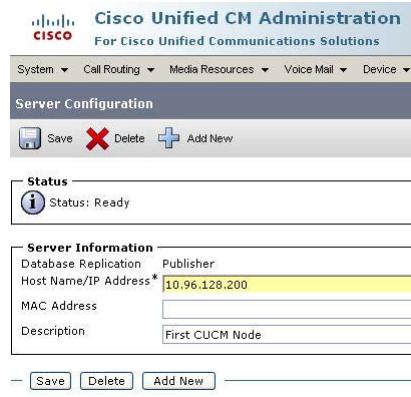
Removing DNS Reliance

This section describes the procedure to remove DNS reliance.

Removing DNS Reliance

Enables Cisco IP phones and other devices controlled by Cisco Unified CM to contact the Cisco Unified CM without resolving a DNS name

1. In Cisco Unified CM Administration, choose **System > Server**. The Find and List Servers window appears.
2. Click on a server name. The Server Configuration window appears.
3. Replace the hostname and enter the IP address of the server in the Host Name/IP Address field. Click **Save**.



In order to change the default behavior of using DNS, perform these steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **System > Server**.
- Step 2** Select the first (next) available server from the list of Cisco Unified Communications Manager servers.
- Step 3** Change the server name to the IP address of the server and save the changes.

Note Repeat steps 2 and 3 for each server in the cluster.

Note By default, hostnames are also used in phone URLs. When removing DNS reliance, hostnames used in these phone URLs also have to be replaced by IP addresses. Phone URLs are configured by so-called enterprise parameters. Enterprise parameters and their configuration are explained in a later topic of this lesson.

Cisco Unified Communications Manager Network and Feature Services

This topic describes Cisco Unified Communications Manager network and feature services.

Network and Features Services

Network Services	Feature Services
Services required for the Cisco Unified CM system to function; for example, database and platform services.	Services that enable certain Cisco Unified CM application features; for example, TFTP, call processing, or serviceability reports.
Automatically activated after Cisco Unified CM installation. Cannot be activated or deactivated.	Must be activated manually using Unified CM Serviceability > Service Activation .
Use Unified CM Serviceability > Control Center > Network Services to stop, start, or restart services.	Use Unified CM Serviceability > Control Center > Feature Services to stop, start, or restart services.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-23

A Cisco Unified Communications Manager cluster can consist of up to 20 servers. Each server can fulfill different tasks, such as running a TFTP or DHCP server, being the database publisher, processing calls, providing media resources, and so on.

Depending on the usage of a server, different services have to be activated on the system. There are two types of services on Cisco Unified Communications Manager servers:

- **Network services:** These services are automatically activated and are required for the operation of the server. Network services cannot be activated or deactivated by the administrator, but they can be stopped, started or restarted from **Cisco Unified Communications Manager Serviceability > Control Center > Network Services**. Examples for network services are Cisco CDP, A Cisco DB Replicator, and Cisco CallManager Admin services.
- **Feature services:** These services can be selectively activated or deactivated per server in order to assign specific tasks or functions (such as call processing, TFTP, and so on) to a certain server. Feature services can be activated and deactivated by the administrator using **Cisco Unified Communications Manager Serviceability > Service Activation**. They can be started or restarted from **Cisco Unified Communications Manager Serviceability > Control Center > Feature Services**. Examples for feature services include Cisco CallManager, Cisco Tftp, and Cisco CallManager Attendant Console Server services.

Network Services

The slide shows a list of network services categorized in groups.

Network Services

Categorized into the following groups:

- **Performance and monitoring services:** Cisco CallManager Serviceability RTMT, Cisco RTMT Reporter Servlet, etc.
- **Backup and restore services:** Cisco DRF Master and Cisco DRF Local
- **System services:** Cisco CallManager Serviceability, Cisco CDP, Cisco Trace Collection tool, etc.
- **Platform services:** Cisco DB, Cisco Tomcat, SNMP master agent, etc.
- **DB services:** Cisco Database Layer Monitor
- **SOAP services:** SOAP-Real-Time Service APIs, etc.
- **CM services:** Cisco CallManager Personal Directory, Cisco Extension Mobility Application, Cisco CallManager, and Cisco IP Phone Services
- **CDR services:** Cisco CDR Repository Manager and CDR Agent
- **Admin services:** Cisco CallManager administration

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-24

Note Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT) is the real-time monitoring tool that can be installed on an administrator PC. The listed Cisco Unified Communications Manager RTMT services are required for the client application running on the administrator PC to communicate with Cisco Unified Communications Manager.

Note DRF stands for the disaster recovery framework. It allows backup and restore tasks to be performed from the Disaster Recovery System (DRS).

Feature Services

The slide shows a list of feature services categorized in groups.

Feature Services

Categorized into the following groups:

- **Database and admin services:** Cisco AXL Web Service, Cisco Bulk Provisioning Service, Cisco TAPS Service
- **Performance and monitoring services:** Cisco Serviceability Reporter, Cisco CallManager SNMP Service
- **CM services:** Cisco CallManager, Cisco TFTP, Cisco CTIManager, Cisco Extension Mobility, etc.
- **CTI services:** Cisco CallManager Attendant Console Server, Cisco IP Manager Assistant, Cisco WebDialer Web Service
- **CDR services:** Cisco SOAP-CDRonDemand Service, Cisco CAR Scheduler, Cisco CAR Web Service
- **Security services:** Cisco CTL Provider, Cisco Certificate Authority Proxy Function
- **Directory services:** Cisco DirSync
- **Voice Quality Reporter services:** Cisco Extended Functions

Service Activation

Feature services are activated from Cisco Unified Communications Manager Serviceability.

Service Activation

To enable Cisco Unified Communications Manager Release 6.0 feature services, perform the following tasks:

- Access Cisco Unified CM Serviceability.
- Go to **Tools > Service Activation**.
- Select your server.
- Enable the necessary services.
- Go to **Tools > Control Center – Feature Services** and select your server.
- Verify that the configured services are up and running.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-26

In order to activate or deactivate feature services for a server, perform the following steps in Cisco Unified Communications Manager Serviceability:

- Step 1** Go to **Tools > Service Activation**.
- Step 2** Select the server where you want to activate or deactivate a service.
- Step 3** Set or remove the checkbox for each service that you want to modify and save the changes.
- Step 4** Verify that the service has been started by using the control center (**Tools > Control Center – Feature Services**).

Service Activation Screenshot

The figure shows a screenshot of the Service Activation web page.

Service Activation Screenshot

Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Serviceability Go

CCMAdministrator | About | Logout

Related Links: Control Center - Feature Services Go

Alarm ▾ Trace ▾ Tags ▾

Service Activation

Status Status : Ready

Save Set to Default Refresh

Select Server Server* 10.96.128.200 Go

Check All Services

CM Services

Service Name	Activation Status
Cisco CallManager	Activated
Cisco Tftp	Activated
Cisco Messaging Interface	Deactivated
Cisco Unified Mobile Voice Access Service	Activated
Cisco IP Voice Media Streaming App	Activated
Cisco CTIManager	Activated
Cisco Extension Mobility	Activated
Cisco Extended Functions	Activated
Cisco Dialed Number Analyzer	Activated
Cisco DHCP Monitor Service	Activated

CTI Services

Optional: Select default services based on a single-server configuration

1. Select the server.

2. Select the services that should be activated.

3. Deselect the services that should be deactivated.

4. Save and perform settings.

5. Go to Control Center – Feature Services page.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-27

The Service Activation web page is used to selectively activate and deactivate feature services per server in the cluster.

Control Center Screenshot

The figure shows a screenshot of the Control Center - Feature Services web page.

The screenshot displays the 'Control Center - Feature Services' interface. At the top, there's a navigation bar with links for Alarm, Trace, Tools, Snmp, Help, CCMAdministrator, and About. Below the navigation is a search bar labeled 'Select Server' with the value '10.96.128.200' and a 'GO' button. The main content area is divided into sections: 'Database and Admin Services', 'Performance and Monitoring Services', and 'CM Services'. Each section contains a table with columns for Service Name, Status*, Activation Status, Start Time, and Up Time. Annotations with callouts point to specific elements: a callout from the 'Status' link in the top-left corner points to the 'Status' column in the tables; another callout from the 'Start, stop, restart, and refresh selected service.' link in the top-left corner points to the 'Activation Status' column; a third callout from the 'Service start time and up time' link in the top-right corner points to the 'Up Time' column; and a fourth callout from the 'Select service to start, stop, or restart.' link in the middle-left points to the 'Activation Status' column in the 'CM Services' table. The tables show data for multiple services across these categories.

Service Name	Status*	Activation Status	Start Time	Up Time
Cisco AXL Web Service	Started	Activated	Sat Jun 2 09:42:45 2007	6 days 02:46:04
Cisco Bulk Provisioning Service	Started	Activated	Sat Jun 2 09:42:46 2007	6 days 02:46:03
Cisco TAPS Service	Not Running	Deactivated		

Service Name	Status*	Activation Status	Start Time	Up Time
Cisco Serviceability	Running	Activated	Sat Jun 2 09:40:48 2007	6 days 02:48:01
Cisco CallManager	Not Running	Deactivated		

Service Name	Status*	Activation Status	Start Time	Up Time
Cisco CallManager	Started	Activated	Sat Jun 2 09:40:25 2007	6 days 02:48:24
Cisco Tftp	Started	Activated	Sat Jun 2 09:40:41 2007	6 days 02:48:08

The control center for feature services is used to start, stop, or restart and to verify the current status (started or not running) and the activation status (activated or deactivated) of feature services per server in the cluster.

Cisco Unified Communications Manager Enterprise Parameters

This topic describes the purpose of enterprise parameters, lists some of them, and shows how to change them.

Enterprise Parameters

- Used to define cluster-wide system settings.
- Apply to all devices and services in the same cluster.
- After installation, enterprise parameters are used to set initial values of device defaults.
- Only change if you fully understand the feature that you are changing or if instructed to do so by Cisco TAC.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-30

Enterprise parameters are used to define cluster-wide system settings and apply to all devices and services in the cluster. After installation, enterprise parameter default values should be verified and modified if required before deploying endpoints. Some enterprise parameters will specify initial values of device defaults.

Note	Change enterprise parameters only if you are fully aware of the impact of your modifications or if instructed to do so by Cisco Technical Assistance Center (TAC).
-------------	--

Example of Enterprise Parameters

The table provides some examples of enterprise parameters with descriptions and their default values.

Example of Enterprise Parameters		
Parameter	Description	Default value
Auto Registration Phone Protocol	Specifies the protocol with which autoregistered phones should boot during initialization.	SCCP
Enable Dependency Records	Determines whether to display dependency records.	False
CCMUser Parameters	These parameters are used to display or hide certain user-configurable settings from the CCMUser web page.	n/a
Phone URL Parameters	URLs for IP phone authentication, directory button, Services button, etc.	Hostnames are used instead of IP addresses
User Search Limit	This parameter specifies the maximum number of users to be retrieved from a search in the Corporate Directory feature on the phone.	64

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-31

Dependency records are a feature of Cisco Unified Communications Manager that allows an administrator to view configuration database records that reference the currently displayed record. They are a useful tool when you want to delete a configuration entry (for example, a device pool), but the deletion fails because the record is still referenced (for example, by an IP phone). Without dependency records, you would have to check each device, whether or not it uses the device pool that you tried to delete.

Changing Enterprise Parameters

Enterprise parameters are changed from Cisco Unified Communications Manager Administration.

Changing Enterprise Parameters

1. From Cisco Unified Communications Manager Administration page, choose **System > Enterprise Parameters**.
2. Update the appropriate parameter settings.
 - To view the description of a particular enterprise parameter, click the parameter name.
 - To view the descriptions of all the enterprise parameters, click the ? button.
3. To save the changes, click **Save**.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-32

In order to modify enterprise parameters, perform the following steps in Cisco Unified Communications Manager Administration:

Step 1 Go to **System > Enterprise Parameters**.

Step 2 Change the enterprise parameter values as desired and save the changes.

Note To obtain additional information about enterprise parameters, click the "?" symbol at the top right corner of the screen.

Enterprise Parameters Screenshot

The figure shows a screenshot of the Enterprise Parameters Configuration web page.

Enterprise Parameter Screenshot

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration

Enterprise Parameters Configuration

Save Set to Default Reset

CCMUser Parameters

Show	Value	Default
Show 2. Save the changes.	False	False
Show Show Speed Dial Settings *	True	True
Show Show Cisco IP Phone Services Settings *	True	True
Show Show Personal Address Book Settings *	True	True
Show Show Message Waiting Lamp Policy Settings *	True	True
Show Show Line Text Label Settings *	True	False
Show Show Locale for Phone Settings *	True	True
Show Show Locale for Web Pages Settings *	True	True
Show Show Change Password Option *	True	True
Show Show Change PIN Option *	True	True
Show Show Download Plugin Option *	True	True
Show Show Online Guide Option *	False	True
Show Show Directory *	True	True
Show Show Mobility Features Option *	True	True

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-33

At the Enterprise Parameters Configuration web page, you will find enterprise parameters grouped into categories with the current configuration and the default value shown per parameter.

Phone URL Enterprise Parameters

The screenshot shows the group of phone URL enterprise parameters.

The screenshot displays the Cisco Unified CM Administration interface under the 'Enterprise Parameters Configuration' section. The 'Phone URL Parameters' tab is selected. Several URL fields are listed, each with a corresponding IP address placeholder. The first field, 'URL Authentication', has the value 'http://10.96.128.200:8080/ccmcip/authenticate.jsp' highlighted with a yellow box. Other fields include 'URL Directories', 'URL Idle', 'URL Idle Time' (set to 0), 'URL Information', 'URL Messages', 'IP Phone Proxy Address', and 'URL Services'. Navigation links for Save, Set to Default, and Reset are visible at the top of the configuration panel.

When removing DNS reliance, change all hostnames in URLs to IP addresses.

- Note** When removing DNS reliance, all hostnames within enterprise URL parameters have to be changed to IP addresses.

Cisco Unified Communications Manager Service Parameters

This topic describes the purpose of service parameters, lists some of them, and shows how to change them.

Service Parameters

Service parameters for Cisco Unified Communications Manager allow you to configure parameters for different services. Examples for service parameters of the Cisco Unified Communications Manager call-processing service are:

- T302 timer to speed up dialing
- Enable call detail records
- Define extension mobility maximum login time
- Define attendant console username
- Define voice media-streaming application codecs

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-36

Service parameters are used to define settings for a specific service (for example, the call-processing Cisco CallManager service). They can be configured separately for each server in the cluster. After installation (or activation of feature services), service parameter default values should be verified and modified, if required, before deploying endpoints. The most important service parameters for the Cisco CallManager service are:

- **T302 timer:** Specifies the interdigit timer for variable-length numbers. Reducing the default value will speed up dialing (shorter post-dial delay).
- **CDR and CMR:** CDRs and CMRs are the basis for call reporting, accounting, and billing. The service parameters are used to enable CDRs and CMRs.
- **Cisco Unified Communications Manager Extension Mobility maximum login time:** After expiration of this timer, a user is logged out of Cisco Unified Communications Manager Extension Mobility regardless of the idle time of the device.
- **Cisco Unified Communications Manager Attendant Console username:** Specifies the application user name that is used by the Cisco Unified Communications Manager Attendant Console application when logging into Cisco Unified Communications Manager Computer Telephony Integration (CTI) Manager interface.
- **Codecs of voice media-streaming applications**

Example of Service Parameters

The table provides some examples of Cisco CallManager service parameters with descriptions and their default values.

Example of Service Parameters		
Parameter	Description	Default value
CDR Enabled Flag	This parameter determines whether call detail records (CDRs) are generated.	False
Station KeepAlive Interval	This parameter designates the interval between KeepAlive messages sent from Cisco IP phones to the primary Unified CM.	30s
T302 Timer	This parameter specifies an interdigit timer for sending the SETUP ACK message. When this timer expires, Cisco Unified CM routes the dialed digits.	15s
Automated Alternate Routing Enable	This parameter determines whether to use automated alternate routing when the system does not have enough bandwidth.	False
Change B-Channel Maintenance Status (Click Advanced button first.)	This parameter allows Cisco Unified CM to change individual B-Channel maintenance status for PRI and CAS interfaces in real time for troubleshooting.	n/a

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-37

By default, not all service parameters are displayed. To see the complete list of service parameters, you have to click the “Advanced” button. The Change B-Channel Maintenance Status service parameter is an example for a Cisco CallManager service parameter, which is not shown by default.

Changing Service Parameters

Service parameters are changed from within Cisco Unified Communications Manager Administration.

Changing Service Parameters

1. From Cisco Unified CM Administration page, choose **System > Service Parameters**.
2. Select the **Server** and choose the **Service**.
3. Update the appropriate parameter settings.
 - If you cannot find the parameter, click the **Advanced** button to display hidden parameters.
4. To save the changes, click **Save**.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-38

In order to modify service parameters, perform the following steps in Cisco Unified Communications Manager Administration:

Step 1 Go to **System > Service Parameters**.

Step 2 Select the server and the service for which you want to change service parameters.

Step 3 Change the service parameter values as desired and save the changes.

Note If you cannot find the service parameter that you want to change, click **Advanced** to see the complete list of available service parameters. By default, not all service parameters are displayed.

Service Parameter Configuration Screenshot

The figure shows a screenshot of the initial Service Parameter Configuration web page.

Service Parameter Configuration Screenshot

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Status: Ready

Select server.

Select service.

Server*: 10.96.128.200 (Active)

Service*: Cisco CallManager (Active)

All parameters

- Not Selected --
- Cisco AMC Service (Active)
- Cisco Bulk Provisioning Service (Active)
- Cisco CTIManager (Active)
- Cisco CTC Provider (Inactive)
- Cisco CallManager (Active)**
- Cisco CallManager Assistant Console Server (Active)
- Cisco CallManager Gateway Service (Inactive)
- Cisco Certificate Authority Proxy Function (Inactive)
- Cisco DRF Local (Active)
- Cisco DRF Master (Active)
- Cisco Database Layer Monitor (Active)
- Cisco DirSync (Active)
- Cisco Extension Functions (Active)
- Cisco Extension Mobility (Active)
- Cisco IP Manager Assistant (Active)
- Cisco IP Voice Media Streaming App (Active)
- Cisco Log Partition Monitoring Tool (Active)
- Cisco Messaging Interface (Inactive)
- Cisco RIS Data Collector (Active)
- Cisco Usability Reporter (Active)
- Cisco TAPS Service (Inactive)
- Cisco Tftp (Active)
- Cisco Trace Collection Service (Active)
- Cisco WebDialer Web Service (Active)

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-39

At the initial screen, you have to select the server and the service for which you want to see or change the service parameters.

Cisco CallManager Service Parameter Screenshot

The screenshot shows some of the Cisco CallManager service parameters.

CallManager Service Parameters Screenshot

Service Parameter Configuration

Optional: Click **Advanced** to show hidden service parameters.

Cisco Call Manager (Active) Parameters on server 10.96.1.28.200 (Active)

2. Save the changes.

Parameter	Value	Suggested Value
CCM Call Throttling		
Code Yellow Entry Latency *	20	20
Code Yellow Exit Latency Calculation *	40	40
Code Yellow Duration *	99999	99999
Max Events Allowed *	2000	2000
System Throttle Sample Size *	10	10
System		
CDR Enabled Flag *	True	False
CDR Log Calls with Zero Duration Flag *	True	False
Digit Analysis Complexity *	StandardAnalysis	StandardAnalysis
Database Debounce Timer *	0	0
Maximum Phone Fallback Queue Depth *	10	10
Maximum Number of Registered Devices *	5000	5000

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-40

At the Service Parameter Configuration web page, you will find service parameters grouped into categories with the current configuration and the default value shown per parameter.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco Unified Communications Manager initial configuration includes network configuration, activation of feature services, and enterprise and service parameter configuration.
- Cisco Unified Communications Manager network configuration options include NTP configuration, DHCP server configuration, and using DNS versus IP addresses.
- The Cisco Unified Communications Manager DHCP service is designed to serve IP phones.
- In order to avoid DNS reliance of IP phones, change hostnames to IP addresses.
- Network services are automatically activated, while Feature services are activated by the Cisco Unified Communications Manager administrator.
- Enterprise parameters are used to define cluster-wide system settings.
- Service parameters are used to configure parameters of specific services.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-41

References

For additional information, refer to these resources:

- Cisco Unified Serviceability Administration Guide for Cisco Unified Communications Manager, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/6_0_1/admin/cmservbk.html
- Cisco Unified Communications Manager Administration Guide
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf

Lesson 3

Managing User Accounts in Cisco Unified Communications Manager

Overview

Cisco Unified Communications Manager includes several features that are related to user accounts, including end-user features and administrative privileges. Cisco Unified Communications Manager user accounts can be managed using Cisco Unified Communications Manager configuration tools or by integrating Cisco Unified Communications Manager with a Lightweight Directory Access Protocol (LDAP) directory. This lesson describes the types of user accounts used by Cisco Unified Communications Manager and how they can be managed.

Objectives

Upon completing this lesson, you will be able to manage user accounts, including integrating Cisco Unified Communications Manager with a corporate LDAP directory and enabling multiple levels of user privileges. This ability includes being able to meet these objectives:

- Identify the different user accounts in Cisco Unified Communications Manager and explain how they are used
- Describe how to add and delete users and how to assign authorization rights to them
- Describe the purpose of the Cisco Unified Communications Manager Bulk Administration Tool (BAT) and list its features
- Describe how Cisco Unified Communications Manager BAT can be used to manage users
- Identify LDAP characteristics and list the types of LDAP support provided by Cisco Unified Communications Manager
- Describe how LDAP can be used for user provisioning
- Describe how LDAP can be used for user authentication

Cisco Unified Communications Manager User Accounts

This topic describes user accounts in Cisco Unified Communications Manager.

Cisco Unified Communications Manager Features Interacting with User Accounts

- Cisco Unified CM user and administrator web interfaces
 - Cisco Unified CM User web pages
 - Cisco Unified CM Administration
 - Cisco Unified CM Serviceability
 - Cisco Unified CM operating system Administration
 - Cisco Unified CM Disaster Recovery System
- Cisco Unified CM applications
 - Cisco Unified CM Attendant Console
 - Cisco Unified CM Extension Mobility
 - Cisco Unified CM Assistant
- Directories
- Cisco IP Phone Services

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-4

Several Cisco Unified Communications Manager features require user accounts to be able to authenticate the user. These features include administrative and user web pages and applications that require the user to log in, such as:

- Cisco Unified Attendant Console
- Cisco Unified Communications Manager Extension Mobility
- Cisco Unified Communications Manager Assistant

Cisco IP phones can browse directories to find the directory number for a given username. In order to be able to provide this information, Cisco Unified Communications Manager needs to know users and their extensions.

When using Cisco CallManager Cisco IP Phone Services, the services can be configured to require a user login before providing access to the service.

Users can authenticate with their username and a password (alphanumeric) or PIN (numeric), depending on the application. Cisco Unified Communications Manager sends authentication requests to an internal library, the Identity Management System library, which is responsible for authenticating the credentials against the embedded database (by default).

Two Types of User Accounts in Cisco Unified Communications Manager

There are two types of user accounts in Cisco Unified Communications Manager.

Two Types of User Accounts in Cisco Unified Communications Manager

End Users	Application Users
Associated with an individual person	Associated with an application
For personal use in interactive logins	For non-interactive logins
Used for user features and individual administrator logins	Used for application authorization
Included in user directory	Not included in user directory
Can be provisioned and authenticated using an external directory service (LDAP)	Cannot use LDAP

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-5

The two types of user accounts in Cisco Unified Communications Manager are:

- **End users:** All end users are associated with a physical person and an interactive login. This category includes all IP telephony users as well as Cisco Unified Communications Manager administrators when using the user groups and roles configurations.
- **Application users:** All application users are associated with Cisco Unified Communications features or applications, such as Cisco Attendant Console, Cisco Unified Contact Center Express, or Cisco Unified Communications Manager Assistant. These applications need to authenticate with Cisco Unified Communications Manager, but these internal "users" do not have an interactive login and serve purely for internal communications between applications.

Examples of application users:

Feature or Application	User Account
Cisco QRT Service	CCMQRTSecureSysUser, CCMQRTSysUser
Cisco Extension Mobility Service	CCMSysUser
Cisco Unified Communications Manager Assistant Service	IPMASecureSysUser, IPMAsysUser
Cisco WebDialer Service	WDSecureSysUser, WDSysUser
Cisco Attendant Console Service	"ac" user created from Cisco Unified Communications Manager Administration

Data Associated with User Accounts

User accounts in Cisco Unified Communications Manager are associated with several attributes.

Data Associated with User Accounts

- Personal and organizational settings
 - **User ID**, First Name, Middle Name and Last Name
 - Manager User ID, Department
 - Phone Number, Mail ID
- **Password**
- Cisco Unified CM configuration settings
 - PIN and **SIP digest credentials**
 - **User privileges (user groups and roles)**
 - Associated PCs, **controlled devices**, and directory numbers
 - Application and feature parameters (Extension Mobility profile, **Presence Group**, Mobility, **CAPF**, etc.)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-6

The attributes associated with end users are separated into three categories and include:

- **Personal and organizational settings**
 - *User ID*, First, Middle, and Last Name
 - Manager User ID, Department
 - Phone Number, Mail ID
- **Password**
- **Cisco Unified Communications Manager configuration settings**
 - PIN and *SIP digest credentials*
 - *User privileges (user groups and roles)*
 - Associated PCs, *controlled devices*, and directory numbers
 - Application and feature parameters (for example, Extension Mobility profile, *Presence Group*, Mobility, *Certificate Authority Proxy Function (CAPF)*, and so on)

Note	Application users are associated with a subset of these attributes, which are the ones that are printed in <i>italics</i> .
-------------	---

User Privileges

Cisco Unified Communications Manager allows the assignment of user privileges to application and end users.

User Privileges

- Privileges are assigned to application users and end users.
- Privileges include these accesses:
 - Access to user web pages.
 - Access to administration web pages.
 - Access to specific administration functions.
 - Access to APIs (CTI, SOAP, etc.)
- User privileges include these configuration elements:
 - User groups (a list of application and end users).
 - Roles (a collection of resources for an application).
 - Each role refers to one application.
 - Each application has one or more resources (static list).
 - Per role, access privileges are configured per application resource.
 - Roles are assigned to user groups.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-7

Privileges that can be assigned to users include:

- Access to administration and user web pages
- Access to specific administrative functions
- Access to application interfaces, such as computer telephony integration (CTI) and Simple Object Access Protocol (SOAP)

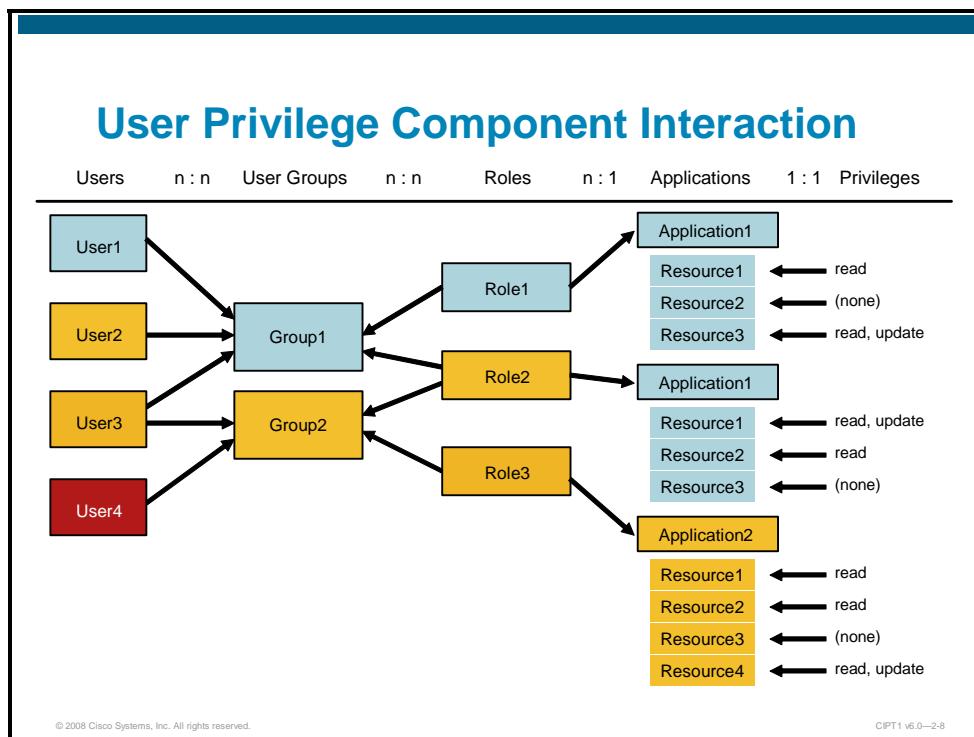
User privileges are configured using two configuration entities:

- **User groups:** a list of application and end users
- **Roles:** a collection of resources for an application

Each role refers to one application, and each application has one or more resources (static list per application). Per role, access privileges are configured per application resource. Roles are assigned to user groups.

User Privilege Component Interaction

The figure illustrates the component interaction of user privilege configuration entities.



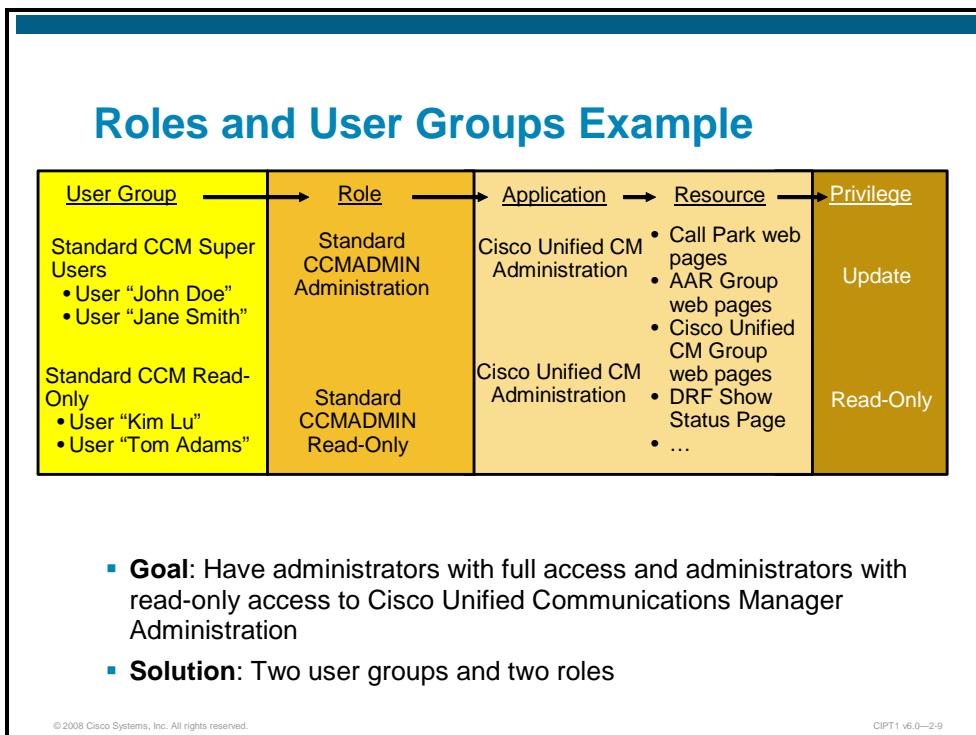
The diagram shows four users (User1 to User4) and two user groups (Group1 and Group2). User1 and User2 are assigned to Group1; User3 is assigned to both groups; and User4 is assigned to Group2.

There are three roles (Role1 to Role3). Role1 is assigned to Group1; Role2 is assigned to both groups; and Role3 is assigned to Group2.

Role1 and Role2 both refer to Application1. Application1 has three application resources (Resource1 to Resource3). Role1 and Role2 have different privileges assigned to resources of Application1. Role3 refers to Application2 and has privileges assigned to the four application resources (Resource1 to Resource4) of Application2.

Roles and User Groups Example

The figure shows an example of roles and user groups.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-9

In the example, the goal is to have administrators who have full access to all configuration pages of Cisco Unified Communications Manager Administration and administrators who have read-only privileges to these configuration pages.

The *Cisco CallManager Administration* (that is, Cisco Unified Communications Manager Administration) application has web pages associated with a function, such as the *Call Park web pages* (used to configure the call park feature), the *AAR Group web pages* (used to configure automated alternate routing), the *CallManager group web pages* (used for configuration), the *Disaster Recovery Framework (DRF) Show Status page* (used to check the status of disaster recovery system backup or restore jobs), and much more. These web pages are application resources of the *Cisco CallManager Administration* application.

Cisco Unified Communications Manager has standard roles (that is, roles that exist by default), which are associated with the *Cisco Call Manager Administration* application, such as role *Standard CCMADMIN Administration* and role *Standard CCMADMIN Read-Only*. The first role has all application privileges set to *update*, while in the second role, all application privileges are set to *read*.

Cisco Unified Communications Manager has several standard user groups, including user group *Standard CCM Super Users* and user group *Standard CCM Read-only*. User group *Standard CCM Super Users* is associated with role *Standard CCMADMIN Administration*, and user group *Standard CCM Read-only* is associated with role *Standard CCMADMIN Read-Only*.

Based on the previously mentioned default roles and user groups, in order to assign full access to all configuration pages of Cisco Unified Communications Manager Administration to an end user, the end user has to be assigned to the standard user group *Standard CCM Super Users*. End users that should have read-only access to all configuration pages of Cisco Unified Communications Manager Administration have to be assigned to the standard user group *Standard CCMADMIN Read-Only*. No further configuration is required, as the appropriate

application privileges are preconfigured in the default roles, and the default roles are pre-assigned to the corresponding default user groups.

Note	Cisco Unified Communications Manager has numerous default user groups (more than 20 in Cisco Unified Communications Manager Release 6.0), which cover the needs for the most typical requirements. Examples of these default user groups are the aforementioned <i>Standard CCM Super Users</i> and <i>Standard CCMADMIN Read-Only</i> user groups and other user groups, such as <i>Standard CAR Admin Users</i> , <i>Standard CCM Server Maintenance</i> , <i>Standard CCM Server Monitoring</i> , <i>Standard CCM Phone Administration</i> , <i>Standard CCM End User</i> , and <i>Standard CCM Gateway Administration</i> .
-------------	---

User Management Options

User accounts in Cisco Unified Communications Manager can be managed in different ways.

User Management Options

One-by-one manual configuration using Cisco Unified Communications Manager Administration

Bulk configuration using Cisco Unified Communications Manager BAT

LDAP integration (for end users only):

- LDAP synchronization
 - For user provisioning
 - Personal and organizational user data are managed in LDAP
- LDAP authentication
 - For user authentication
 - Passwords managed in LDAP

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-10

User management options in Cisco Unified Communications Manager include:

- **Using Cisco Unified Communications Manager Administration, User Management menu items:** This option is suitable for configuring a small amount of users or doing single updates to the configuration. It does not scale for mass deployment of users.
- **Using Cisco Unified Communications Manager Bulk Administration Tool (BAT):** Cisco Unified Communications Manager BAT allows bulk administration of several configuration elements including users. Cisco Unified Communications Manager BAT is a good option for initial (mass) deployment when LDAP integration is not used.
- **LDAP integration:** This option is available only to end users. LDAP integration provides two functions, which can be enabled independent of each other:
 - **LDAP synchronization:** Allows user provisioning where personal and organizational data are managed in an LDAP directory and replicated to the Cisco Unified Communications Manager configuration database.
 - **LDAP authentication:** Allows user authentication against an LDAP directory. When using LDAP authentication, passwords are managed in LDAP.

LDAP

This section describes the characteristics of LDAP.

LDAP

- Specialized database stores information about users
 - Centralized storage of user information
 - Available to all enterprise applications
- LDAPv3 – Lightweight Directory Access Protocol version 3
- Examples
 - Microsoft Active Directory, Netscape, iPlanet, SunONE
- Cisco Unified CM supports two types of integration
 - LDAP synchronization
 - LDAP authentication
- When using LDAP, some user data are no longer controlled via Cisco Unified Communications Manager Administration

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-11

LDAP directories are services that store user information in a specialized database. The database is optimized for a high number of reads and searches, and occasional writes and updates. Directories typically store data that do not change often, such as employee information, user privileges on the corporate network, and so on.

The LDAP provides applications with a standard method for accessing and potentially modifying the information stored in the directory. This capability enables companies to centralize all user information in a single repository available to several applications, with a remarkable reduction in maintenance costs through the ease of adds, moves, and changes.

Examples for LDAP directories are Microsoft Active Directory (AD), Netscape, iPlanet and Sun ONE. Cisco Unified Communications Manager supports two types of integration: LDAP synchronization and LDAP authentication. When using LDAP, some user data are not controlled by Cisco Unified Communications Manager administration web pages.

Cisco Unified Communications Manager End-User Data Location

The table shows where user data are stored without LDAP integration, when using LDAP synchronization, and when using LDAP authentication.

	No LDAP Integration	LDAP Synchronization	LDAP Authentication
Personal and organizational settings: User ID First, Middle, and Last Name Manager User ID and Department Phone Number and Mail ID	Local	LDAP (replicated to local)	LDAP (replicated to local) or Local
Password	Local	Local	LDAP
Cisco Unified CM Settings: PIN and Digest Credentials Groups and Roles Associated PCs Controlled Devices Extension Mobility Profile and CAPF Presence Group and Mobility	Local	Local	Local

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-12

As shown in the table, without LDAP integration, all end-user data are stored in the Cisco Unified Communications Manager database and configured via Cisco Unified Communications Manager Administration.

Note Application user data are always controlled by Cisco Unified Communications Manager Administration and stored in the Cisco Unified Communications Manager database.

When using LDAP synchronization, personal and organizational settings are configured and stored in LDAP. With each synchronization, the data is replicated to the Cisco Unified Communications Manager database. However, as long as LDAP synchronization is enabled, this data cannot be modified in Cisco Unified Communications Manager. User passwords and Cisco Unified Communications Manager configuration settings are still configured using Cisco Unified Communications Manager Administration and stored in the Cisco Unified Communications Manager database only.

When using LDAP authentication, personal and organizational settings are either controlled by Cisco Unified Communications Manager or by LDAP. Which one depends on the use of LDAP synchronization and is independent of LDAP authentication. User passwords, however, are configured and stored in LDAP only. The passwords are not replicated to the Cisco Unified Communications Manager database. In order to store the password for a Cisco Unified Communications Manager user (the user has to exist in the Cisco Unified Communications Manager database so that Cisco Unified Communications Manager settings can be configured for the user) in LDAP, the user has to exist in both databases (that is, in LDAP and in the Cisco

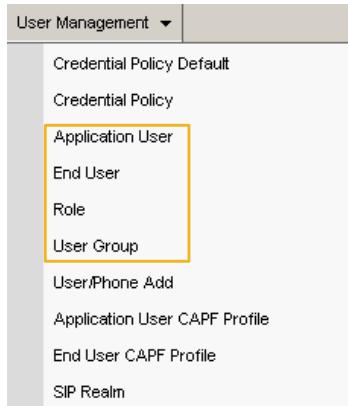
Unified Communications Manager database). Therefore, it is recommended to combine LDAP authentication with LDAP synchronization. This step avoids inconsistencies in usernames and eliminates the need for maintaining usernames twice.

Managing User Accounts Using the Administration GUI

This topic describes how to manage user accounts using Cisco Unified Communications Manager Administration.

User Management Using Unified Communications Manager Administration

- Performed from **Unified CM Administration > User Management**
 - Requires sufficient privileges
 - Use master administrator account created during installation.
 - Use end-user account with user management privilege.
 - Available options include
 - Application User
 - End User
 - Role
 - User Group



The screenshot shows a dropdown menu titled "User Management". The menu items are: Credential Policy Default, Credential Policy, Application User (which is highlighted with a yellow box), End User, Role, User Group, User/Phone Add, Application User CAPF Profile, End User CAPF Profile, and SIP Realm.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-14

Cisco Unified Communications Manager user management is performed from **Cisco Unified Communications Manager Administration > User Management**. To be able to manage users, the administrator needs to use an account that has sufficient privileges. It can be the default administrator account, which is created during Cisco Unified Communications Manager installation, or any end-user account that has the user management privilege assigned.

The user management menu includes options to configure application users, end users, roles, and user groups.

Application User Configuration Page

The figure shows the Application User Configuration page.

The screenshot displays the 'Application User Configuration' interface. At the top, the title 'Application User Configuration Page' is centered. Below it, the 'Application User Information' section contains several input fields:

- User ID* (highlighted with a yellow box)
- Password
- Confirm Password
- Digest Credentials
- Confirm Digest Credentials
- Presence Group* (dropdown menu set to 'Standard Presence group')

Below these are four checkboxes:

- Accept Presence Subscription
- Accept Out-of-dialog REFER
- Accept Unsolicited Notification
- Accept Replaces Header

On the left side of the 'Device Information' section, there is a table:

Available Devices
SEP00070E576F43 SEP001201545D98 SEP001AA182D475

Next to the table are three buttons: 'Find more Phones', 'Find more Route Points', and 'Find more Pilot Points'. On the right side of the 'Device Information' section, there is another table:

Controlled Devices
[empty]

At the bottom of the page, copyright information reads: '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—2-15'.

The most important settings are the User ID and the Password.

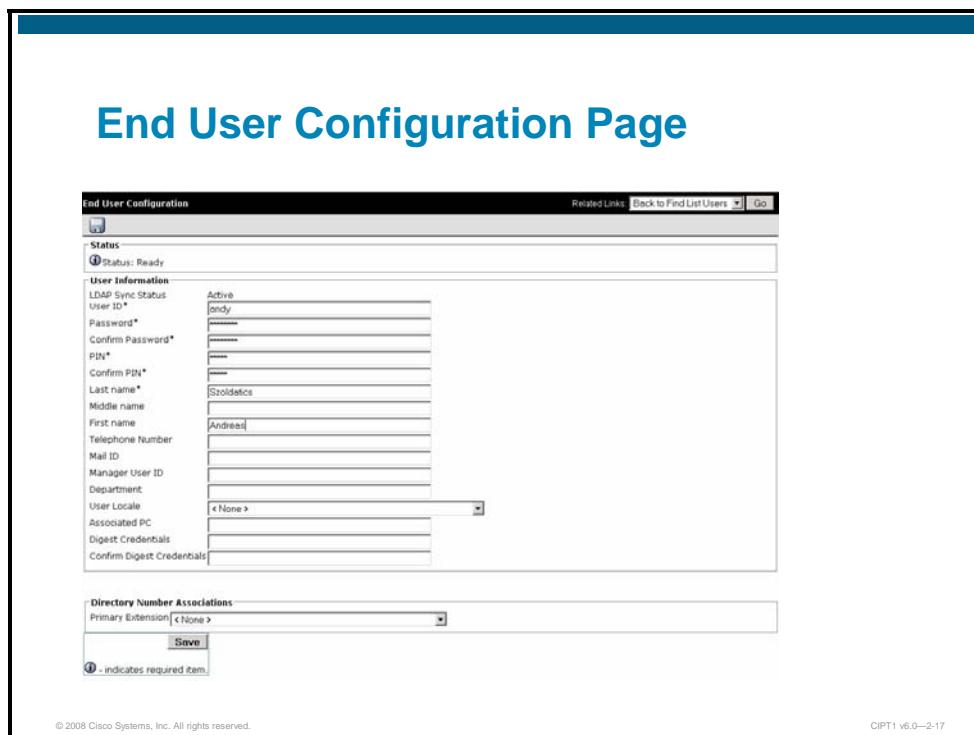
Application User Configuration Page (Cont.)

The screenshot shows the 'Application User Configuration' page. At the top, there's a section for 'CAPF Information' with a list of 'Associated CAPF Profiles'. Below this is a 'Permissions Information' section divided into 'Groups' and 'Roles' tabs. The 'Groups' tab is active, displaying a list of groups with 'Add to User Group' and 'Remove from User Group' buttons. The 'Roles' tab is also shown. A callout box points to the 'Add to User Group' button with the text 'Add application user to user groups.' Another callout box points to the 'View Details' link under the 'Groups' tab with the text 'View roles of application user.'

At the bottom of the Application User Configuration page, the application user can be added to user groups. The roles that are assigned to the user groups, of which the application user is a member, are displayed in the Roles list box.

End User Configuration Page

The figure shows the End User Configuration page.



The screenshot shows the 'End User Configuration' page. The main form is titled 'End User Configuration'. It has two main sections: 'Status' and 'User Information'. The 'Status' section shows 'Status: Ready'. The 'User Information' section contains various input fields for user details like User ID, Password, PIN, and contact information. Below the user information is a 'Directory Number Associations' section with a dropdown for Primary Extension. At the bottom are 'Save' and 'Cancel' buttons, and a note about required fields.

The End User Configuration screen is similar to the Application User Configuration screen. The User ID, Password and Group Membership (not shown on the screenshot) are the most important settings.

Roles

Cisco Unified Communications Manager includes standard roles as shown in the figure.

The screenshot shows a 'Find and List Roles' interface with a title bar 'Roles'. Below it is a toolbar with buttons for 'Add New', 'Select All', 'Clear All', and 'Delete Selected'. A table lists various standard roles:

Name	Application	Description	Copy
Standard AXL API Access	Cisco Call Manager AXL Database	Access the AXL APIs	Copy
Standard Admin Rep Tool Admin		Administer CAR	Copy
Standard CCM Admin Users		All users with access to CCM web site	Copy
Standard CCM End Users		Access to CCM User Option Pages	Copy
Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	Copy
Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management	Copy
Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management	Copy
Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management	Copy
Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management	Copy
Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management	Copy
Standard CCM User Management	Cisco Call Manager Administration	Standard CCM User Management	Copy
Standard CCM User Privilege Management	Cisco Call Manager Administration	Standard CCM User Privilege Management	Copy
Standard CCMADMIN Administration	Cisco Call Manager Administration	Administer all aspects of CCMAdmin system	Copy
Standard CCMADMIN Read Only	Cisco Call Manager Administration	Read access to all CCMAdmin resources	Copy
Standard CCMUSER Administration	Cisco Call Manager End User	Administer all aspects of CCMUser system	Copy
Standard CTI Allow Call Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of calls	Copy

Below the table, two bullet points describe role creation:

- Standard (default) roles exist; standard roles cannot be deleted.
- Custom roles can be created by adding new roles or by copying and then modifying standard roles.

At the bottom left is a copyright notice: © 2008 Cisco Systems, Inc. All rights reserved. At the bottom right is a page number: CIPT1 v6.0—2-18.

Standard roles cannot be deleted or modified. Custom roles can be created from scratch or by copying and then modifying a standard role.

Role Configuration Page

The figure shows the Role Configuration page.

The screenshot displays the 'Role Configuration Page' interface. At the top, there are buttons for 'Copy' and 'Add New'. Below this, the 'Role Information' section shows an application named 'Cisco Call Manager Administration' and a name 'Standard CCM Route Plan Management'. A callout box labeled 'Selected application' points to the application name. The 'Resource Access Information' section contains a table mapping resources to privileges. A callout box labeled 'Configured privilege per application resource' points to the 'read' and 'update' checkboxes for the 'Application Dial Rules web pages' row, where both are checked. A general note at the bottom states: 'Roles are configured per application and consist of application resource privileges.'

Resource	Privilege
	<input type="checkbox"/> read <input checked="" type="checkbox"/> update
AAR Group web pages	<input type="checkbox"/> read <input type="checkbox"/> update
Access List	<input type="checkbox"/> read <input type="checkbox"/> update
Add Unity User	<input type="checkbox"/> read <input type="checkbox"/> update
Announcer web pages	<input type="checkbox"/> read <input type="checkbox"/> update
Application Dial Rules web pages	<input checked="" type="checkbox"/> read <input checked="" type="checkbox"/> update
Application Server	<input type="checkbox"/> read <input type="checkbox"/> update
Application User CAPF	<input type="checkbox"/> read <input type="checkbox"/> update
Application User Web Pages	<input type="checkbox"/> read <input type="checkbox"/> update
BLF Directed Call Park	<input type="checkbox"/> read <input type="checkbox"/> update
BLF Speeddial	<input type="checkbox"/> read <input type="checkbox"/> update

As shown in the figure, an application has to be selected on the Role Configuration page. After selecting an application, the application resources are displayed, and read or update privilege can be assigned to each application resource.

User Groups

Cisco Unified Communications Manager includes standard user groups as shown in the figure.

User Groups

Find and List User Groups

Add New Select All Clear All Delete Selected

Standard CAR Admin Users		
Standard CCM Admin Users		
Standard CCM End Users		
Standard CCM Gateway Administration		
Standard CCM Phone Administration		
Standard CCM Read Only		
Standard CCM Server Maintenance		
Standard CCM Server Monitoring		
Standard CCM Super Users		
Standard CTI Allow Call Monitoring		
Standard CTI Allow Call Park Monitoring		
Standard CTI Allow Call Recording		
Standard CTI Allow Calling Number Modification		
Standard CTI Allow Control of All Devices		
Standard CTI Allow Reception of SRTP Key Material		

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-20

Standard user groups cannot be deleted or modified. Custom user groups can be created from scratch or by copying and then modifying a standard user group.

User Group Configuration Page: User Assignment

The figure shows the User Group Configuration page.

User Group Configuration Page: User Assignment

User Group Configuration Related Links: Back To Find/List Go

Name* Standard CCM Super Users

User (1 - 1 of 1)				Rows per Page 50		
Find User where User ID begins with		Find	Clear Filter	+	-	
<input type="checkbox"/>	User ID	CCMAdministrator	Full Name	Permission	i	
		Add End Users to Group	Add App Users to Group	Select All	Clear All	Delete Selected

↓

User (1 - 1 of 1)				Rows per Page 50	
Find User where First name begins with arief		Find	Clear Filter	+	-
<input type="checkbox"/>	User ID	Arief	Last Name	Department	
<input checked="" type="checkbox"/>	ariefm	Arief	Muslim		
		Select All	Clear All	Add Selected	Close

End users and application users are added to user groups.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-21

As shown in the figure, application and end users can be assigned to the user group on the User Group Configuration page.

User Group Configuration Page: Role Assignment

The figure illustrates how to assign roles to user groups.

The screenshot shows the 'User Group Configuration Page: Role Assignment' window. On the left, there's a sidebar with 'User Group >' and 'Related Links: Assign Role to User Group'. Below that is a search interface for 'Find and List Roles' with fields for 'Status' (set to 'Ready'), 'Search Options' (with 'Find Role where Name begins with' dropdown), and a 'Search Results' table showing role names like 'CCM Read Dial Plan' and 'Standard AXL API Access'. A red arrow points to the 'Search Results' table. On the right, the main panel has 'User Group Configuration' at the top, followed by 'User Group Information' (Name: 'Call Routing Operators') and 'Role Assignment'. It features a large text input field, a 'Save' button, and a 'Role Assignment' table listing roles with their descriptions and copy options. A red box highlights the 'Assign Role to Group' button in the top right of the main panel. At the bottom, there are buttons for 'Select All', 'Clear All', 'Add Selected' (which is also highlighted with a red box), and 'Close', along with a 'Rows per Page' dropdown set to 50. A copyright notice at the bottom left reads '© 2008 Cisco Systems, Inc. All rights reserved.' and a page number 'CIPT1 v6.0—2-22' at the bottom right.

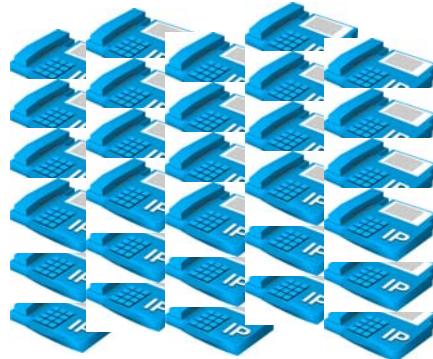
In order to assign roles to a user group, select the “Assign Role to Group” item from the Related Links list box at the User Group Configuration page. A new window, in which you can assign or delete roles, will be displayed.

Cisco Unified Communications Manager BAT

This topic describes the Cisco Unified Communications Manager BAT.

Cisco Unified Communications Manager BAT

Cisco Unified Communication Manager BAT allows management of many devices and records within a short period of time.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-24

Cisco Unified Communications Manager BAT allows mass configuration of Cisco Unified Communications Manager configuration items, including users, phones, directory numbers, gateways, and so on.

Cisco Unified Communications Manager BAT Characteristics

This section describes the characteristics of Cisco Unified Communications Manager BAT.

Cisco Unified Communications Manager BAT Characteristics

- Performs bulk transactions to the Cisco Unified Communications Manager database.
- Adds, updates, or deletes a large number of similar phones, users, or ports at the same time.
- Exports data (phones, users, gateways, etc.).
 - Exported files can be modified and re-imported.
- Integrated with the Cisco Unified Communications Manager Administration pages and available by default (no plug-in required).
- Supports localization.
- Cisco Unified CM Autoregister Phone Tool (formerly TAPS) is also available from the Bulk Administration menu but requires additional products.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-25

Cisco Unified Communications Manager BAT has the following characteristics:

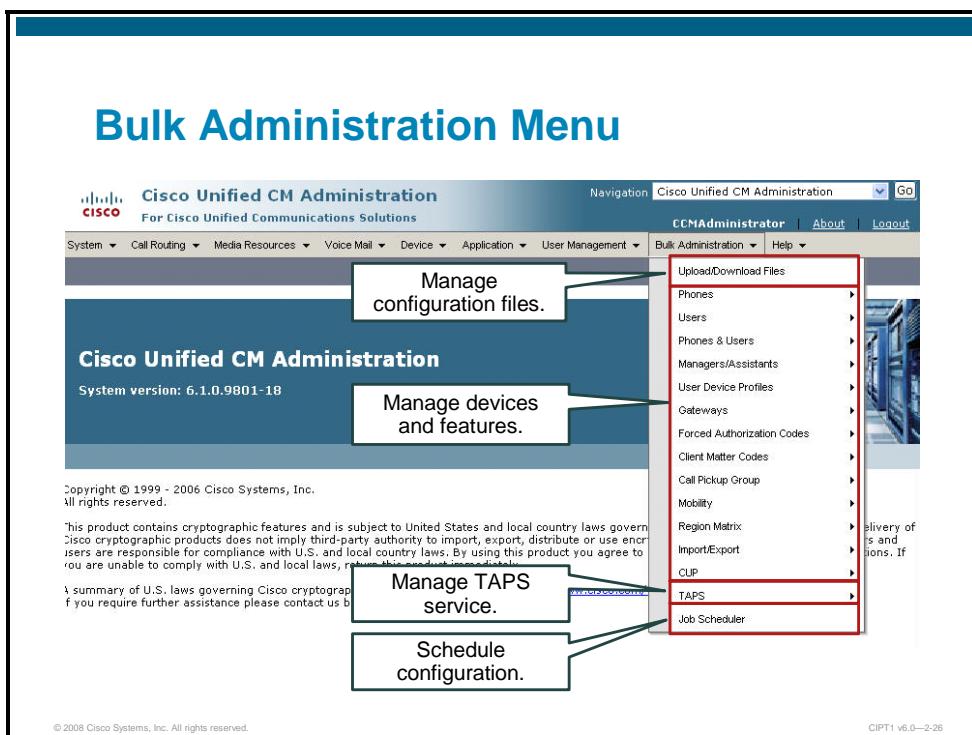
- Performs bulk transactions to the Cisco Unified Communications Manager database
- Adds, updates, or deletes a large number of similar phones, users, or ports at the same time
- Exports data (phones, users, gateways, and so on); exported files can be modified and re-imported

Note	The import and export function of Cisco Unified Communications Manager BAT can be used to move data records from one Cisco Unified Communications Manager cluster to another, for instance, when adding a new Cisco Unified Communications Manager cluster to a site that previously used the centralized call-processing model. This process cannot be done using the Disaster Recovery System (DRS) as a backup, and restore function includes all configuration data and allows only data to be restored to the same server from which it was backed up.
-------------	---

- Integrated with the Cisco Unified Communications Manager Administration pages and available by default (no plug-in required)
- Supports localization
- Cisco Unified Communications Manager Autoregister Phone Tool (formerly TAPS) is also available from the Bulk Administration menu but requires additional products

Bulk Administration Menu

Cisco Unified Communications Manager BAT has its own main menu in Cisco Unified Communications Manager Administration.



As shown in the figure, Cisco Unified Communications Manager BAT menu items include the ability to upload and download files, to manage devices, users and features, and to control submitted BAT jobs.

Cisco Unified Communications Manager BAT Components

This section describes components of Cisco Unified Communications Manager BAT that are used to perform bulk configuration jobs.

Cisco Unified Communications Manager BAT Components

Cisco Unified Communications Manager BAT administration consists of these features:

- Cisco Unified CM BAT templates are used to define general settings that fit all of the devices that should be added.
- CSV files are used to define devices and record specific settings that should be bulk-configured.
- Adding, updating, and deleting devices and records is done automatically based on queries and CSV files.
- Additions, updates, and deletions can be scheduled to be performed at a defined time.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-27

Cisco Unified Communications Manager BAT templates are used to define general settings that fit all of the devices that should be added. Comma-separated values (CSV) files are used to define specific settings per device that should be bulk-configured. Adding, updating, and deleting devices and records is initiated from the Cisco Unified Communications Manager Administration BAT menu, based on BAT configuration requests referring to BAT templates and BAT CSV files. BAT jobs can be executed immediately or scheduled for a later time.

Cisco Unified Communications Manager BAT can be used to work with the following types of devices and records:

- Add, update, and delete IP phones including voice gateway phones, CTI ports, and H.323 clients
- Migrate phones from Skinny Client Control Protocol (SCCP) to session initiation protocol (SIP)
- Add, update, and delete users
- Add, update, and delete user device profiles
- Add, update, and delete Cisco Unified Communications Manager Assistant and managers associations
- Add, update, and delete ports on a Cisco Catalyst 6000 FXS Analog Interface Module
- Add or delete Cisco VG200 and Cisco VG224 analog gateways and ports

Note The Cisco WS-X6624 and VG200 products have reached end of life (EOL).

-
- Add or delete Forced Authorization Codes (FACs)

- Add or delete client matter codes
- Add or delete Call Pickup groups
- Update or export Cisco Unified Presence or Cisco Unified Personal Communicator users
- Populate or depopulate the Region Matrix
- Insert, delete, or export the access list
- Export or import configuration
- Insert, delete, or export remote destination and remote destination profile

Bulk Provisioning Service

Cisco Unified Communications Manager BAT utilizes a dedicated feature service, the Bulk Provisioning Service (BPS), for maintaining and administering submitted BAT jobs.

Bulk Provisioning Service

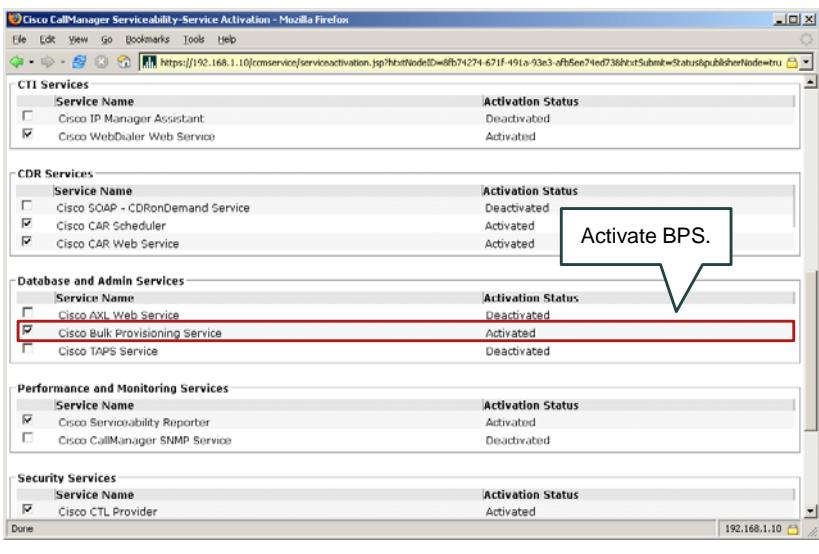
- Bulk Provisioning Service (BPS) administers and maintains all jobs that are submitted through Cisco Unified CM BAT.
- BPS is listed under database services in the service activation pages.
- Service should be activated for scheduled jobs to be executed.
- BPS has to be activated only on the Cisco Unified Communications Manager publisher.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-28

The BPS is activated from **Cisco Unified Communications Manager Serviceability > Tools > Service Activation**. It is required for executing submitted BAT jobs. The BPS has to be activated on the Cisco Unified Communications Manager publisher server only.

Bulk Provisioning Service (Cont.)



The figure shows the BPS being activated in the Service Activation page of Cisco Unified Communications Manager Serviceability.

Managing User Accounts Using the Cisco Unified Communications Manager BAT

This topic describes how to use Cisco Unified Communications Manager BAT to add users.

Cisco Unified Communications Manager BAT Configuration Process

The Cisco Unified Communications Manager BAT configuration procedure includes these steps:

- Step 1: Configure Cisco Unified CM BAT user template.
- Step 2: Create the CSV data input file.
- Step 3: Upload the CSV data input file.
- Step 4: Start Cisco Unified CM BAT job to add users.
- Step 5: Verify status of Cisco Unified CM BAT job.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-31

The configuration procedure includes these steps:

- Step 1** Configure a BAT user template. This template is configured with default settings that apply to all users (unless overwritten in the comma-separated values [CSV] file).
- Step 2** Create the CSV data input file. This file includes the users to be added to the configuration database. For each user, there will be one record containing all settings of the corresponding user.
- Step 3** Upload the CSV data input file. The CSV file needs to be uploaded to the Cisco Unified Communications Manager publisher server.
- Step 4** Start the BAT job to add users.
- Step 5** Verify status of BAT job.

Step 1: Configuring Cisco Unified Communications Manager BAT User Template

The figure shows the Cisco Unified Communications Manager BAT User Template Configuration page.

Step 1: Configuring Cisco Unified CM BAT User Template

Save

User Template Configuration

User Template Name* CIPT_Users Enter the user template name.

Default Password to User ID

Default PIN to Telephone Number

Default Telephone Number to Primary Extension

Default Mail ID to User ID

Manager User ID

Department

User Locale English, United States

Associated PC

Default Profile < None >

Presence Group* Standard Presence group

SUBSCRIBE Calling Search Space < None >

Allow Control of Device from CTI

User Group Standard CCM End Users

Digest Credentials

Confirm Digest Credentials

Enable Mobility

Enable Mobile Voice Access

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-32

This screenshot shows the 'User Template Configuration' page for Cisco Unified Communications Manager. The 'User Template Name' field is set to 'CIPT_Users'. A callout box points to this field with the text 'Enter the user template name.' Below the configuration table, there is a red box highlighting the 'Default user parameters' section, which includes fields for Manager User ID, Department, User Locale (set to English, United States), Associated PC, Default Profile, Presence Group (set to Standard Presence group), SUBSCRIBE Calling Search Space, and several checkboxes for device control and mobility features. Another callout box points to this red box with the text 'Configure default user parameters.' At the bottom left, it says '© 2008 Cisco Systems, Inc. All rights reserved.' and at the bottom right, 'CIPT1 v6.0—2-32'.

A name for the phone template has to be configured, and the default user configuration parameters have to be selected. These default values can be overwritten with specific values per user name in the data CSV file.

Step 2: Creating the CSV Data Input File

In the next step, the CSV file is created.

Step 2: Creating the CSV Data Input File

Cisco provides a template to create CSV files that have the mandatory format to work with Cisco Unified CM BAT:

- The template is a Microsoft Excel spreadsheet that uses macros.
- The template can be personalized for specific needs.
- The file can also be created using a text editor, such as Microsoft Notepad:
 - Use a separate line to enter data for each record.
 - Separate each data field with a comma and include comma separators for blank fields.
 - Do not enter blank lines, otherwise errors occur during the insert transaction.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-33

The CSV file has to be in a special format and has to include specific values, therefore, it is recommended to create the CSV file by using an Excel macro that can be downloaded from the Cisco Unified Communications Manager server. Use the Upload/Download Files menu item in the Bulk Administration menu to download the file. The Excel macro will allow you to enter the configuration data in a spreadsheet and then save the data in the appropriate CSV format. Alternatively, you can create the CSV file on your own as long as you use the correct sequence of configuration parameters (separated by a comma). Make sure that you follow these rules when creating a CSV file on your own:

- Use a separate line to enter data for each record.
- Separate each data field with a comma and include comma separators for blank fields.
- Do not enter blank lines; otherwise, errors occur during the insert transaction.

Step 3: Uploading CSV Data Input Files

Now the CSV file has to be uploaded to Cisco Unified Communications Manager.

Step 3: Uploading CSV Data Input File

File Upload Configuration

Upload the CSV file

File: * C:\XlsDataFiles\Users-09202007130337.txt

Select The Target * Users

Select Transaction Type * Insert Users

Overwrite File if it exists.**

a) Select the user data file.
b) Select target.
c) Select activity type.
d) Start file upload.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-34

You have to specify the local file, the configuration target (users, phones, gateways, and so on), and the transaction type (add, delete, or update).

Note At this time, you only uploaded the CSV file. The selected transaction type will not be executed unless you proceed with the next step.

Step 4: Starting Cisco Unified Communications Manager BAT Job to Add Users

The figure shows the Insert Users Configuration page.

Step 4: Starting Cisco Unified CM BAT Job to Add Users

Insert Users Configuration

Insert Users

File Name * [\(View File\)](#) [\(View Sample File\)](#)

User Template Name *

File created with Export Users

Job Information

Job Description

Run Immediately Run Later (To schedule and activate this job, use Job Scheduler page.)

Submit

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-35

To start a BAT job for adding users, go to **Cisco Unified Communications Manager Administration > Bulk Administration > Users > Insert Users**. At the Insert Users configuration page, select the phone template (which you created in step 1), the CSV file (which you created and uploaded in steps 2 and 3), and specify to either run the job immediately or to run the job later. If you choose the option to run the job later, you will have to configure the start time using the Job Scheduler.

Step 5a: Job Status – List of Jobs

The submitted BAT job can be configured (in case of a scheduled job) or monitored using the Job Scheduler.

The screenshot shows the 'Find and List Jobs' page with the title 'Step 5a: Job Status: List of Jobs'. At the top, there are buttons for 'Select All', 'Clear All', 'Delete Selected', 'Activate Selected', and 'Stop Processing'. Below this is a status bar indicating '1 records found'. The server date and time is listed as 'September 20, 2007 14:15:37 PDT'. A search bar allows filtering by 'User' and 'Scheduled Date Time'. The main table displays one job entry:

Job Id	Scheduled Date Time	Submit Date Time	Description	Status	Last User
119032295	September 20, 2007 14:09:55 PDT	September 20, 2007 14:09:55 PDT	Insert Users	Completed	CCMAdministrator

Below the table are buttons for 'Select All', 'Clear', 'Delete Selected', 'Activate Selected', and 'Stop Processing'. Two callouts point to specific elements: 'a) Click Job Id to see details.' points to the 'Job Id' column, and 'b) See job status.' points to the 'Status' column.

To access the Job Scheduler, go to **Cisco Unified Communications Manager Administration > Bulk Administration > Job Scheduler**. The Job Scheduler provides a list of jobs, displays the status of the jobs, and allows configuration of the start time for scheduled jobs.

Step 5b: Verifying Job Status – Job Details

When clicking a job ID from the list of BAT jobs displayed by the Job Scheduler, you can obtain details about the corresponding BAT job.

Step 5b: Verifying Job Status: Job Details

Job Scheduler Related Links: [Back To Find/List](#) [G](#)

Status: (i) Status: Ready

Server Date and Time: September 20, 2007 14:10:27 PDT

Job Details:

Job id*	1190322595
Job Status*	Completed
Scheduled Date Time	09/20/2007 14:09:55
Submit Date Time	09/20/2007 14:09:55
Sequence*	1
Job Description	Insert Users
Frequency*	Once
Job End Time	
Last Modified By	CCMAdministrator

a) See job result information.
b) Click to open log file.

Transaction Details:

CSV File Name	Users-09202007130337.txt
User Template Name	CIPT_Users

Job Results:

Job Launched Date Time	Job Result Status	Number Of Records Processed	Number Of Records Failed	Total Number Of Records	Log File Name.
09/20/2007 14:10:05	Success	2	0	2	1190322595#09202007140956.txt

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-37

The job details include information about the job result, the number of records processed, and the number of records failed. If you want to see more details, for example, if your job had errors, then click the log file name.

LDAP Overview

This topic describes LDAP directory services.

LDAP Characteristics

- LDAP directories typically store data that do not change often, e.g. employee information.
- Information is stored in a database optimized for these instances:
 - High number of read and search requests
 - Occasional write and update requests
- LDAP directories store all user information in a single, centralized repository available to all applications.
- LDAP directories provide applications with a standard method for accessing and modifying information.
 - LDAPv3 – Lightweight Directory Access Protocol version 3

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-39

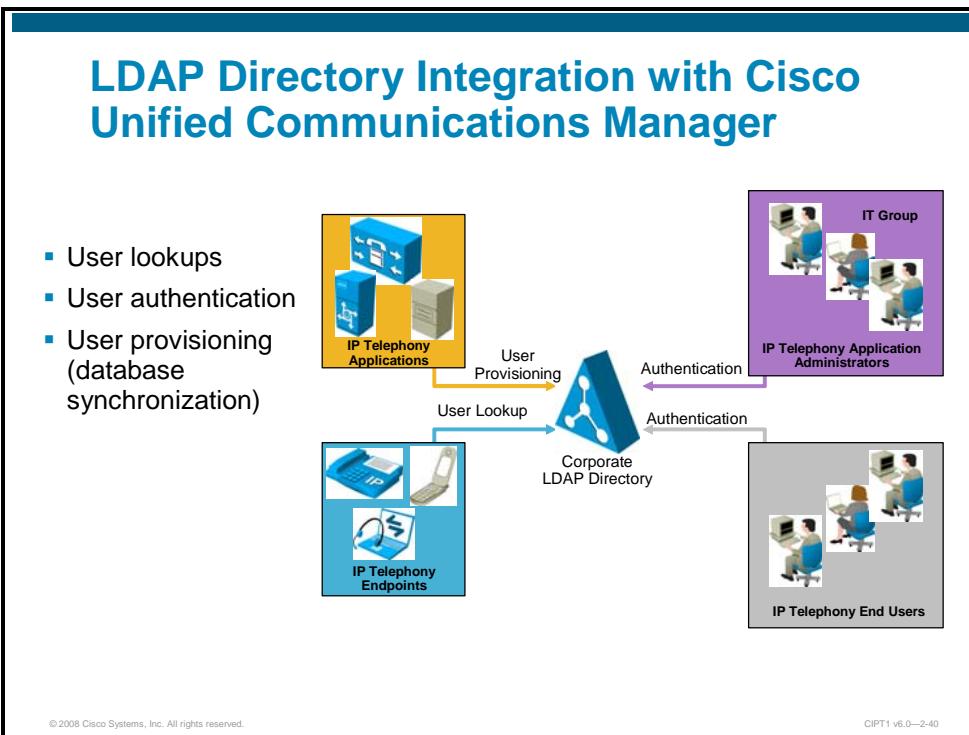
LDAP directories typically store data that do not change often, such as employee information, user privileges on the corporate network, and so on.

The information is stored in a database that is optimized for a high number of read and search requests and occasional write and update requests.

LDAP directories store all user information in a single, centralized repository that is available to all applications. Applications can access the directory using the LDAP, providing a standard method for reading and potentially modifying the information stored in the directory.

LDAP Directory Integration with Cisco Unified Communications Manager

Cisco Unified Communications Manager can integrate with LDAP directories in order to benefit from a centralized user repository.



Integration between voice applications and a corporate LDAP directory is a common task for many enterprise IT organizations. However, the exact scope of the integration varies from company to company, and it can translate to one or more specific and independent requirements.

For example, one common requirement is to enable user lookups (sometimes called the "white pages" service) from IP phones, so that users can dial a contact directly after looking up its number in the directory.

Another requirement is to provision users automatically from the corporate directory into the user database of unified communications applications. This method avoids having to add, remove, or modify core user information manually each time that a change occurs in the corporate directory.

Often, authentication of end users and administrators of the unified communications applications using the corporate directory credentials is also required. This method enables the IT department to deliver single log-on functionality and reduces the number of passwords that each user needs to maintain across different corporate applications.

Each of these requirements can be satisfied by a Cisco Unified Communications system using different mechanisms according to the Cisco Unified Communications Manager version used.

Cisco Unified IP Phones equipped with a display screen can search a user directory when a user presses the Directories button on the phone. The IP phones use HTTP to send requests to a web server. The responses from the web server must contain some specific Extensible Markup Language (XML) objects that the phone can interpret and display.

By default, Cisco Unified IP phones are configured to perform user lookups against the embedded database of Cisco Unified Communications Manager. However, it is possible to change this configuration so that the lookup is performed on a corporate LDAP directory. In this case, the phones send their HTTP requests to an external web server that operates as a proxy and translates these requests into LDAP queries against the corporate directory. The LDAP responses are then encapsulated in the appropriate XML objects and sent back to the phones via HTTP.

LDAP Support in Cisco Unified Communications Manager

Cisco Unified Communications Manager supports two types of LDAP integration and can interact with several LDAP servers.

LDAP Support in Cisco Unified CM

- Supported directories.
 - Microsoft Active Directory (2000 and 2003)
 - Netscape Directory Server 4.x
 - iPlanet Directory Server 5.1
 - SunONE Directory Server 5.2
- Cisco Unified CM supports two types of integration.
 - LDAP synchronization
 - LDAP authentication
- When using LDAP, some end-user data are no longer controlled via Cisco Unified CM administration.
- Application users are **not** affected by LDAP integration.
 - Always configured from Cisco Unified CM Administration.
 - All application user data are always stored in Cisco Unified CM database.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-41

Cisco Unified Communications Manager supports the following directories:

- Microsoft Active Directory (2000 and 2003)
- Netscape Directory Server 4.x
- iPlanet Directory Server 5.1
- Sun ONE Directory Server 5.2
- Cisco Unified Communications Manager supports two types of LDAP integration, which can be enabled independent of each other:
 - **LDAP synchronization:** Allows user provisioning where personal and organizational data are managed in an LDAP directory and replicated to the Cisco Unified Communications Manager configuration database.
 - **LDAP authentication:** Allows user authentication against an LDAP directory. When using LDAP authentication, passwords are managed in LDAP.

Note	Application users are not affected by LDAP integration. They are always configured from Cisco Unified Communications Manager Administration, and their data are always stored in the Cisco Unified Communications Manager configuration database.
-------------	---

LDAP Integration: Synchronization

LDAP synchronization is used for user provisioning.

LDAP Integration: Synchronization

LDAP is used for user provisioning

- Users cannot be added or deleted from Cisco Unified CM Administration.
- Users are added or deleted in LDAP directory.
- All personal and organizational user data are configured in LDAP.
- Users and their personal and organizational data are replicated from LDAP to Cisco Unified CM; these data are read-only in Unified CM Administration.
- User passwords and Cisco Unified CM settings are still configured from Cisco Unified CM Administration; they cannot be configured in LDAP.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-42

This process uses a service called directory synchronization (DirSync) on Cisco Unified Communications Manager to synchronize a number of user attributes (either upon request or periodically) from a corporate LDAP directory. When this feature is enabled, users are automatically provisioned from the corporate directory.

When using this feature, end users cannot be added or deleted from Cisco Unified Communications Manager Administration. They are added and deleted in the LDAP directory, and all personal or organizational settings associated with the users are configured in LDAP.

Users and their associated personal and organizational data are replicated from LDAP to Cisco Unified Communications Manager. These parameters are read-only in Cisco Unified Communications Manager Administration. User passwords and Cisco Unified Communications Manager settings are still configured from Cisco Unified Communications Manager Administration and are stored only in the Cisco Unified Communications Manager database. Therefore, these settings cannot be configured in LDAP.

Cisco Unified Communications Manager LDAP Synchronization Data Storage

The table shows how different user data are treated when using LDAP synchronization and contrasts it to a scenario where no LDAP integration is used or LDAP authentication is enabled.

	No LDAP Integration	LDAP Synchronization	LDAP Authentication
Personal and organizational settings: User ID First, Middle, and Last Name Manager User ID and Department Phone Number and Mail ID	Local	LDAP (replicated to local)	LDAP (replicated to local) or Local
Password	Local	Local	LDAP
Cisco Unified CM Settings: PIN and Digest Credentials Groups and Roles Associated PCs Controlled Devices Extension Mobility Profile and CAPF Presence Group and Mobility	Local	Local	Local

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-43

LDAP Integration: Authentication

LDAP authentication is used to authenticate users against the LDAP directory instead of having passwords stored in the Cisco Unified Communications Manager database.

LDAP Integration: Authentication

LDAP is used for user authentication

- Users must exist in LDAP directory (LDAP synchronization not mandatory but recommended).
- User passwords are configured and stored in LDAP only.
- User passwords are **not** replicated to Cisco Unified CM database and cannot be configured from Cisco Unified CM Administration or Cisco Unified CM User web pages.
- User authentication is performed against LDAP directory (fails if LDAP directory is not accessible).
- Users and their personal and organizational data are still stored in Cisco Unified CM local database.
 - Replicated from LDAP if LDAP synchronization is used
 - Locally configured via Cisco Unified CM Administration if LDAP synchronization is not used

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-44

With LDAP authentication, Cisco Unified Communications Manager authenticates user credentials against a corporate LDAP directory. When this feature is enabled, end-user passwords are not stored in the Cisco Unified Communications Manager database anymore (and also are not replicated to that database) but are only stored in the LDAP directory.

Personal user data are either managed in LDAP and replicated into the Cisco Unified Communications Manager database (if LDAP synchronization is enabled) or are controlled only (managed and stored) by Cisco Unified Communications Manager.

Cisco Unified Communications Manager user data (such as associated PCs or controlled devices) are stored in the Cisco Unified Communications Manager database for each individual user. As a consequence, the username has to be known in the Cisco Unified Communications Manager database (to assign Cisco Unified Communications Manager user settings to the user) and in the LDAP directory (to assign the password to the user). In order to avoid separate management of user accounts in these two databases, it is recommended to combine LDAP authentication with LDAP synchronization.

Cisco Unified Communications Manager LDAP Authentication Data Storage

The table shows how different user data are treated when using LDAP authentication and contrasts it to a scenario where no LDAP integration is used or LDAP synchronization is enabled.

	No LDAP Integration	LDAP Synchronization	LDAP Authentication
Personal and organizational settings: User ID First, Middle, and Last Name Manager User ID and Department Phone Number and Mail ID	Local	LDAP (replicated to local)	LDAP (replicated to local) or Local
Password	Local	Local	LDAP
Cisco Unified CM Settings: PIN and Digest Credentials Groups and Roles Associated PCs Controlled Devices Extension Mobility Profile and CAPF Presence Group and Mobility	Local	Local	Local

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-45

LDAP Integration Considerations

This section provides information about LDAP integration considerations.

LDAP Integration Considerations

- Full synchronization.
 - Microsoft Active Directory 2000
 - Microsoft Active Directory 2003
- Incremental synchronization.
 - Netscape Directory Server 4.x
 - iPlanet Directory Server 5.1
 - SunONE Directory Server 5.2
- All synchronization agreements must integrate with the same LDAP family (Microsoft Active Directory or Netscape, iPlanet, and SunONE).
- Cisco Unified CM uses standard LDAPv3 to access data.
- One LDAP user attribute is chosen to map into the Cisco Unified CM User ID field.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-46

Depending on the directory server used, LDAP synchronization is performed in one of the following ways:

- **Full synchronization:** This method is used with Microsoft AD 2000 and 2003. Full synchronization means that all records are replicated from the LDAP directory to the Cisco Unified Communications Manager database. In large deployments, this method can cause considerable load; therefore, synchronization times and jobs have to be carefully selected.
- **Incremental synchronization:** This method is used with all other supported directory servers. As only changes are propagated to the Cisco Unified Communications Manager database, this method requires fewer resources than the full synchronization method.

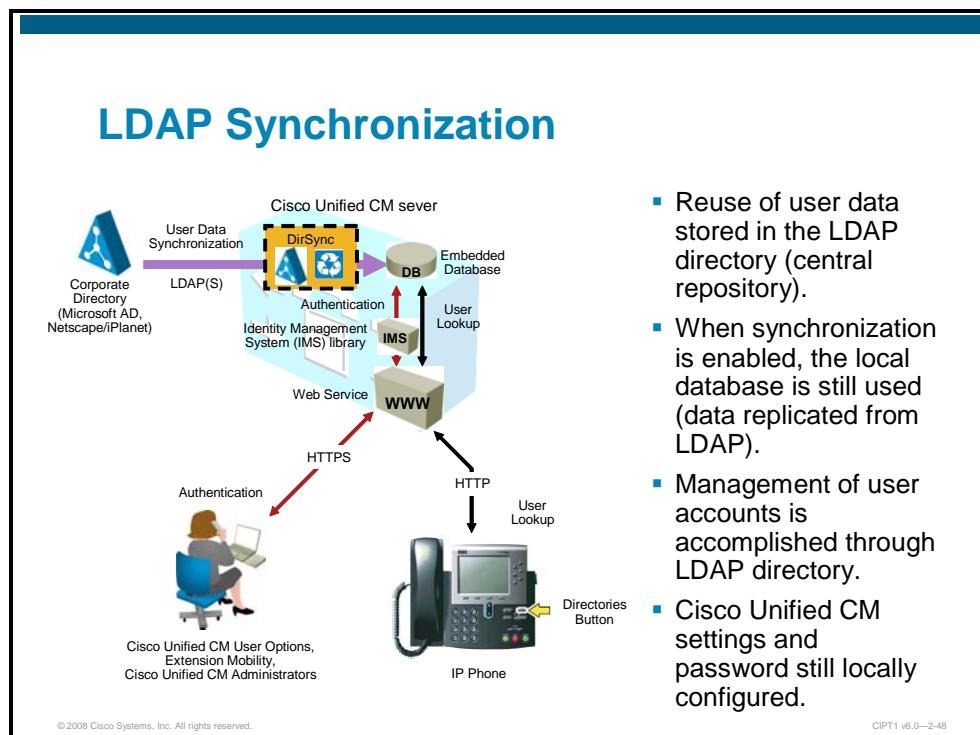
All synchronization agreements (these are pointers to a certain domain or sub-domain within an LDAP structure) have to use the same synchronization method. You cannot mix synchronization agreements with Microsoft AD and any other LDAP server.

Cisco Unified Communications Manager uses the LDAP version 3.

One LDAP user attribute (for example sAMAccountName, uid, mail, or telephoneNumber) has to be mapped to the User ID field of a user in Cisco Unified Communications Manager and must be unique across all users.

Using LDAP for User Provisioning

This topic describes how to enable LDAP synchronization in Cisco Unified Communications Manager.



Synchronization of Cisco Unified Communications Manager with a corporate LDAP directory allows reusing data stored in the LDAP directory and allows the corporate LDAP directory to serve as the central repository for that information. Cisco Unified Communications Manager has an integrated database for storing user data and a web interface within Cisco Unified Communications Manager Administration for creating and managing user data in that database. When synchronization is enabled, that local database is still used, but the Cisco Unified Communications Manager facility to create user accounts becomes disabled. Management of user accounts is then accomplished through the interface of the LDAP directory.

The user account information is imported from the LDAP directory into the database located on the Cisco Unified Communications Manager publisher server. Information that is imported from the LDAP directory may not be changed from Cisco Unified Communications Manager administration. Additional user information specific to the Cisco Unified Communications Manager implementation is managed by Cisco Unified Communications Manager and stored only within its local database. For example, device-to-user associations, speed dials, and user PINs are data that are managed by Cisco Unified Communications Manager, and they do not exist in the corporate LDAP directory.

LDAP Synchronization – Data Attributes Imported by Cisco Unified Communications Manager

The table shows which information is replicated from LDAP to the Cisco Unified Communications Manager database and how the LDAP user attributes map to the Cisco Unified Communications Manager user attributes.

LDAP Synchronization: Data Attributes Imported by Cisco Unified CM		
Cisco Unified CM Field	MS Active Directory Attribute	Netscape, iPlanet, Sun ONE
User ID	One of: sAMAccountName mail employeeNumber telephoneNumber UserPrincipalName	One of: uid mail employeeNumber telephonePhone
First Name	givenName	givenname
Middle Name	One of: middleName Initials	initials
Last Name	sn	sn
Manager ID	manager	manager
Department	department	department
Phone Number	One of: telephoneNumber ipPhone	telephonenumber
Mail ID	One of: mail sAMAccountName	One of: mail uid

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-49

The data that Cisco Unified Communications Manager imports are all from standard LDAP user attributes. As shown in the table, the attributes differ between the two groups of LDAP servers.

LDAP Attributes Mapping

Some rules have to be followed regarding the attribute mappings.

LDAP Attributes Mapping

Mapping LDAP directory attributes to Cisco Unified CM:

- The data of the directory attribute that is mapped to the Cisco Unified CM user ID must be unique within all entries for that cluster.
- The “sn” attribute (last name) must be populated with data, otherwise that record will not be imported.
- If the primary attribute used during import of end-user accounts matches an application user, that user is skipped.
- Some Cisco Unified CM database fields provide a choice of directory attributes; choose only a single mapping for each field.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-50

The data of the directory attribute that is mapped to the Cisco Unified Communications Manager User ID must be unique within all entries for that cluster. The “sn” attribute must be populated with data, otherwise that record will not be imported from the corporate directory. If the primary attribute used during import of end-user accounts matches any application user in the Cisco Unified Communications Manager database, that user is skipped.

Some Cisco Unified Communications Manager database fields provide a choice of directory attributes, but you can choose only a single mapping for each synchronization agreement.

Synchronization Agreements

This section describes synchronization agreements.

Synchronization Agreements

Synchronization agreements specify search bases.

- When Cisco DirSync is enabled, one or more synchronization agreements can be configured.
 - An agreement specifies a search base that is a position in the LDAP tree, where Cisco Unified CM will begin its search.
 - Cisco Unified CM can import only end users that exist in the area of the domain specified in the search base.
- When users are organized in a structure in the LDAP directory, use that structure to control which user groups are imported.
- A synchronization agreement can be used to specify the root of the domain, but that search base would import all user accounts.
 - The search base does not have to specify the domain root.
 - The search base may specify any point in the tree.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-51

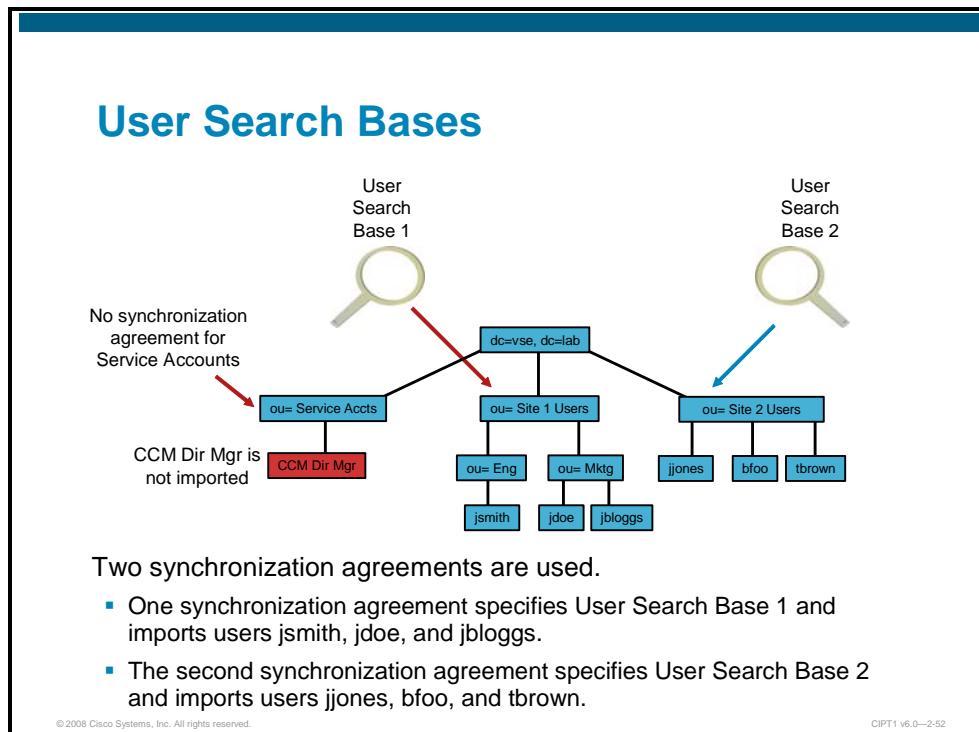
A synchronization agreement specifies a so-called search base. A search space is an area of the directory that should be considered for the synchronization. This consideration is achieved by specifying a position in the directory tree where Cisco Unified Communications Manager begins its search (that is, it has access to all lower levels but not to higher levels).

When users are organized in a structure in the LDAP directory, you can use that structure to control which user groups are imported. If a single synchronization agreement specifies the root of the domain, all users of the domain (including service accounts) will be synchronized. The search base does not have to specify the domain root; it may specify any point in the tree.

Note	As discussed in a later section of this lesson, synchronization agreements with Microsoft Active Directory roots work in a different way.
-------------	---

User Search Bases

The figure shows an example with three top-level organizational units, where two of them are specified as user search bases in synchronization agreements.



In this figure, two synchronization agreements are represented. One synchronization agreement specifies User Search Base 1 and imports users jsmith, jdoe, and jbloggs. The other synchronization agreement specifies User Search Base 2 and imports users jjones, bfoo, and tbrown. The CCMDirMgr account is not imported because it does not reside within one of the two user search bases.

The structure in this LDAP directory was used to control which users are synchronized. In this example, a single synchronization agreement could have been used to specify the root of the domain, but that search base would also have imported the CCMDirMgr user located under Service Accts.

To import the data into the Cisco Unified Communications Manager database, the system performs a bind to the LDAP directory using the account specified in the configuration as the LDAP Manager Distinguished Name, and reading of the database is done with this account. The account must be available in the LDAP directory for Cisco Unified Communications Manager to log in, and it is recommended that you create a specific account with the permission to read all user objects within the subtree that was specified by the user search base.

The synchronization agreement specifies the fully distinguished name of that account so that the account may reside outside of the configured search bases, anywhere within the domain. In the example, CCMDirMgr is the account used for the synchronization.

It is possible to control the import of accounts by limiting read permissions of the LDAP manager distinguished name account. In this example, if that account is restricted to have read access to ou=Eng but not to ou =Mktg, then only the accounts located under Eng will be synchronized.

Synchronization agreements have the ability to specify multiple directory servers to provide redundancy.

You can specify an ordered list of up to three directory servers in the configuration that will be used when attempting to synchronize. The servers are tried, in order, until the list is exhausted. If none of the directory servers responds, then the synchronization fails, but it will be attempted again according to the configured synchronization schedule.

Synchronization Mechanism

This section describes synchronization agreement characteristics and depicts the synchronization process.

Synchronization Mechanism

Synchronization mechanism characteristics

- The synchronization agreement specifies
 - A time for synchronizing to begin
 - A period for re-synchronizing (hours, days, weeks, or months)
- A synchronization agreement can also be set up to run only once.
- Synchronization process
 - All existing Cisco Unified CM end-user accounts are deactivated.
 - LDAP end-user accounts that exist in Cisco Unified CM database (now deactivated) are activated and settings are updated (if different in LDAP).
 - LDAP end-user accounts that exist in LDAP only are added to Cisco Unified CM database (and activated).
 - Deactivated accounts are purged from Cisco Unified CM database after 24 hours.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-53

Each synchronization agreement is configured with the time when the synchronization should begin and a period (hours, days, weeks, or months) for resynchronization. A synchronization agreement can also be configured to run only once.

The synchronization process is as follows:

- At the beginning of the synchronization process, all existing Cisco Unified Communications Manager end-user accounts are deactivated.
- LDAP user accounts that exist in the Cisco Unified Communications Manager database (which are now deactivated) are reactivated, and their settings are updated if there are any changes. This step ensures that updates are propagated.
- LDAP user accounts that exist in LDAP only are added to the Cisco Unified Communications Manager database and activated. This step enables new users to be provisioned.
- Deactivated accounts are purged from the Cisco Unified Communications Manager database after 24 hours. This step enables the “safe” deletion of users.

Note	The deletion is safe because deactivated accounts are not deleted immediately. An accidentally deleted user will not lose all of its parameters (password if LDAP authentication is not used, and all Cisco Unified Communications Manager settings), which are stored only in the Cisco Unified Communications Manager database, if the user is added back into LDAP within 24 hours. If the accidental deletion is discovered after 24 hours, and the user is added back into LDAP, all user parameters that were stored in Cisco Unified Communications Manager are lost and have to be reconfigured.
-------------	--

LDAP Synchronization Best Practices

This section lists best practices when enabling LDAP synchronization.

LDAP Synchronization Best Practices

- Use a specific account within the corporate directory to allow the Cisco Unified CM synchronization agreement to connect and authenticate.
 - Dedicated account for Cisco Unified CM
 - Minimum permissions set to “read” all user objects
 - Password set to “never to expire”
- Choose synchronization times that occur during quiet periods.
- When having multiple synchronization agreements, configure them with different start times to reduce load.
- Ensure the LDAP directory attribute chosen to map into the Cisco Unified CM user ID is unique within all synchronization agreements.
- Configure at least two LDAP servers for redundancy and use IP addresses instead of hostnames.
- Enable Secure LDAP.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-54

The account that Cisco Unified Communications Manager uses to read the LDAP directory should be configured in the following way:

- A dedicated account used only for this purpose should be created.
- The account should be permitted to read all user objects located below the user search bases specified in the synchronization agreements.
- The password of the account should be set to never expire.

Synchronization times should be set to non-office hours to minimize any potential impact to call processing caused by the load during synchronization.

When multiple synchronization agreements are configured, different start times should be set to reduce the load on the servers.

Ensure that the LDAP directory attribute that is chosen to map the Cisco Unified Communications Manager User ID (for example, sAMAccountName or uid) is unique across all synchronization agreements and that the name is not used as an application user inside Cisco Unified Communications Manager.

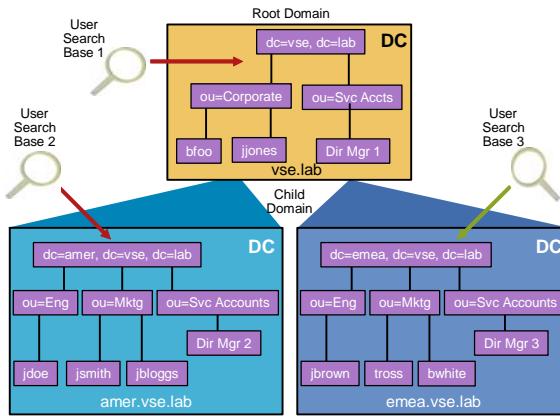
Avoid a single point of failure by configuring at least two LDAP servers and use IP addresses instead of hostnames to eliminate Domain Name System (DNS) reliance.

The connection between the Cisco Unified Communications Manager publisher server and the directory server can be secured by enabling Secure LDAP on Cisco Unified Communications Manager and the LDAP server. Secure LDAP enables LDAP to be sent over a Secure Sockets Layer (SSL).

Integrating Microsoft Active Directory with Multiple Active Directory Domains

This section provides information that must be considered when integrating with Microsoft Active Directory with multiple active directory domains.

Considerations for Microsoft Active Directory with Multiple Active Directory Domains



- A synchronization agreement for a domain will not synchronize users outside of that domain nor within a child domain.
- Three synchronization agreements are required to import all users in this example.
- Although User Search Base 1 specifies the root, it will not import users that exist in either of the child domains.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-65

In the figure, each of the domains and subdomains is associated to at least one domain controller, and three synchronization agreements each specify the appropriate domain controller as LDAP server. The domain controllers have information only on users within the domain where they reside; therefore, three synchronization agreements are required to import all of the users.

Note	The information provided earlier, that a single search base pointing to the top root would include all child domains, does not apply in this case.
-------------	--

Integrating Microsoft Active Directory with Multiple Active Directory Trees

This section provides information that must be considered when integrating with Microsoft Active Directory with multiple active directory trees.

Considerations for Microsoft Active Directory with Multiple Active Directory Trees

- When synchronization is enabled with an Active Directory forest containing multiple trees, multiple synchronization agreements are needed (two in this example).
- The UserPrincipalName (UPN) attribute is guaranteed by Active Directory to be unique across the forest.
- The UPN must be chosen as the attribute that is mapped to the Cisco Unified CM user ID.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-56

When synchronization is enabled with an active directory forest containing multiple trees, as shown in the figure, multiple synchronization agreements are needed for the same reasons previously listed. In addition, the UserPrincipalName (UPN) attribute must be chosen as the attribute that is mapped to the Cisco Unified Communications Manager UserID, because only this one is guaranteed by Microsoft Active Directory to be unique across the forest.

LDAP Synchronization Configuration Procedure

This section lists the required steps for enabling LDAP synchronization.

LDAP Synchronization Configuration Procedure

1. Add Cisco Unified CM directory user and assign administrator access rights in LDAP directory (depends on used LDAP directory server).
2. Activate Cisco DirSync service.
3. Configure the LDAP system.
4. Configure the LDAP directory.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-57

The LDAP synchronization configuration procedure includes the following steps:

- Step 1** Add Cisco Unified Communications Manager directory user and assign administrator access rights in LDAP directory (this configuration depends on LDAP directory server that is used).
- Step 2** Activate Cisco DirSync service.
- Step 3** Configure the LDAP system.
- Step 4** Configure the LDAP directory.

Step 2: Activate Cisco DirSync Service

The second configuration task in Cisco Unified Communications Manager is to activate the Cisco DirSync service.

Step 2: Activate Cisco DirSync Service

- In Cisco Unified CM Serviceability, navigate to **Tools > Service Activation**.
- Select the publisher server and activate the Cisco DirSync service.
- Verify in **Tools > Control Center – Feature Services** that the Cisco DirSync service is running.

Service Activation

Directory Services		Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco DirSync		Activated

Control Center – Feature Services

Directory Services		Service Name	Status*	Activation Status	Start Time	Up Time
<input checked="" type="radio"/>	Cisco DirSync	Started	Activated	Wed Jun 20 01:45:04 2007	0 days 04:27:51	

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-58

The synchronization is performed by a feature service called Cisco DirSync, which is enabled through the Serviceability web page. It has to be activated on the publisher server.

The Cisco DirSync service has some configurable service parameters that can be configured under **Cisco Unified Communications Manager Administration > System > Service Parameters**, followed by the selection of the Cisco DirSync service. These service parameters include the maximum number of synchronization agreements, the maximum number of hosts (directory servers), and several timers.

Step 3: LDAP System Configuration

The next step is the configuration of the LDAP system.

Step 3: LDAP System Configuration

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System > LDAP > LDAP System

LDAP System Configuration

Status: Status: Ready

LDAP System Information:

- Enable Synchronizing from LDAP Server
- LDAP Server Type: Microsoft Active Directory
- LDAP Attribute for User ID: sAMAccountName

* indicates required item.

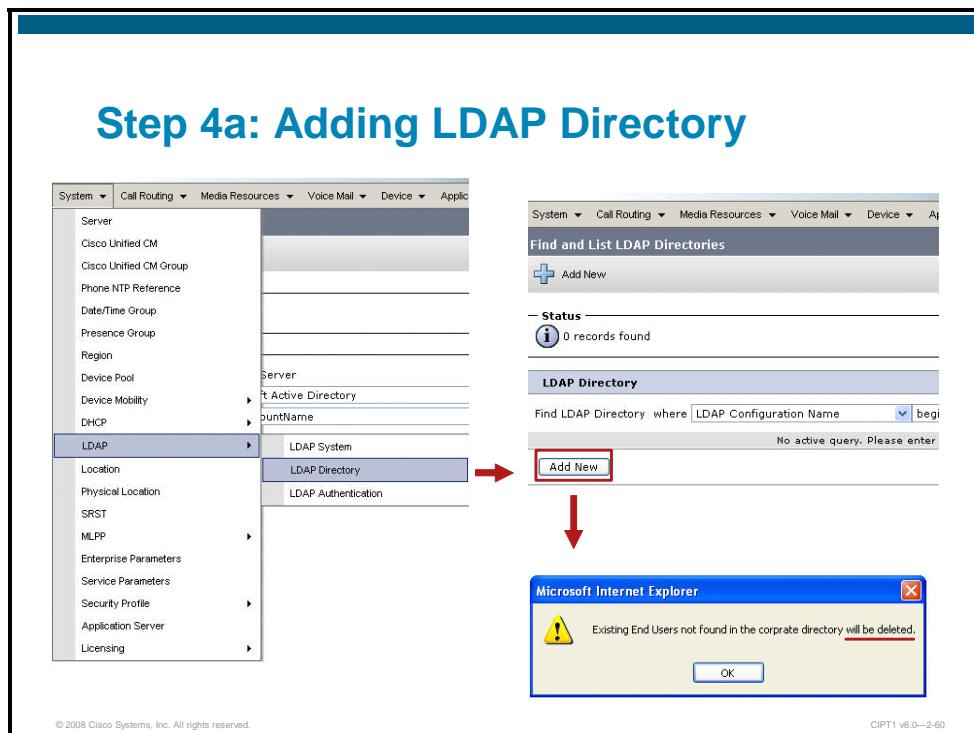
Save

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-59

Go to **System > LDAP > LDAP System** to configure the LDAP server type (Microsoft Active Directory or other) and the LDAP attribute that should be mapped to the Cisco Unified Communications Manager User ID. Activate the Enable Synchronization check box from LDAP server.

Step 4a: Adding LDAP Directory

The final configuration task, adding the LDAP directory, has to be performed once per synchronization agreement (once per different user search base).



Go to **System > LDAP > LDAP Directory** and click **Add New** to add a new synchronization agreement. A warning will be displayed indicating that all existing end users that are not found in the LDAP directory will be deleted.

Step 4b: LDAP Directory Configuration

After confirming the warning by clicking **OK**, the LDAP Directory configuration page is displayed.

Step 4b: LDAP Directory Configuration

LDAP Directory

LDAP Configuration Name * VSE Corporate Directory

LDAP Manager Distinguished Name * Directory Manager

LDAP Password *

Confirm Password *

LDAP User Search Base * ou=site-1, dc=vse, dc=lab

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every * 7 DAY

Next Re-sync Time (YYYY-MM-DD hh:mm) * 2007-07-03 00:00

User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP User Fields	Cisco Unified Communications Manager User Fields	LDAP User Fields
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	telephoneNumber	Mail ID	mail

LDAP Server Information

Host Name or IP Address for Server * 192.168.10.10

Add Another Redundant LDAP Server

LDAP Port * 389 Use SSL

Save

At the LDAP Directory configuration page, you have to configure the following parameters:

- Cisco Unified Communications Manager directory user as configured in the LDAP directory (as stated in step 1)
- User search base
- Synchronization schedule
- User field mappings
- LDAP server(s)

LDAP Synchronization Verification

To verify successful LDAP synchronization, go to **User Management > End User** and check the LDAP Sync Status for the listed users.

LDAP Synchronization Verification

- Navigate to **User Management > End User** and click **Find**.
- The synchronized users are marked Active.
- Inactive users were configured on Cisco Unified CM but not in LDAP directory and will be deleted after 24 hours.

User (1 - 3 of 3)						Rows per Page: 50
Find User where First name begins with						Find Clear Filter
	User ID	First Name	Last Name	Department	LDAP Sync Status	
<input type="checkbox"/>	dmckoy	Danny	McKoy		Inactive	
<input type="checkbox"/>	edeline	Ed	Deline		Active	
<input type="checkbox"/>	lgibbs	Leroy	Gibbs		Active	

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—2-62

Synchronized users are marked active; inactive users were configured in Cisco Unified Communications Manager but not in LDAP and will be deleted after 24 hours. Note that you cannot add or delete users.

LDAP Synchronization Verification (Cont.)

- The Add and Delete function is disabled for end users.
- Personal user settings (user ID, names, manager, etc.) are read-only (as configured in LDAP and replicated to Cisco Unified CM).
- Password and Cisco Unified CM settings (PIN, associated PC, digest credentials, etc.) are still configured in Cisco Unified CM.

User Information

NOTE: The add and delete function are disabled because the user directory is sync with LDAP.
(i.e. The Enable Synchronization From LDAP Server flag on the LDAP System Configuration is checked).

LDAP Sync Status	Active
User ID*	lgibbs
Password	[REDACTED]
Confirm Password	[REDACTED]
PIN	[REDACTED]
Confirm PIN	[REDACTED]
Last name*	Gibbs
Middle name	
First name	Leroy
Telephone Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC	
Digest Credentials	
Confirm Digest Credentials	

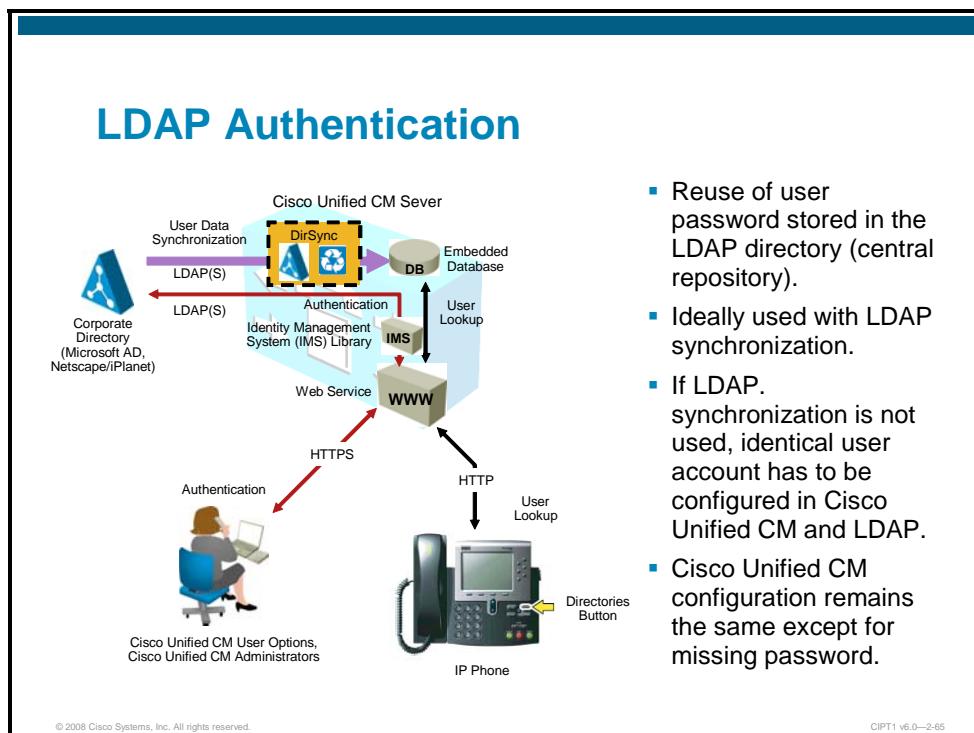
© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-63

When clicking an active user, you will get to the configuration page of the particular user. You will note that you cannot change the username and personal or organizational settings, but you can modify password and Cisco Unified Communications Manager settings such as PIN, digest credentials, and associated PC.

Using LDAP for User Authentication

This topic describes how to enable LDAP authentication in Cisco Unified Communications Manager.



The LDAP authentication function can be enabled independently of the LDAP synchronization function. However, if authentication is enabled alone, the user IDs in Cisco Unified Communications Manager match the user IDs defined in the corporate directory. Due to the high potential of errors, it is recommended to combine LDAP authentication and LDAP synchronization.

The following statements describe the behavior of Cisco Unified Communications Manager when LDAP authentication is enabled:

- End-user passwords are authenticated against the corporate directory.
- End-user passwords are managed in LDAP, not in Cisco Unified Communications Manager.
- End-user passwords are stored only in LDAP; they are not replicated to Cisco Unified Communications Manager.

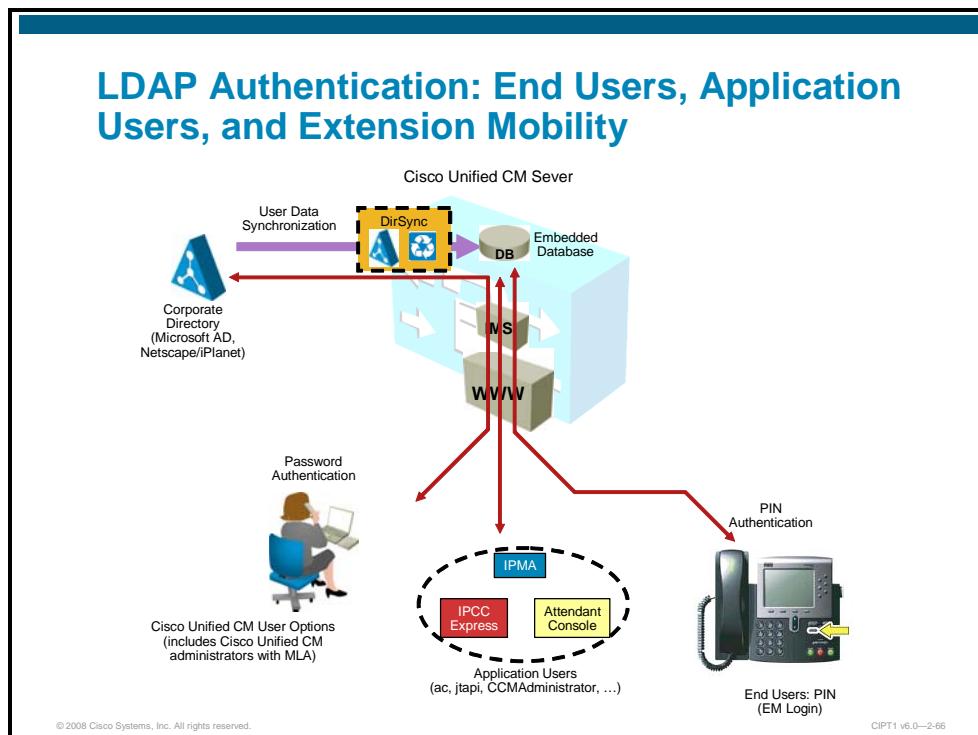
Application users are still authenticated against the Cisco Unified Communications Manager database. Their passwords are stored only in the Cisco Unified Communications Manager database.

End-user PINs and other Cisco Unified Communications Manager user settings are configured and stored in Cisco Unified Communications Manager only.

Personal and organizational user settings such as phone number, manager, first, middle, and last name are either managed and stored in LDAP and replicated to Cisco Unified Communications Manager (if LDAP synchronization is used) or managed and stored in Cisco Unified Communications Manager only (if LDAP synchronization is not used).

LDAP Authentication – End Users, Application Users, and Extension Mobility

The figure shows a scenario with LDAP authentication for end users.



In the example, LDAP authentication is enabled. Therefore, end users are authenticated against the LDAP directory. Application users, however, are still authenticated against the Cisco Unified Communications Manager database (because application LDAP authentication only applies to end users). When an end user logs in to an application that checks the PIN of the user (such as with Cisco Unified Communications Manager Extension Mobility), the PIN of the end user is NOT authenticated against LDAP, because the PIN is a Cisco Unified Communications Manager user setting that is not stored in LDAP.

LDAP Authentication Best Practices

This section lists best practices when enabling LDAP authentication.

LDAP Authentication Best Practices

- Create an account within the corporate directory to allow Cisco Unified CM to connect and authenticate to it.
- Configure at least two LDAP servers for redundancy.
- Manage end-user passwords from within the corporate directory interface.
- Manage end-user PINs from Cisco Unified CM Administration or from the User Options page.
- Manage application user passwords from Cisco Unified CM Administration.
- Enable single logon for Cisco Unified CM administrators by adding their corresponding end user to the Cisco Unified CM Super Users user group.
- When enabling LDAP authentication with Microsoft Active Directory, configure Cisco Unified CM to query a Microsoft Active Directory global catalog server for faster response times.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-67

Use a dedicated account in the LDAP directory, used only by Cisco Unified Communications Manager for the purpose of interacting with LDAP.

Avoid a single point of failure by configuring at least two LDAP servers and use IP addresses instead of hostnames to eliminate DNS reliance.

End users have to manage their passwords from within the LDAP directory.

End users have to manage their PINs from Cisco Unified Communications Manager User web pages. Alternatively, the Cisco Unified Communications Manager administrator can manage PINs from Cisco Unified Communications Manager Administration.

Application users are always managed from Cisco Unified Communications Manager Administration only.

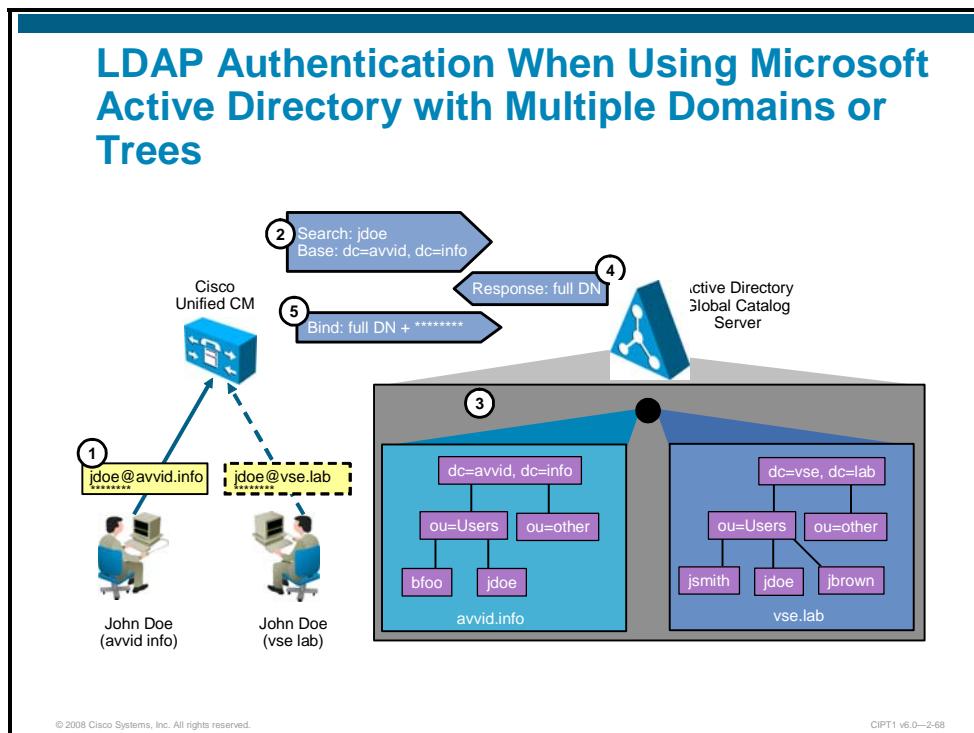
Cisco Unified Communications Manager administrators should use individual end-user accounts with the corresponding privileges. Be aware that logins will fail if the connection to the LDAP server(s) cannot be established. In this case, use the default Cisco Unified Communications Manager administrator account (application user account) that was created during Cisco Unified Communications Manager installation.

When you enable LDAP authentication with Microsoft Active Directory, it is recommended that you configure Cisco Unified Communications Manager to query a Microsoft Active Directory Global Catalog server for faster response times. To enable queries against the Global Catalog, simply configure the LDAP Server Information in the LDAP Authentication page to point to the IP address or host name of a Domain Controller that has the Global Catalog role enabled and configure the LDAP port as 3268.

Note	The global catalog is created automatically on the initial domain controller of a Microsoft Active Directory forest. It stores a full replica of all objects in the directory for its host domain and a partial replica of all objects contained in the directory of every other domain in the forest. The replica is partial because it stores some, but not all, of the property values for every object in the forest. The global catalog performs two key directory roles. First, it enables network logon by providing universal group membership information to a domain controller when a login process is initiated. Secondly, it enables finding directory information regardless of which domain in the forest actually contains the data. For more information regarding the global catalog, refer to www.microsoft.com .
-------------	---

LDAP Authentication When Using Microsoft Active Directory with Multiple Domains or Trees

The figure illustrates the LDAP authentication process when using Microsoft Active Directory.



The use of global catalog for authentication becomes even more efficient if the users belong to multiple Microsoft Active Directory domains, because it allows Cisco Unified Communications Manager to authenticate users immediately without having to follow referrals. For these cases, point Cisco Unified Communications Manager to a global catalog server and set the LDAP User Search Base to the top of the root domain.

In the case of a Microsoft Active Directory forest that encompasses multiple trees, some additional considerations apply. Because a single LDAP search base cannot cover multiple namespaces, Cisco Unified Communications Manager must use a different mechanism to authenticate users across these discontinuous namespaces.

As mentioned in the LDAP synchronization topic, in order to support synchronization with a Microsoft Active Directory forest that has multiple trees, the UserPrincipalName (UPN) attribute must be used as the user ID within Cisco Unified Communications Manager. When the user ID is the UPN, the LDAP authentication configuration page within Cisco Unified Communications Manager Administration does not allow you to enter the LDAP Search Base field, but instead it displays the note “LDAP user search base is formed using userid information.”

In fact, the user search base is derived from the UPN suffix for each user, as shown in the figure. In this example, a Microsoft Active Directory forest consists of two trees, `avvid.info` and `vse.lab`. Because the same username may appear in both trees, Cisco Unified Communications Manager has been configured to use the UPN to uniquely identify users in its database during the synchronization and authentication processes.

A user named John Doe exists in both the `avvid.info` tree and the `vse.lab` tree. The following steps illustrate the authentication process for the first user, whose UPN is `jdoe@avvid.info`:

1. The user authenticates to Cisco Unified Communications Manager via HTTPS with its user name (which corresponds to the UPN) and password.
2. Cisco Unified Communications Manager performs an LDAP query against a Microsoft Active Directory global catalog server, using the username specified in the UPN (anything before the @ sign) and deriving the LDAP search base from the UPN suffix (anything after the @ sign). In this case, the username is `jdoe`, and the LDAP search base is "`dc=avvid, dc=info`".
3. Microsoft Active Directory identifies the correct distinguished name corresponding to the user name in the tree specified by the LDAP query. In this case, "`cn=jdoe, ou=Users, dc=avvid, dc=info`".
4. Microsoft Active Directory responds via LDAP to Cisco Unified Communications Manager with the full distinguished name for this user.
5. Cisco Unified Communications Manager attempts an LDAP bind with the distinguished name provided and the password initially entered by the user, and the authentication process then continues as in the standard case.

Support for LDAP authentication with Microsoft Active Directory forests containing multiple trees relies exclusively on the approach described in this scenario. Therefore, support is limited to deployments where the UPN suffix of a user corresponds to the root domain of the tree where the user resides. If the UPN suffix is disjointed from the actual namespace of the tree, it is not possible to authenticate Cisco Unified Communications Manager users against the entire Microsoft Active Directory forest. (It is, however, still possible to use a different attribute as user ID and limit the integration to a single tree within the forest.)

LDAP Authentication Configuration Procedure

This section lists the required steps for enabling LDAP synchronization.

LDAP Authentication Configuration Procedure

1. Add Cisco Unified CM directory user and assign administrator access rights in LDAP directory (depends on used LDAP directory server).
2. Configure LDAP authentication.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-69

The LDAP synchronization configuration procedure includes the following steps:

- Step 1** Add Cisco Unified Communications Manager directory user and assign administrator access rights in LDAP directory (this configuration depends on LDAP directory server that is used).
- Step 2** Configure LDAP authentication.

Step 2: LDAP Authentication Configuration

The only configuration task in Cisco Unified Communications Manager is to configure LDAP authentication.

Step 2: LDAP Authentication Configuration

Cisco Unified CM Administration

System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Actions

LDAP Authentication

Status: Ready

LDAP Authentication for End Users:

- Use LDAP Authentication for End Users
- LDAP Manager Distinguished Name: Directory Manager
- LDAP Password: (redacted)
- Confirm Password: (redacted)
- LDAP User Search Base: ou=site-1, dc=use, dc=lab

LDAP Server Information:

- Host Name or IP Address for Server: 192.168.10.10
- LDAP Port: 389
- Use SSL:
- Add Another Redundant LDAP Server

Save

Configure Unified CM directory user (as configured in LDAP).

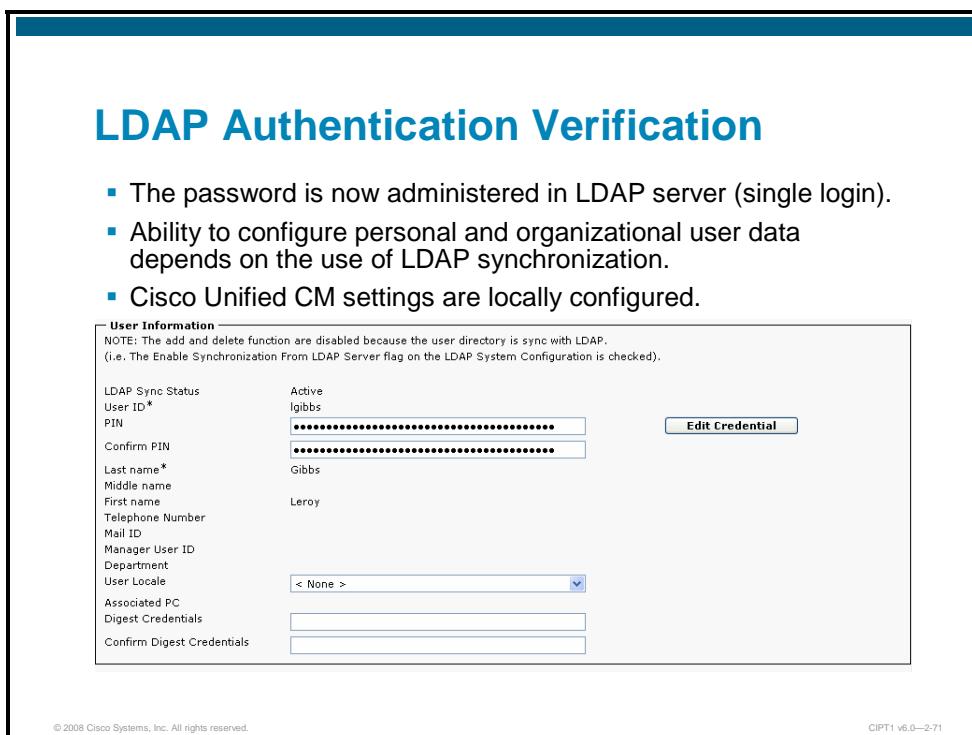
Configure LDAP server(s.).

Configure search base for LDAP authentication.

Go to **System > LDAP > LDAP Authentication** to configure the Cisco Unified Communications Manager directory user as configured in the LDAP directory (as stated in step 1), the user search base, and the LDAP server(s). Activate the Enable Authentication for End Users check box.

LDAP Authentication Verification

To verify successful LDAP authentication configuration, go to **User Management > End User** and click one of the end-user accounts.



LDAP Authentication Verification

- The password is now administered in LDAP server (single login).
- Ability to configure personal and organizational user data depends on the use of LDAP synchronization.
- Cisco Unified CM settings are locally configured.

User Information	
LDAP Sync Status	Active
User ID*	lgibbs
PIN	*****
Confirm PIN	*****
Last name*	Gibbs
Middle name	
First name	Leroy
Telephone Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC	
Digest Credentials	
Confirm Digest Credentials	

You cannot change the password of end users in Cisco Unified Communications Manager anymore. The ability to change the username and personal or organizational settings depends on the use of LDAP synchronization and is independent of LDAP authentication. Regardless of the use of LDAP integration, you can change Cisco Unified Communications Manager settings such as PIN, digest credentials, and associated PC.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco Unified CM has application users and end users.
- Application and end users can be configured one-by-one using Cisco Unified CM Administration.
- The Cisco Unified Communications Manager BAT allows bulk configuration of users, phones, and other configuration entities.
- Cisco Unified CM BAT can be used for mass user configuration.
- LDAP directories are centralized storage of user information.
- Cisco Unified CM can integrate with LDAP for user provisioning.
- Cisco Unified CM can integrate with LDAP for user authentication.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-72

References

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager Bulk Administration Guide 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/bat/6_0_1/bat-wrapper.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
[http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfg/bccm.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf)
- Cisco Unified Communications Manager System Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmsys/accm.pdf

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- Cisco Unified Communications Manager provides four GUIs and a CLI for administration purposes.
- Initial configuration of Cisco Unified Communications Manager includes service activation, general configuration of service and enterprise parameters, and network configuration such as removing DNS reliance.
- Cisco Unified Communications Manager application users are always configured locally. For end users, user provisioning and user authentication can be performed by LDAP integration.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—2-1

This module describes Cisco Unified Communications Manager Administration GUIs and Cisco Unified Communications Manager command-line interface (CLI). It explains when to use which one and how to access them. In addition, the module describes Cisco Unified Communications Manager service activation and initial configuration parameters. Finally, the module describes the user-management options available in Cisco Unified Communications Manager.

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager (CallManager) – Maintain and Operate Guides
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- Cisco Unified Serviceability Administration Guide for Cisco Unified Communications Manager, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/6_0_1/admin/cmservbk.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
[http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfg/bccm.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf)
- Cisco Unified Communications Solution Reference Network Design (SRND) Document Based on Cisco Unified Communications Manager Release 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html

- Cisco Unified Communications Manager Bulk Administration Guide 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/bat/6_0_1/bat-wrapper.html
- Cisco Unified Communications Manager System Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmsys/accm.pdf

Module Self-Check

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

- Q1) How many administration and user interfaces are available in Cisco Unified Communications Manager Release 6.0? (Source: Understanding Cisco Unified Communications Manager Administration Options)
- A) 4 GUIs and 1 CLI
 - B) 5 GUIs and 2 CLIs
 - C) 4 GUIs and 2 CLIs
 - D) 5 GUIs and 1 CLI
- Q2) Which function is not provided by the Cisco Unified Communications Manager user web pages? (Source: Understanding Cisco Unified Communications Manager Administration Options)
- A) forward all calls
 - B) configure speed dials
 - C) add users
 - D) subscribe to IP phone services
 - E) configure personal address book and fast dials
- Q3) The Cisco Unified Communications Manager Administration GUI can be accessed using which URL? (Source: Understanding Cisco Unified Communications Manager Administration Options)
-
- Q4) Which two functions are not provided by the Cisco Unified Serviceability web page? (Choose two.) (Source: Understanding Cisco Unified Communications Manager Administration Options)
- A) configure alarms and logs
 - B) configure traces
 - C) configure CDR disk storage and external billing servers
 - D) upload license files
 - E) download application plug-ins
 - F) configure serviceability reports
- Q5) Which account is used to log in to the Disaster Recovery System web page? (Source: Understanding Cisco Unified Communications Manager Administration Options)
- A) Platform administrator account
 - B) CCMAAdministrator
 - C) DRS Administrator account
 - D) CARAdmin
 - E) OSAdmin

- Q6) Which function is not provided by the Cisco Unified Operating System Administration web page? (Source: Understanding Cisco Unified Communications Manager Administration Options)
- A) check software and hardware status
 - B) view or update IP addresses
 - C) manage NTP servers
 - D) ping other network devices
 - E) restart the system
- Q7) Which protocol can be used to access the Cisco Unified Communications Manager CLI? (Source: Understanding Cisco Unified Communications Manager Administration Options)
- A) HTML
 - B) SSH
 - C) RPC
 - D) Telnet
- Q8) Which two options are not initial configuration steps? (Choose two.) (Source: Managing Services and Initial Configuration of Cisco Unified Communications Manager)
- A) configure network settings
 - B) configure partitions and Calling Search Space
 - C) configure enterprise parameters
 - D) configure default device profiles
 - E) configure service parameters
- Q9) Which is not a network configuration option of Cisco Unified Communications Manager? (Source: Managing Services and Initial Configuration of Cisco Unified Communications Manager)
- A) HSRP
 - B) NTP
 - C) DNS
 - D) DHCP
- Q10) Cisco Unified Communications Manager Release 6.0 _____ provide IP phones with IP addresses by DHCP. (Source: Managing Services and Initial Configuration of Cisco Unified Communications Manager)
- A) has to
 - B) cannot
 - C) can
 - D) subscribers
- Q11) What needs to be done in order to remove DNS reliance? (Source: Managing Services and Initial Configuration of Cisco Unified Communications Manager)
- A) change the Cisco Unified Communications Manager names to IP addresses
 - B) change option 150 in the DHCP settings
 - C) set the DNS server IP address to 0.0.0.0
 - D) change the Cisco Unified Communications Manager server names to IP addresses

- Q12) _____ cannot be activated or deactivated by the administrator. (Source: Managing Services and Initial Configuration of Cisco Unified Communications Manager)
- A) enterprise services
 - B) cluster-wide services
 - C) network services
 - D) feature services
- Q13) Which two of the following characteristics do not apply to enterprise parameters? (Choose two.) (Source: Managing Services and Initial Configuration of Cisco Unified Communications Manager)
- A) They are used to define cluster-wide system settings.
 - B) A reload is required after changing any of them.
 - C) They apply to all devices and are configured per services.
 - D) They allow the configuration of IP phone URLs.
 - E) They can be configured per Cisco Unified Communications Manager server.
- Q14) _____ are used to configure cluster-wide or per-server service-specific parameters. (Source: Managing Services and Initial Configuration of Cisco Unified Communications Manager)
- A) Service parameters
 - B) Global parameters
 - C) Feature parameters
 - D) Application parameters
- Q15) Which two of the following options are features that do not interact with Cisco Unified Communications Manager user accounts (Choose two.) (Source: Managing User Accounts in Cisco Unified Communications Manager)
- A) Cisco Unified User web pages
 - B) Cisco Unified Device Mobility
 - C) Cisco Unified Attendant Console
 - D) Cisco Unified Extension Mobility
 - E) Cisco Unified Phone Autoregistration
- Q16) Which two configuration elements are used to assign privileges to users? (Choose two.) (Source: Managing User Accounts in Cisco Unified Communications Manager)
- A) functional groups
 - B) roles
 - C) user groups
 - D) common user settings
 - E) privilege groups
- Q17) Which two functions are not performed by the Cisco Unified Communications Manager Bulk Administration Tool? (Choose two.) (Source: Managing User Accounts in Cisco Unified Communications Manager)
- A) add or delete a large number of similar records
 - B) export data records
 - C) update a large number of similar records
 - D) backup of the complete Cisco Unified Communications Manager configuration
 - E) import data records
 - F) convert SIP phones to SCCP

- Q18) Which option is not a step of adding users with the Cisco Unified Communications Manager Bulk Administration Tool? (Source: Managing User Accounts in Cisco Unified Communications Manager)
- A) verify the status of the Cisco Unified Communications Manager BAT job
 - B) upload a user template
 - C) upload a CSV data input file
 - D) start Cisco Unified Communications Manager BAT job to add users
- Q19) Which two of the following choices are the supported LDAP integration options? (Choose two.) (Source: Managing User Accounts in Cisco Unified Communications Manager)
- A) LDAP synchronization
 - B) LDAP replication
 - C) LDAP authentication
 - D) LDAP authorization
 - E) LDAP distribution
- Q20) With LDAP _____, end users are provisioned in the LDAP directory and cannot be added, modified, or deleted in Cisco Unified Communications Manager. (Source: Managing User Accounts in Cisco Unified Communications Manager)
- A) synchronization
 - B) replication
 - C) authentication
 - D) authorization
 - E) distribution
- Q21) _____ users cannot be authenticated using LDAP. (Source: Managing User Accounts in Cisco Unified Communications Manager)
- A) End
 - B) Internal
 - C) Application
 - D) Phone
 - E) Web

Module Self-Check Answer Key

- Q1) D
- Q2) C
- Q3) <https://server-address/ccmadmin>
- Q4) D, E
- Q5) A
- Q6) E
- Q7) B
- Q8) B, D
- Q9) A
- Q10) C
- Q11) D
- Q12) C
- Q13) A,D
- Q14) A
- Q15) B, E
- Q16) B, C
- Q17) D, F
- Q18) B
- Q19) A, C
- Q20) A
- Q21) C

Module 3

Single-Site On-Net Calling

Overview

Enabling a Cisco Unified Communications Manager cluster for on-net calls includes several components of the Cisco Unified Communications architecture. It involves providing the IP network infrastructure, the selection of endpoints such as Cisco IP phones, and their integration into the network.

This module describes the endpoints that are supported by Cisco Unified Communications Manager, their characteristics, protocol, and feature support. The module also describes unique features of Cisco IP phones and how Cisco Catalyst switches can provide power to endpoints and support VLAN separation for voice and data traffic. Finally, the module explains how to implement Cisco IP and third-party phones using the different protocols, and how Cisco IP phones can be hardened.

Module Objectives

Upon completing this module, you will be able to configure Cisco Unified Communications Manager to support on-cluster calling. This ability includes being able to meet these objectives:

- Describe the general features and unique characteristics of the H.323, SCCP, and SIP endpoints that are supported by Cisco Unified Communications Manager
- Configure Cisco IOS Catalyst switches to support Cisco IP phones, third-party IP phones, and software-based phones
- Implement SCCP and SIP (Cisco and third-party) phones in Cisco Unified Communications Manager and harden the Cisco IP phones

Lesson 1

Understanding Endpoints in Cisco Unified Communications Manager

Overview

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

This lesson describes the various models of Cisco IP phones and how they work within a Cisco IP telephony solution. The lesson introduces the basic features of Cisco IP phones; the IP phone power-up and registration process; and the audio coders-decoders (codecs) that are supported by Cisco IP phones. The lesson also describes third-party session initiation protocol (SIP) and H.323 endpoints.

Objectives

Upon completing this lesson, you will be able to describe the general features and unique characteristics of the H.323, Skinny Client Control Protocol (SCCP), and SIP endpoints that interwork with Cisco Unified Communications Manager. This ability includes being able to meet these objectives:

- List the endpoints supported by Cisco Unified Communications Manager
- Describe the features supported by different Cisco IP phone models
- Describe the boot sequence of Cisco IP phones
- Describe how H.323 endpoints are supported by Cisco Unified Communications Manager
- Describe how SIP third-party IP phones are supported by Cisco Unified Communications Manager

Cisco Unified Communications Manager Endpoints

This topic describes endpoints that can be used with Cisco Unified Communications Manager.



A variety of endpoints, Cisco as well as third-party products, can be used with Cisco Unified Communications Manager. Endpoints include IP phones, analog station gateways, which allow analog phones to interact with Cisco Unified Communications Manager, and video endpoints.

Cisco Unified Communications Manager supports three protocols to be used for endpoints: SCCP, SIP, and H.323.

Cisco Unified Communications Manager Endpoint Support

The table lists Cisco IP phone models and examples of third-party IP phones.

Cisco Unified Communications Manager Endpoint Support

Cisco Unified IP Phones (SCCP and SIP)	Type A: 7940, 7960, 7905, 7912 Type B: 7906, 7911, 79[46][125], 79[015]
Cisco softphone	Cisco IP Communicator
Other Cisco endpoints (SCCP only)	7902, 7910, and 7931 (IP phones), 7920 and 7921 (WiFi phones), 7935 and 7936 (conference stations), 7985 (desktop video phone)
Third-party endpoints (various)	SCCP: Nokia dual-mode cell phone SCCP client, Tandberg video endpoints, IP blue VTGO, etc. SIP: various hard-and software phones H.323: various hard- and software phones

Cisco IP phone models displayed in *italic* are end-of-sale.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-5

Cisco IP phones that support SCCP and SIP are split into two categories:

- **Type A phones:** These are the following Cisco Unified IP Phones: 7905, 7912, 7940, and 7960.
- **Type B phones:** These are the following Cisco Unified IP Phones: 7906, 7911, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, and 7975.

Cisco also offers a software-based phone to be installed on a Microsoft Windows PC—the Cisco IP Communicator, which is similar to the Cisco Unified IP Phone 7970 except that it runs on a PC. The Cisco IP Communicator supports SCCP, and SIP support has been added in Cisco IP Communicator version 2.1.

The Cisco Unified IP Phone 7902, 7910, and 7931 are Cisco IP phones that support SCCP only.

Other Cisco endpoints are the Cisco Unified IP Phone 7985 (a desktop video phone), the Cisco Unified IP Phone 7920 and 7921 models (Wi-Fi phones), and the Cisco Unified IP Phone 7935 and 7936 models (conference stations). All these endpoints support SCCP only.

Note The Cisco Unified IP Phones 7902, 7905, 7910, 7912, and 7935 are end-of-sale.

Third-party products are available for all supported protocols. Nokia supports the Cisco Unified Mobile Communicator (an SCCP software client to be installed on Nokia dual mode mobile phones). Tandberg produces SCCP-based video endpoints, IP blue offers an SCCP-based software IP phone that emulates standard Cisco 79xx phone lines towards Cisco Unified Communications Manager. In addition, many third-party endpoints for SIP and H.323 can be found on the market.

Cisco Unified Communications Manager Endpoint Feature Support

This topic describes the how the number of supported telephony features depends on the protocols used and the endpoint types.

Unified CM Endpoint Telephony Feature Support Dependencies

Unified CM supports endpoints using SCCP, SIP, and H.323:

- Cisco proprietary SCCP:
 - Only used by Cisco IP phones (few third-party endpoints exist)
 - Rich set of telephony features, most features supported on all Cisco IP phone models
- Standard SIP or H.323:
 - Supported on all standard compliant third-party phones and few Cisco IP phones
 - Provide only basic telephony features
- Standard SIP with Unified CM extensions:
 - Only used by Cisco IP phones
 - Rich set of telephony features, but support depends heavily on Cisco IP phone model

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-7

From a feature support perspective, the protocols can be categorized into three groups:

- **SCCP:** SCCP is a Cisco proprietary protocol and typically only used by Cisco IP endpoints, except for a few third-party products, such as Tandberg video phones and the VTGO softphone application from IP blue. SCCP offers a rich set of telephony features, most of which are supported on *all* Cisco IP phone models.
- **Standard SIP or H.323:** Cisco Unified Communications Manager supports standards-based SIP and H.323 endpoints. The number of standardized telephony features, however, is limited compared to feature-rich SCCP.
- **Cisco Unified Communications Manager SIP support for Cisco IP phones:** When Cisco Unified Communications Manager interacts with Cisco IP phones using the SIP protocol, many features are supported in addition to the standard feature set of SIP. Cisco Unified Communications Manager supports approximately the same features for Cisco IP phones that are supported with SCCP, but the number of features supported depends on the particular model of Cisco IP phone.

Cisco Unified Communications Manager Telephony Feature Support by Protocol and Type of Endpoint

The table illustrates the feature richness of different endpoints per protocol.

Unified CM Telephony Feature Support by Protocol and Type of Endpoint

	Standard SIP	Unified CM SIP	(Unified CM) SCCP	H.323 (Standard)
Works also with products other than Unified CM	Yes	No	No	Yes
Number of telephony features	Small	Type A: Medium Type B: High	High	Small
Supported phones	Third-party phones 7940, 7960	Type A: 7940, 7960, 7905 , 7912 Type B: 7906, 7911, 7931, 79[46][125], 797[015]	All Cisco Unified endpoints Third-party SCCP endpoints	Third-party phones 7905 , 7912

Cisco IP phone models displayed in *italic* are end-of-sale.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-8

As shown in the table, standard SIP and H.323 endpoints can be used with other IP telephony devices or systems, including Cisco Unified Communications Manager, but are limited regarding the number of supported telephony features.

The Cisco Unified IP Phones 7940 and 7960 can be loaded with a special firmware that provides standard SIP support. This is not typically done when these phones interact with Cisco Unified Communications Manager because these phones support more features when using a Cisco Unified Communications Manager SIP or SCCP implementation. This option is generally used by customers who connect to other IP communication systems, but who want to take advantage of the excellent voice quality of these Cisco IP phones. Some Internet telephony service providers (ITSPs) offering standard SIP telephony services provide their customers with preconfigured Cisco Unified IP Phones 7940 or 7960 to be used to connect to their SIP proxy servers.

The Cisco Unified IP Phones 7905 and 7912 can be loaded with an H.323 firmware. As with the Cisco Unified IP Phones 7940 and 7960 that use a standard SIP firmware, this is typically used when connecting to a non-Cisco Unified Communications Manager H.323-based environment.

Note When Cisco Unified IP Phones 7905, 7912, 7940, and 7960 are loaded with special firmware, as described above, they will not support general Cisco IP phone features such as Cisco Discovery Protocol, voice VLANs, TFTP configuration file support, and so on.

When you use Cisco IP phones with SIP, the number of features depends on the phone models. Type A phones (Cisco Unified IP Phones 7905, 7912, 7940, and 7960) support fewer features and have a different look and feel when used with SIP.

In summary, endpoints using standard SIP or H.323 support fewer telephony features, and type A Cisco IP phones have some limitations when using SIP.

Cisco IP Phone Model Differences

This section describes characteristics of Cisco IP phones.

Cisco IP Phone Model Differences

The wide range of Cisco IP phones offers a wide choice of hardware capabilities:

- Screen: resolution, size, and color; touch-screen?
- Codec support: G.729, G.711, iLBC, wideband?
- LAN: speed, PC port?
- Buttons, navigation clusters?
- Speakerphone and headset support?
- Number of lines?
- Special features: video, conference station, Wi-Fi?

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-9

Cisco IP phones cover a wide range of types, from simple, display-less entry-level phones to upper-level phones with high-resolution, color, touch-screen displays. Differences in hardware-related capabilities include the following:

- **Screen:** Different models have screens with different resolution, size, color, and touch-screen capabilities.
- **Codec support:** All Cisco IP phones support G.711 and G.729 codecs. High-end models also support iLBC and wideband codecs for superior voice quality.
- **LAN:** Most IP phones have a PC port so that a PC can be connected to the network without requiring its own wall socket, in-house cabling, and physical switch port. Different phone models support different speeds on the PC port and on the IP phone switch port (the port connected to a LAN switch).
- **Buttons, navigation clusters, and so on:** The number of IP phone buttons, softkeys, and other buttons also differs per phone model. There are also differences in the type of navigation clusters (2-way or 4-way).
- **Speakerphone and headset support:** Some IP phones offer speakerphone and headset support.
- **Number of lines:** The number of lines also differs per phone model.
- **Other features:** Some IP phones provide other special features such as video, Wi-Fi support, or dedicated support for use in conference rooms (enhanced speakerphone capabilities, including the option to connect multiple microphones).

Entry-Level Cisco IP Phones

The figure shows entry-level Cisco IP phones and lists some of their characteristics.

Entry-Level Cisco IP Phones

Cisco Unified
IP Phone 7906



Cisco Unified
IP Phone 7911



- Basic-featured Cisco IP phones for low-to-medium telephone use
- Single line or directory number
- Message waiting indicator

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-10

The Cisco Unified IP Phones 7906 and 7911 fill the communication needs of cubicle, retail, classroom, or manufacturing workers or anyone who conducts low-to-moderate telephone traffic. Four dynamic softkeys guide users through core business features and functions, while a pixel-based display combines intuitive features, calling information, and Extensible Markup Language (XML) services into a rich user experience.

Both phones offer numerous important security features, plus the choice of IEEE 802.3af Power over Ethernet (PoE), Cisco inline power, or local power through an optional power adaptor.

Midrange Cisco IP Phones

The figure shows midrange Cisco IP phones and lists some of their characteristics.

Midrange Cisco IP Phones

Cisco Unified IP Phone 794[012] Cisco Unified IP Phone 796[012]

7940 7941 7960 7961

- Full-featured Cisco IP phones for medium-to-high telephone use
- Multiline
- Message waiting indicator
- Large pixel-based displays
- Integrated switches
- Built-in headsets and high-quality speakerphones

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-11

Midrange Cisco Unified IP Phones 7940, 7941, 7942, 7960, 7961, and 7962 address the communications needs of a transaction-type worker. They provide two or four programmable line and feature keys, plus a high-quality speakerphone. These phone models have four dynamic softkeys that guide users through call features and functions. A built-in headset port and an integrated Ethernet switch are standard with these phones. The phones also include audio controls for the full-duplex, high-quality, hands-free speakerphone, handset, and headset.

The Cisco Unified IP Phones 7941 and 7961 have lighted line keys, and the Cisco Unified IP Phones 7942 and 7962 add support for the high-fidelity wideband codec.

Note For a detailed list of features per phone model, refer to the data sheets of the Cisco Unified IP Phone 7900 Series products.

Upper-End Cisco IP Phones

The figure shows the upper-end Cisco IP phones and lists some of their characteristics.

Upper-End Cisco IP Phones

<p>Cisco Unified IP Phone 7945</p> 	<p>Cisco Unified IP Phone 7965</p> 	<p>Cisco Unified IP Phone 797[015]</p>  7970	 7975
--	--	---	---

- Addresses needs of executives
- Large, color, pixel-based displays
- Touch-sensitive display on 797[015] models
- Two to eight telephone lines, or combinations of lines and direct access to telephony features
- Four or five interactive softkeys
- Built-in headsets and high-quality, hands-free speakerphones

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-12

Upper-end Cisco Unified IP Phones 7945, 7965, 7970, 7971, and 7975 demonstrate the latest advances in VoIP telephony, including wideband audio support, backlit color displays, and an integrated Gigabit Ethernet port. They address the needs of executives and transaction-type workers with significant phone traffic, and the needs of those working with bandwidth-intensive applications on collocated PCs.

These IP phones include a large, backlit, easy-to-read color display for easy access to communication information, timesaving applications, and features such as date and time, calling party name, calling party number, digits dialed, and presence information. They also accommodate XML applications that take advantage of the display. The phones provide direct access to two to eight telephone lines (or combination of lines, speed dials, and direct access to telephony features), four or five interactive softkeys that guide you through call features and functions, and an intuitive four-way (plus Select key) navigation cluster. A hands-free speakerphone and handset designed for high-fidelity wideband audio are standard, as is a built-in headset connection.

Note	For a detailed list of features per phone model, refer to the data sheets of the Cisco Unified IP Phone 7900 Series products.
-------------	---

Other Cisco IP Phones

The figure shows other Cisco IP phones and lists some of their characteristics.

Other Cisco IP Phones

<p>Cisco Unified IP Phone 7985</p> 	<p>Cisco Unified IP Conference Station 7936</p> 	<p>Cisco Unified Wireless IP Phone 792[01]</p>  7921	<p>Cisco Unified IP Phone 7931</p> 
--	---	--	--

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-13

Other Cisco Unified IP phones and endpoints include the following models:

- **Cisco Unified IP Phone 7985:** This is a personal desktop video phone for the Cisco Unified Communications solution. Offering executives and managers a productivity-enhancing tool that makes instant, face-to-face communication possible from their offices, the Cisco Unified IP Phone 7985 has a video call-camera, LCD screen, speaker, keypad, and a handset-incorporated into one easy-to-use unit.
- **Cisco Unified IP Conference Station 7936:** This conference station combines state-of-the-art speakerphone conferencing technologies with award-winning Cisco voice communication technologies. The net result is a conference room phone that offers superior voice and microphone quality, with simplified wiring and administrative cost benefits. A full-featured, IP-based, hands-free conference station, the new Cisco Unified IP Conference Station 7936 is designed for use on desktops, conference rooms, and in executive suites.
- **Cisco Unified Wireless IP Phone 7921:** This phone provides a powerful, converged solution with an intelligent wireless infrastructure. This wireless phone supports a host of calling features and voice-quality enhancements. Because the Cisco Unified Wireless IP Phone 7921 is designed to grow with system capabilities, features will keep pace with new system enhancements.
- **Cisco Unified IP Phone 7931:** This phone meets the communication needs of retail, commercial, manufacturing workers, and anyone with moderate telephone traffic but also specific call requirements. Dedicated hold, redial, and transfer keys facilitate call handling in a retail environment. Illuminated mute and speakerphone keys give a clear indication of speaker status. A pixel-based display with a white backlight makes calling information easy to see and delivers a rich user experience.

Note	For a detailed list of features per phone model, refer to the data sheets of the Cisco Unified IP Phone 7900 Series products.
-------------	---

Special Functions Used By Cisco IP Phones

This section describes special functions that can be used with Cisco IP phones.

Special Functions Used By Cisco IP Phones

- Cisco Discovery Protocol : Cisco IP phones generate and listen to Cisco Discovery Protocol messages.
- DHCP: Cisco IP phones can get their IP addresses via DHCP.
- Identification by MAC address: Phones are identified by a unique device ID and not by their IP address.
- TFTP: Cisco IP phones are configured automatically by downloading device-specific configuration files from a TFTP server.
- PoE: Phones can be powered over the Ethernet network cable.
- PC Port: Phones allow a PC connected to the phone to share a single connection to the switch.

Note: PoE and PC port support is not available on all models.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-14

Cisco IP phones integrate seamlessly into a Cisco Unified Communications deployment. In conjunction with other components of the overall solution, Cisco IP phones can provide the following features:

- **Cisco Discovery Protocol:** Cisco IP phones generate Cisco Discovery Protocol messages like almost all other Cisco network products. Cisco IP phones can also listen to Cisco Discovery Protocol messages sent out by Cisco Catalyst switches. This way, a Cisco Catalyst switch can indirectly *configure* the LAN configuration of the phone, including the voice VLAN and class of service (CoS) settings for traffic received from an attached PC.

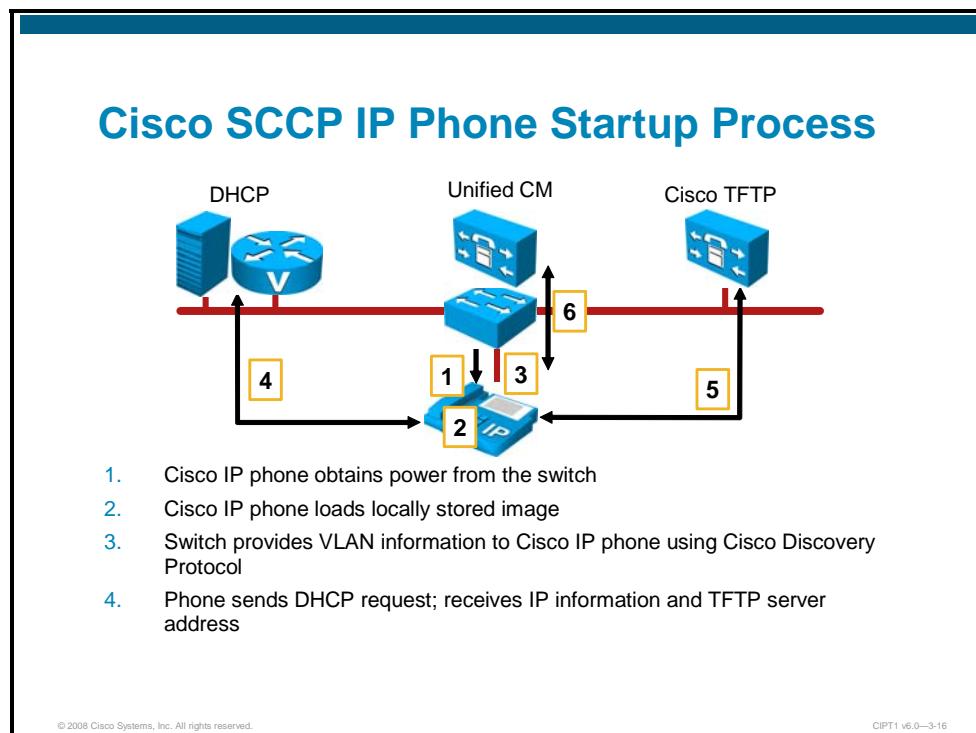
The Cisco Discovery Protocol messages sent by the IP phone are important when using Cisco Unified Video Advantage, a solution in which IP phones can be used for video calls by interacting with video hardware and software installed on the PC.

- **DHCP:** Cisco IP phones can have static IP configuration, entered at the IP phone, or use DHCP to obtain IP addresses assigned from a DHCP server.
- **MAC address-based device identification:** Cisco IP phones are identified by a device ID, which is based on the MAC address of the IP phone. This allows the device to be moved between subnets and simplifies DHCP configuration, because no specific IP address is required for an individual phone.
- **TFTP:** Cisco IP phone configuration does not take place individually at the phone, but centralized in Cisco Unified Communications Manager. Cisco Unified Communications Manager generates device-specific configuration files and makes them available for download at one or more TFTP servers. Cisco IP phones will learn the IP address of the TFTP server via DHCP, and then load the appropriate configuration file automatically as part of their boot sequence.

- **Power over Ethernet:** Cisco IP phones do not require wall power, but can obtain power over the Ethernet from any PoE-compliant LAN switch, such as a Cisco Catalyst switch. This eliminates the need for extra power adapters and cabling on the user desk.
- **PC port:** Cisco IP phones allow PCs to be connected to a PC port at the IP phone and then share the uplink towards the switch. By using the voice VLAN feature of Cisco Catalyst switches and Cisco IP phones, the IP phone and the PC can be separated into different VLANs on a single access port at the LAN switch.

Cisco IP Phones Boot Sequence

This topic describes the Cisco IP phone boot sequence and compares the use of SCCP and SIP.

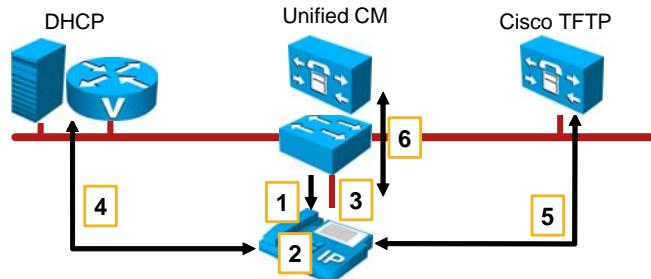


When connecting to the VoIP network, the Cisco IP phone goes through a standard startup process consisting of several steps. Depending on your specific network configuration, not all of these steps may occur on your Cisco IP phone:

- Step 1 Obtaining power from the switch:** The Cisco IP phone obtains power from the switch, if PoE is used. Alternatively, the IP phone can be powered by wall power or an in-line power injector.
- Step 2 Loading the stored phone image:** The Cisco IP phone has nonvolatile flash memory in which the phone firmware image is stored. At startup, the phone runs a bootstrap loader that loads the phone image from flash memory. Using this image, the phone initializes its software and hardware.
- Step 3 Configuring VLAN:** If the Cisco IP phone is connected to a Cisco Catalyst switch, the switch uses Cisco Discovery Protocol to inform the phone whether or not to use a dedicated voice VLAN for Ethernet frames carrying traffic to or from the IP phone (and leaving untagged frames for PC use). If the voice VLAN feature is not enabled at the switch and announced by Cisco Discovery Protocol, the Cisco IP phone does not send VLAN-tagged Ethernet frames.
- Step 4 Obtaining an IP address:** If the Cisco IP phone uses DHCP to obtain an IP address, the phone queries the DHCP server to obtain an IP address. DHCP also informs the IP phone about how to reach the TFTP server (DHCP Option 150). If DHCP is not used in your network, a static IP address and TFTP server address must be assigned to each IP phone locally. If the DHCP server does not respond, the IP phone will make use of the last used configuration stored in NVRAM.

Note	More information about the IP phone boot process can be found at the document "Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 5.0 (SIP) – Understanding the Phone Startup Process" at: http://www.cisco.com/en/US/products/hw/phones/ps379/products_administration_guide_chapter09186a00805f1f18.html#wp1043419
-------------	--

Cisco SCCP IP Phone Startup Process (Cont.)



5. Cisco IP phone gets configuration from TFTP server
6. Cisco IP phone registers with Cisco Unified Communications Manager server
 - Unified CM sends softkey template to SCCP phone using SCCP messages.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-17

Step 5 Requesting the configuration file and the profile file: The TFTP server has configuration files and profile files. A configuration file includes parameters for connecting to Cisco Unified Communications Manager and information about which image load a phone should be running. A profile file contains various parameters and values for phone and network settings.

The IP phone first requests its `SEP<mac>.cnf.xml` file from the TFTP server. If the TFTP server does not respond, the IP phone falls back to the last used configuration stored in NVRAM. If the TFTP server responds but the `SEP<mac>.cnf.xml` file is not found on the server, the phone requests the `XMLDefault.cnf.xml` file. From that file, the IP phone obtains its list of Cisco Unified Communications Managers and then attempts to auto-register to the primary server.

Then the phone will attempt to download a Certificate Trust List (CTL) file which is only used if cryptographic features are enabled in Cisco Unified Communications Manager.

Step 6 Registering on Cisco Unified Communications Manager: The configuration file includes a prioritized list of Cisco Unified Communications Manager servers. After obtaining the file from the TFTP server, the phone attempts to register with the highest priority Cisco Unified Communications Manager on the list. If the phone is not configured in Cisco Unified Communications Manager and auto-registration is enabled, Cisco Unified Communications Manager adds the device, and the phone can then register. Once the phone has registered, the Cisco Unified Communications Manager sends the softkey template configured for this IP phone to the IP phone using SCCP messages.

Boot Sequence Differences Between Cisco SCCP and SIP Phones

This subtopic identifies the boot sequence differences between Cisco SCCP IP phones and Cisco SIP IP phones.

Boot Sequence Differences Between Cisco SCCP and SIP Phones

The boot sequences for SIP and SCCP are similar. The **first 4 steps** remain the same. The main differences are :

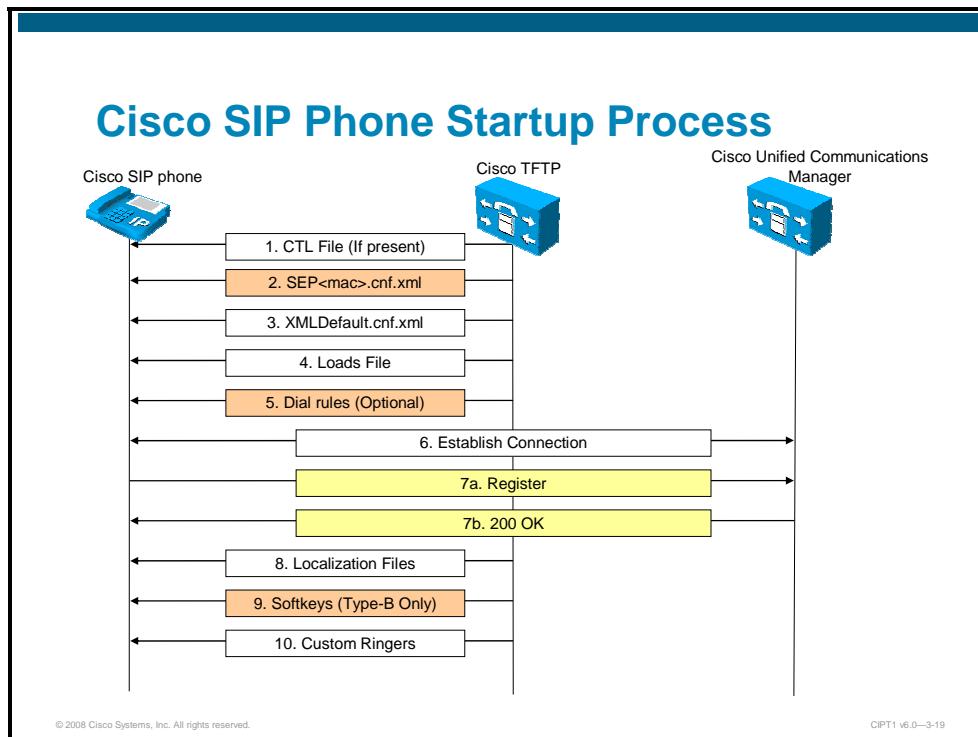
- **SEP<mac>.cnf.xml:** The SIP phones get all of their configuration from the configuration file. Therefore, the SEP<mac>.cnf.xml file is much larger for SIP than for SCCP.
- **Dialplan file (optional):** The SIP phones can download and use local dial plans.
- **Softkey file:** The SIP (Type-B only) phones download their softkey sets in this XML file.

The boot sequences for SIP phones are similar to those used for SCCP phones, except for these three main differences:

- **SEP<mac>.cnf.xml:** The SIP phones obtain all of their configuration from the config file. Therefore, the SEP<mac>.cnf.xml file is larger for SIP than for SCCP.
- **Dialplan file (optional):** The SIP phones can download and use local dial plans.
- **Softkey file:** The SIP phones download their softkey sets in this XML file.

Cisco SIP Phone Startup Process

This subtopic describes the startup process of a Cisco SIP IP phone.



The first four steps are the same as with SCCP phones and are not shown in the diagram. In the diagram and following steps it is assumed that the SIP phone has obtained an IP address and information about how to reach a TFTP server:

- Step 1** The SIP phone boots and tries to download a CTL file. The CTL file contains a set of certificates and is only used when Cisco Unified Communications Manager cluster security has been enabled.
- Step 2** The SIP phone requests its SEP<mac>.cnf file from the Cisco TFTP server. If a SIP phone is new, this file will not be found, because the phone is not currently configured in the Cisco Unified Communications Manager database.
- Step 3** The SIP phone downloads the default configuration file XMLDefault.cnf.xml from the TFTP server. This configuration file contains system-wide configuration parameters, including the location of the Cisco Unified Communications Manager of the SIP phone. For autoregistration to work for SIP, this file also contains a parameter called *auto_registration_name*. If this parameter is blank, then the SIP phone will not attempt to autoregister. If this parameter is not blank, the SIP phone will attempt to autoregister if it finishes the boot sequence and still does not have any legitimate directory number lines configured.
- Step 4** The SIP phone requests the .Loads file, if one was specified in the default configuration file, to see what image the phone should be running. If the .Loads file specifies an image that is different from the image contained in the SIP phone, the SIP phone attempts to obtain the new images from the Cisco TFTP server. If the image is downloaded and verified successfully, the SIP phone will reboot to load the new image.

- Step 5** The next step is to register with the highest priority Cisco Unified Communications Manager server. The default SIP configuration file indicates whether the SIP phone should connect using User Datagram Protocol (UDP) or TCP.
- Step 6** If the SIP phone does not have any directory number lines provisioned, but it does have the Cisco Unified Communications Manager IP address and port, the phone will check the *auto_registration_name* parameter. If the parameter contains a name, that name is used as the directory number line in the SIP Register message sent to the SIP proxy. Upon receiving this message, the Cisco Unified Communications Manager should do the following:
- Identify that the special autoregistration name has been used.
 - Create an entry in the database for the new phone based on the current autoregistration settings.
 - Generate the SEP<mac>.cnf.xml file for the new phone.
 - Accept the registration with the 200 OK response.
 - Reset the registered phone using the reset notify mechanism.
 - The phone will automatically reset and reboot.

This procedure describes the boot sequence of type A Cisco IP phones. The boot procedure for type B Cisco IP phones (Cisco Unified IP Phones 7940 and 7960) is slightly different from this procedure. Type B Cisco IP phones first download the SIPdefault.cnf file. This file contains the default configuration parameters shared by all SIP phones that use this TFTP server. Then, the Cisco SIP phone continues requesting the SIP<mac>.cnf file.

H.323 Endpoint Support in Cisco Unified Communications Manager

This topic describes Cisco Unified Communications Manager support for H.323 endpoints.

Unified CM H.323 Endpoint Support

- Cisco Unified Communications Manager supports any third-party H.323 phone that complies with the H.323 standards.
- H.323 phones can have multiple lines.
- H.323 endpoints can be both voice or video devices.
- H.323 endpoints are normally H.323 terminal devices, especially video endpoints.
- H.323 phones do not register with Cisco Unified Communications Manager and only have to be known by IP address.
- H.323 phones need to have their own dial plan and act as a peer to Cisco Unified Communications Manager.
- H.323 client consumes two license units.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-21

Cisco Unified Communications Manager supports any third-party H.323 phone that supports the H.323 protocol. H.323 phones support multiple lines and can be either video or audio endpoints (where video endpoints include audio capabilities). In H.323 terminology, the endpoints are H.323 terminals.

H.323 phones do not register with Cisco Unified Communications Manager but are configured by IP address, which becomes a problem if dynamic IP addresses are used. In such a case, an H.323 gatekeeper can be used for dynamic endpoint registration.

Configuration must be performed on both Cisco Unified Communications Manager and on the phone itself. This includes dial plan configuration, because the H.323 phone routes calls autonomously—however, all calls can be routed to Cisco Unified Communications Manager. Each H.323 phone consumes two device license units in Cisco Unified Communications Manager.

H.323 Endpoints

The figure shows some examples of H.323 endpoints.

H.323 Endpoints

- Cisco Unified IP Phone 7905 can be loaded with an H.323 firmware.
- From Cisco Unified Communications Manager perspective, they look like any other (third-party) H.323 endpoint.
- Other commonly used H.323 phones are Microsoft Windows NetMeeting or H.323 video devices from vendors like Tandberg or Sony.



Cisco 7905 IP Phone



Third-Party H.323 Endpoints

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-22

The Cisco Unified IP Phone 7905 can be loaded with an H.323 firmware. In this case, the phone is treated as any other H.323 endpoint and needs to be configured as a standard H.323 phone rather than as a Cisco Unified IP Phone 7905.

Other commonly used H.323 endpoints are Microsoft Windows NetMeeting and H.323 video devices from different vendors. H.323 endpoints are often deployed with an H.323 gatekeeper handling the registration of the devices.

Features Not Supported for H.323 Endpoints

This subtopic provides an overview of the features that are not supported for H.323 endpoints.

Features Not Supported for H.323 Endpoints

H.323 phones only support a few features compared to Cisco IP phones using SCCP or SIP. The features that are not supported include but are not limited to:

- MAC address registration
- Phone buttons templates
- Softkey templates
- Telephony features and applications such as:
 - IP phone services
 - Cisco Unified Communications Manager Assistant
 - Cisco Unified Video Advantage
 - Call Pickup
 - Barge
 - Presence, etc.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-23

H.323 endpoints support only few features compared to Cisco IP phones using SCCP or SIP. The features that are *not* supported include but are not limited to the following:

- MAC address-based registration: H.323 phones need to be configured by their IP address in Cisco Unified Communications Manager instead of a MAC address-based device ID.
- There is no support for phone button templates and softkey templates. The user interface depends on the H.323 product used.
- Telephony features and applications such as the following are not supported:
 - IP phone services
 - Cisco Unified Communications Manager Assistant
 - Cisco Unified Video Advantage
 - Call Pickup
 - Barge
 - Presence

H.323 Phone Configuration Requirements

This subtopic lists the configuration requirements when implementing H.323 phones.

H.323 Phone Configuration Requirements

H.323 endpoints typically require fewer configuration steps on the Cisco Unified Communications Manager compared to other types of endpoints. Configuration steps are as follows:

1. Configure the H.323 phone in Cisco Unified Communications Manager with IP address and DN(s).
2. Configure the H.323 phone with the IP address of Cisco Unified Communications Manager and specify the numbers that should be routed to Cisco Unified Communications Manager.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-24

The high-level configurations for H.323 phone implementations include the following points:

- The H.323 phone has to be added to Cisco Unified Communications Manager with its IP address and directory numbers specified.
- The H.323 phone has to be configured with the IP address of Cisco Unified Communications Manager.

Note	A dial plan must be configured on both devices. Typically, all calls from the H.323 phone are routed to Cisco Unified Communications Manager in order to take advantage of the centralized dial plan of Cisco Unified Communications Manager.
-------------	---

SIP Third-Party IP Phone Support in Cisco Unified Communications Manager

This topic describes support for third-party SIP phones in Cisco Unified Communications Manager.

Third-Party SIP Phone Support

- There are two categories of RFC 3261-compliant, third-party SIP phones supported by Cisco Unified Communications Manager:
 - Basic phones support one line and consume three license units.
 - Advanced support up to eight lines and video, and consume six license units.
- Third-party SIP phones register with Cisco Unified Communications Manager but are not recognized by a device ID such as a MAC address. SIP Digest Authentication is used instead to identify the endpoint that is trying to register.
- Configuration is performed on Cisco Unified Communications Manager and on the phone itself.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-26

Cisco Unified Communications Manager supports third-party RFC 3261-compliant SIP phones, but Cisco IP phones using the SIP protocol have many more telephony features than third-party phones using the SIP protocol.

Two different types of third-party SIP phones can be added to Cisco Unified Communications Manager:

- **Basic phones:** Support only a single line and consume three device license units
- **Advanced phones:** Support up to eight lines and video and consume six device license units

In terms of telephony features, there is no difference in basic versus advanced third-party SIP phones.

Third-party SIP phones register with Cisco Unified Communications Manager but do not use a MAC address-based device ID. Cisco Unified Communications Manager uses SIP digest authentication in order to identify a registering third-party SIP phone.

Both Cisco Unified Communications Manager and the third-party SIP phone must be configured.

SIP standards and drafts supported by Cisco Unified Communications Manager include the following:

- RFC 3262: PRACK
- RFC 3264: Session Description Protocol (SDP) offer/answer
- RFC 3311: UPDATE

- RFC 3515: REFER
 - RFC 3842: MWI Package
 - RFC 3891: Replaces Header
 - RFC 3892: Referred-by Mechanism
 - draft-levy-sip-diversion-08.txt: Diversion Header
 - draft-ietf-sip-privacy-04.txt: Remote-Party-ID Header
-

Note For more information about the support of these standards, refer to the document *Cisco SIP IP Administrator Guide*, version 8.0 – “Compliance with RFC 3261,” at http://www.cisco.com/en/US/products/sw/voicesw/ps2156/products_administration_guide_chapter09186a00807f47e3.html.

The following audio and video standards are supported for third-party SIP phones:

- Audio
 - Audio codecs: G.711 mu-law, Global System for Mobile Communications (GSM) Full Rate, G.723.1, G.711 a-law, G.722, G.728, G.729
 - RFC 2833 dual tone multifrequency (DTMF) (telephony event)
- Video
 - Video codecs: H.261, H.263, H.263 version 2, H.263 version 3, H.264

Third-Party SIP Phones

The figure shows some examples of SIP endpoints.

Third-Party SIP Phones

- Cisco Unified IP Phones 7940 and 7960 can be loaded with a standard SIP software, which is different from using SIP with Cisco Unified Communications Manager extensions on these phones.
- From Cisco Unified Communications Manager perspective, these phones look like any other (third-party) SIP endpoints.
- Many third-party SIP phones are available on the market.



Cisco 7960 IP Phone



Third-Party SIP Endpoints

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-27

Cisco Unified IP Phones 7940 and 7960 can be loaded with a standard SIP firmware. In this case, the phone is configured as a third-party SIP phone rather than as a Cisco Unified IP Phone 7940 or 7960 in Cisco Unified Communications Manager.

Cisco is working with key third-party vendors who are part of the Cisco Technology Development Partner Program and who are developing solutions that leverage the SIP capabilities of the new Cisco Unified Communications Manager and Cisco Unified Communications Manager Express. Vendors include Linksys (hardware phones), IPcelerate (unified client for educational environment usage), Research in Motion (RIM) (Blackberry 7270 wireless LAN handsets), IP blue (softphone), and Grandstream (Grandstream GXP2000 IP phone).

Cisco is also participating in an independent third-party testing and interoperability verification process being offered by tekVizion. This independent service was established to enable third-party vendors to test and verify the interoperability of their endpoints with Cisco Unified Communications Manager and Cisco Unified Communications Manager Express.

Features Not Supported for Third-Party SIP Endpoints

This subtopic describes the features that are not supported for SIP endpoints.

Features Not Supported for Third-Party SIP Endpoints

Third-party SIP phones only support a few features compared to Cisco IP phones using SCCP or SIP. The features that are not supported include but are not limited to the following:

- MAC address registration
- Phone button template
- Softkey templates
- Telephony features and applications such as:
 - IP phone services
 - Cisco Unified Communications Manager Assistant
 - Cisco Unified Video Advantage
 - Call Pickup
 - Barge
 - Presence

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-28

The limitations of third-party SIP endpoints are the same that apply to H.323 endpoints. These include but are not limited to the following:

- MAC address-based registration: SIP phones need to be configured by their IP address in Cisco Unified Communications Manager instead of a MAC address-based device ID.
- There is no support for phone button templates and softkey templates. The user interface depends on the SIP product used.
- Telephony features and applications such as the following are not supported:
 - IP phone services
 - Cisco Unified Communications Manager Assistant
 - Cisco Unified Video Advantage
 - Call Pickup
 - Barge
 - Presence

SIP Digest Authentication

This subtopic describes SIP digest authentication.

SIP Digest Authentication

- Digest authentication provides authentication of SIP messages by a username and a keyed MD5 hash.
- Digest authentication is based on a client/server model.
- Cisco Unified Communications Manager can challenge SIP endpoints and trunks, but can only respond to challenges on SIP trunks.
- Digest authentication is used to identify a third-party SIP device, because no MAC address is provided in the registration message.
- Cisco Unified Communications Manager can be configured to check the key (i.e. digest credentials) of a username used by a third-party SIP device, or to ignore the key and only search for the username.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-29

SIP digest authentication is specified in RFC 3261 and RFC 2617. It is based on a client/server model, in which the server challenges and the client responds, and provides authentication of SIP messages by a username and a keyed hash.

SIP digest authentication allows Cisco Unified Communications Manager to act as a server to challenge the identity of a SIP device when it sends a request to Cisco Unified Communications Manager. When digest authentication is enabled for a phone, Cisco Unified Communications Manager challenges all SIP phone requests except keepalive messages.

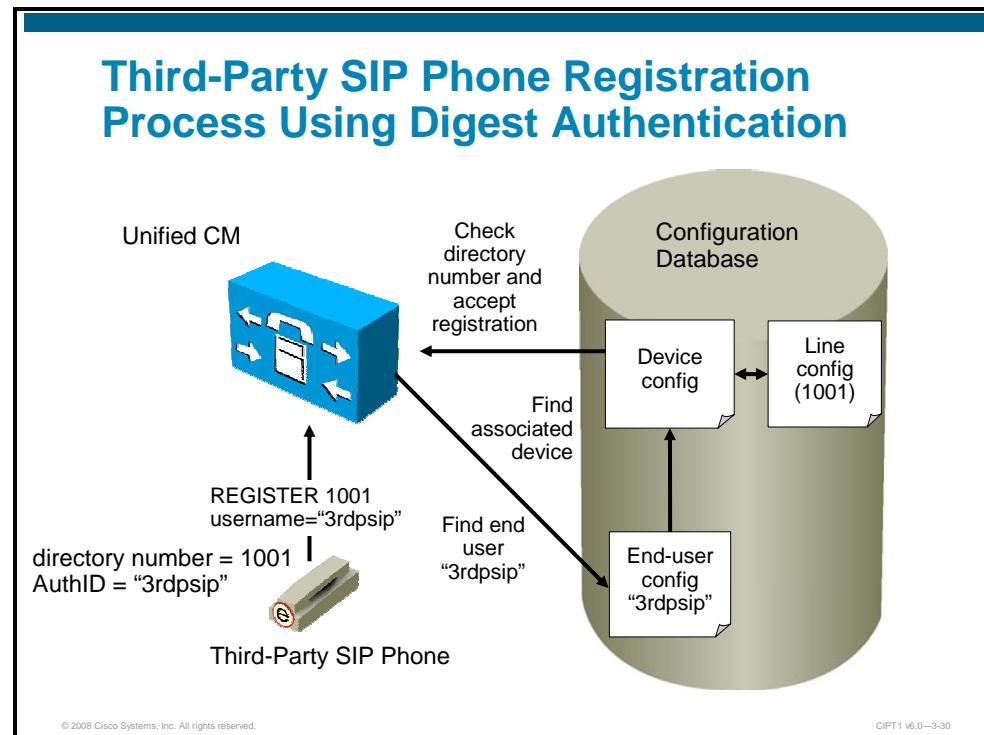
Cisco Unified Communications Manager does not support responding to challenges from SIP phones, but it can challenge SIP devices connecting through a SIP trunk and can respond to challenges received on its SIP trunk interface.

In Cisco Unified Communications Manager, SIP digest authentication is used to identify a third-party SIP phone because these phones do not register with a MAC address-based device ID.

Cisco Unified Communications Manager can ignore the keyed hash that is provided in a digest authentication response and only check if the provided username exists and is bound to a third-party SIP phone. This is the default behavior. Alternatively, Cisco Unified Communications Manager can be configured to check that the key that was used at the third-party SIP phone to generate the keyed hash matches the locally configured key (called “digest credentials”) at the end-user configuration in Cisco Unified Communications Manager.

Third-Party SIP Phone Registration Process Using Digest Authentication

This subtopic describes how digest authentication is used for third-party SIP phone registration in Cisco Unified Communications Manager.



Third-party SIP phones cannot be configured by using the Cisco Unified Communications Manager TFTP server. Instead, they need to be configured using the native phone configuration mechanism, which is usually a web page or a TFTP file. The device and line configuration in the Cisco Unified Communications Manager database must be synchronized with the native phone configuration manually (for example, extension 1002 on the phone and 1002 in Cisco Unified Communications Manager). Also, if the directory number of a line is changed, it must be changed in both Cisco Unified Communications Manager Administration and in the native phone configuration mechanism.

Third-party SIP phones include their directory number in the registration message. They do not send a MAC address; they must identify themselves by using digest authentication. For this purpose, the SIP REGISTER message includes a header with a username and the keyed hash, as shown in the example:

```
Authorization: Digest
username="3rdpsip",realm="ccmsipline",nonce="GBauADss2qoWr6k9Y
3hGGVDAqnLf0Lk5",uri="sip:172.18.197.224",algorithm=MD5,respone
se="126c0643a4923359ab59d4f53494552e"
```

When Cisco Unified Communications Manager receives the registration message, it searches for an end user that matches the provided username in the SIP message (in this case, 3rdpsip). If found, Cisco Unified Communications Manager will use the digest credentials configured for that user to verify the keyed hash ("response" in the above example). If the keyed hash is acceptable (that is, Cisco Unified Communications Manager and the third-party SIP phone share the same key used for the hash), the user passes authentication.

Note	Cisco Unified Communications Manager must be explicitly configured to verify the keyed hash. By default, Cisco Unified Communications Manager only searches for the end user name.
-------------	--

Cisco Unified Communications Manager then searches for a third-party SIP phone that is associated with the end user, and verifies that the configured directory number matches the number provided by the third-party SIP phone in its registration message. If the phone is found and the directory number is the same, the third-party SIP phone registered successfully with Cisco Unified Communications Manager.

Third-Party SIP Phone Configuration Requirements

The figure lists the steps to add and configure a third-party SIP phone to Cisco Unified Communications Manager.

Third-Party SIP Phone Configuration Requirements

The following steps have to be performed when configuring third-party SIP endpoints:

1. Configure an end user in Cisco Unified Communications Manager.
2. Configure the third-party SIP phone and its directory numbers in Cisco Unified Communications Manager.
3. Associate the third-party SIP phone with the end user.
4. Configure the third-party SIP phone with the IP address of Cisco Unified Communications Manager (proxy address), end-user ID, digest credentials (optional), and directory numbers.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-31

To implement a third-party SIP phone, perform the following high-level steps:

- Step 1** Configure an end user in Cisco Unified Communications Manager and, optionally, specify the digest credentials.
- Step 2** Add the third-party SIP phone in Cisco Unified Communications Manager and configure its directory numbers.

Note	When configuring the third-party SIP phone in Cisco Unified Communications Manager, you must specify a dummy MAC address. The entered MAC address will not be used to identify the device, but is required because inside the Cisco Unified Communications Manager configuration database, phone records are uniquely identified by MAC addresses.
-------------	--

- Step 3** Associate the third-party SIP phone with the end user configured in Step 1.
- Step 4** Configure the third-party SIP phone with the IP address of Cisco Unified Communications Manager (proxy address), end-user ID, digest credentials (optional), and directory numbers.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco Unified Communications Manager supports SIP, SCCP, and H.323 protocol for endpoints.
- Feature differences exist between SIP, SCCP, and H.323 endpoints and between different IP phone models.
- Cisco IP phones follow a specific boot process, allowing the IP phone to learn a voice VLAN ID, obtain IP configuration from a DHCP server, and download its configuration from a TFTP server.
- H.323 phones have to be configured on both Cisco Unified Communications Manager and also manually on the phone.
- Third-party SIP phones register by their directory number and a username, provided by digest authentication.

References

For additional information, refer to these resources:

- Voice and Unified Communications – Compare Products and Solutions
http://www.cisco.com/en/US/products/sw/voicesw/products_category_buyers_guide.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html

Lesson 2

Configuring Cisco Catalyst Switches for Endpoints

Overview

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

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

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

Objectives

Upon completing this lesson, you will be able to configure Cisco IOS Catalyst switches and Cisco Catalyst operating system switches to support Cisco IP phones, third-party IP phones, and software-based phones. This ability includes being able to meet these objectives:

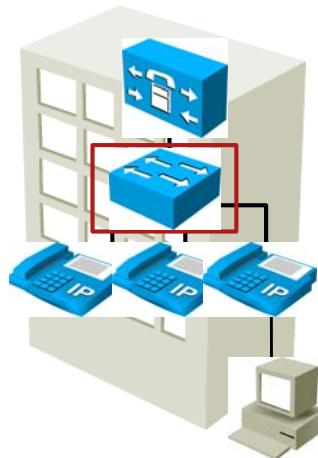
- Describe the role and features of Cisco LAN switches in a Cisco Unified Communications solution
- Describe how power can be provided to IP phones by Cisco LAN switches
- Configure Cisco LAN switches to provide power to IP phones
- Describe how to provide voice VLAN support to IP phones that have a PC attached to their PC port
- Describe why allowed VLANs on trunk ports should be limited
- Describe how to configure voice VLANs in Cisco IOS LAN switches
- Describe how to configure voice VLANs in Cisco Catalyst operating system LAN switches

Cisco LAN Switch Essentials

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

Cisco Catalyst Switch Role in IP Telephony

- Supplies inline power to IP phones
- Supports voice and data VLANs on a single access port
- Prioritizes voice traffic with CoS or DSCP marking



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-4

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

- **Inline power:** Inline power capabilities allow a Cisco Catalyst switch to send power through an Ethernet cable to a Cisco IP phone or other inline power-compatible device (such as wireless access point) without the need for an external power supply.
- **Voice VLAN support:** You can connect one or more network devices to the back of a Cisco IP phone because some Cisco IP phones have built-in switches. Voice VLANs allow you to place the IP phone, and the devices that are attached through the IP phone, on separate VLANs.
- **CoS marking:** CoS marking is data link layer (Layer 2) marking that is used to prioritize network traffic. Prioritizing voice traffic is critical in IP telephony networks. If voice traffic is not given priority, poor voice quality may result when voice frames wait in the switch queue behind large data frames.

Applying Switch Features

The table describes when and how to use some of the Cisco Catalyst switch features related to Cisco IP phones.

Applying Switch Features

Switch Features	When to Use	How to Use
PoE	When you require the reliability, availability and flexibility of PoE	Identify the PoE type required. PoE is enabled by default.
Voice VLAN	When you want to connect a PC to an IP phone and have both using a single physical port at the switch but with separate VLANs	Configure voice VLAN in addition to access VLAN.
QoS / CoS	When you want to ensure that voice quality is not affected by network traffic congestion	Identify the trust boundary and the applications. Configure the QoS base for your traffic requirements.

© 2008 Cisco Systems, Inc. All rights reserved.

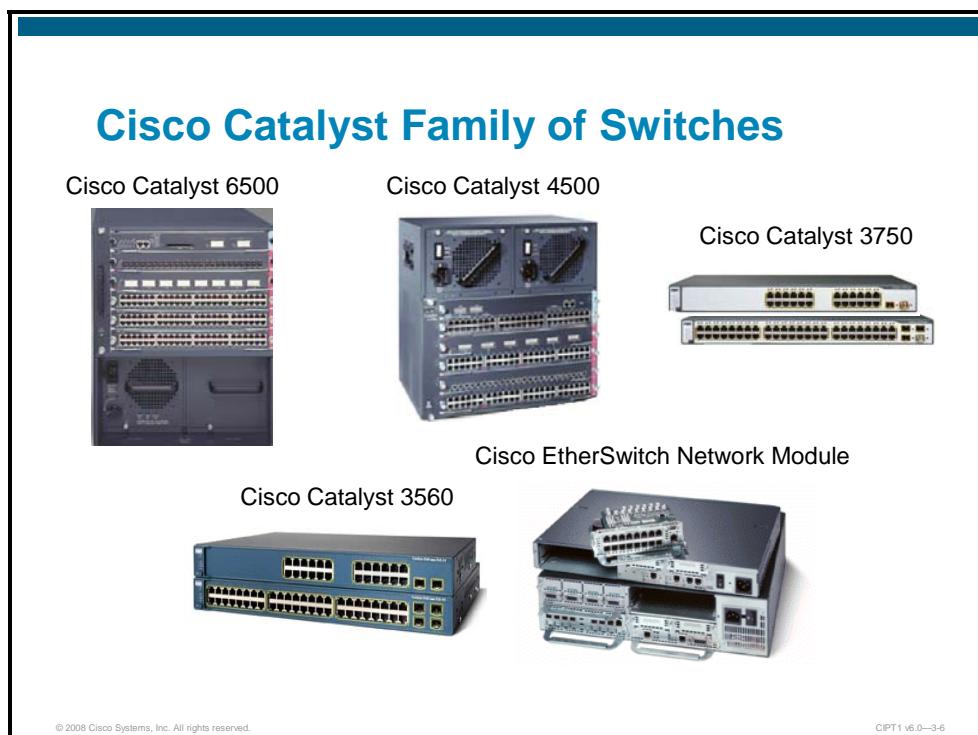
CIPT1 v6.0—3-5

Cisco Catalyst LAN switches provide the following three features to support Cisco IP phones:

- **Power over Ethernet (PoE):** You should use PoE when the reliability, availability, and flexibility of PoE is required. There are currently two types of PoE delivery: IEEE 802.3af-compliant PoE and a Cisco prestandard version. Before implementing PoE in the Cisco Unified Communications infrastructure, you should identify the proper PoE type in order to have PoE support on all switches in the network. PoE is enabled by default. With PoE, there is no need for power cubes to be connected to IP phones. IP phones have a single physical connection (Ethernet cable) which is used for providing power and for accessing the network.
- **Voice VLAN:** To reduce the number of required switch ports, Cisco IP phones provide a port to IP phones so that the IP phone and PC are connected to a single switch port. However, PCs and IP phones should usually be in different VLANs (voice vs. data). The voice VLAN feature of Cisco switches and IP phones allows an IP phone to use a VLAN other than the attached PC. When the Cisco Catalyst switch is configured for a voice VLAN, it will instruct the IP phone to use IEEE 802.1Q with the configured voice VLAN ID for its traffic, while the PC sends untagged traffic.
- **QoS/CoS:** This feature is used to ensure that voice quality is not affected by network traffic congestion. QoS is configured based on identified network traffic requirements, the trust boundary, and applications. If the voice VLAN feature is used on the Cisco Catalyst switch, the switch can instruct the phone to set a certain CoS value for traffic sent from a PC through an IP phone toward a switch.

Cisco Catalyst Family of Switches

The Cisco Catalyst LAN switching portfolio delivers a robust range of security and QoS capabilities.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-6

The Cisco Catalyst switch portfolio allows organizations to enable new business applications and integrate new technologies such as wireless and IP telephony into their network infrastructure. The following are the switches in the Cisco Catalyst family:

- **Cisco Catalyst modular switching:** The Cisco Catalyst 6500 Series delivers a 96-port 10BASE-T/100BASE-T line card, 48-port 10BASE-T/100BASE-T line card, and 10BASE-T/100BASE-T/1000BASE-T line card. The Catalyst 6500 Series offers a modular PoE daughter card architecture for the 96-port card and the 48-port 10/100/1000 card. The Cisco Catalyst 4500 Series delivers 48-port 10/100 and 10/100/1000 line cards. All line cards support both 802.3af and Cisco prestandard inline power. The Cisco Catalyst modular chassis switches can deliver 15.4W per port for all 48 ports on a module simultaneously.

Note	Overall power calculation has to be performed when power supply redundancy is desired. When too many PoE ports are used, power supply redundancy might fail because of too high load caused by PoE ports.
-------------	---

- **Cisco Catalyst stackable switching:** The Cisco Catalyst 3750 Series offers 48- and 24-port Fast Ethernet switches that comply with 802.3af and Cisco prestandard PoE. The Cisco Catalyst 3560 Series offers 48- and 24-port Fast Ethernet switches that support both the industry standard 802.3af and Cisco standard PoE.

- **Cisco EtherSwitch modules:** The Cisco 36- and 16-port 10/100 EtherSwitch modules for Cisco 2600, 2800, 3700, and 3800 Series routers offer branch office customers the option to integrate switching and routing in one platform. These modules can support Cisco prestandard PoE and provide straightforward configuration, easy deployment, and integrated management in a single platform. The Cisco 2600 Series requires a separate external PoE power supply; while the Cisco 2800, 3700, and 3800 Series can integrate the power supply.

The table lists the Cisco Catalyst PoE options.

Catalyst Switch PoE Options

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

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

Providing Power to IP Phones

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

Three Ways to Power Cisco IP Phones

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

The diagram illustrates three methods for powering a Cisco IP phone:

- Power over Ethernet (PoE):** Shows a Cisco Catalyst switch connected to an IP phone. A label "Power" points to the connection between the switch and the phone.
- Midspan power injection:** Shows a Cisco Unified IP Phone Power Injector (a blue rectangular device) inserted between a standard LAN switch and an IP phone. Labels indicate "No Power" entering the injector, "Power Injector" inside, and "Power" exiting to the IP phone.
- Wall power:** Shows an AC Source (a wall outlet) connected to a 110 V AC Wall Power to 48 V DC Converter (represented by a yellow rectangle). This converter is then connected to the IP phone.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-8

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

- **PoE:** With PoE, the phone plugs into the data jack that connects to the switch, and the user PC in turn connects to the IP phone. With power-sourcing equipment (PSE), such as Cisco Catalyst PoE-capable modular and fixed-configuration switches, power is inserted into the Ethernet cable, such as an IP phone or IEEE 802.11 wireless access point.
- **Midspan power injection:** Because some switches do not support PoE, a midspan power source may be used instead. This midspan device sits between the LAN switch and the powered device and inserts power on the Ethernet cable to the powered device. A major technical difference between the midspan and inline power mechanism is that power is delivered on the spare pairs (pins 4, 5, 7, and 8). An example of midspan PSE is a Cisco Unified IP Phone Power Injector.

Note More information about the Cisco Unified IP Phone Power Injector can be found in the document Cisco Unified IP Phone Power Injector at:
<http://www.cisco.com/en/US/partner/products/ps6951/index.html>.

■ **Wall power:** Wall power needs a DC converter for connecting the IP phone to a wall outlet.

Note The wall power supply must be ordered separately from the Cisco IP phone.

Two Types of PoE Delivery

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

Two Types of PoE Delivery

Cisco original implementation:

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

IEEE 802.3af Power over Ethernet:

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

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-9

Cisco provides the following two types of inline power delivery:

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

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

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

Power classification defines these five classes:

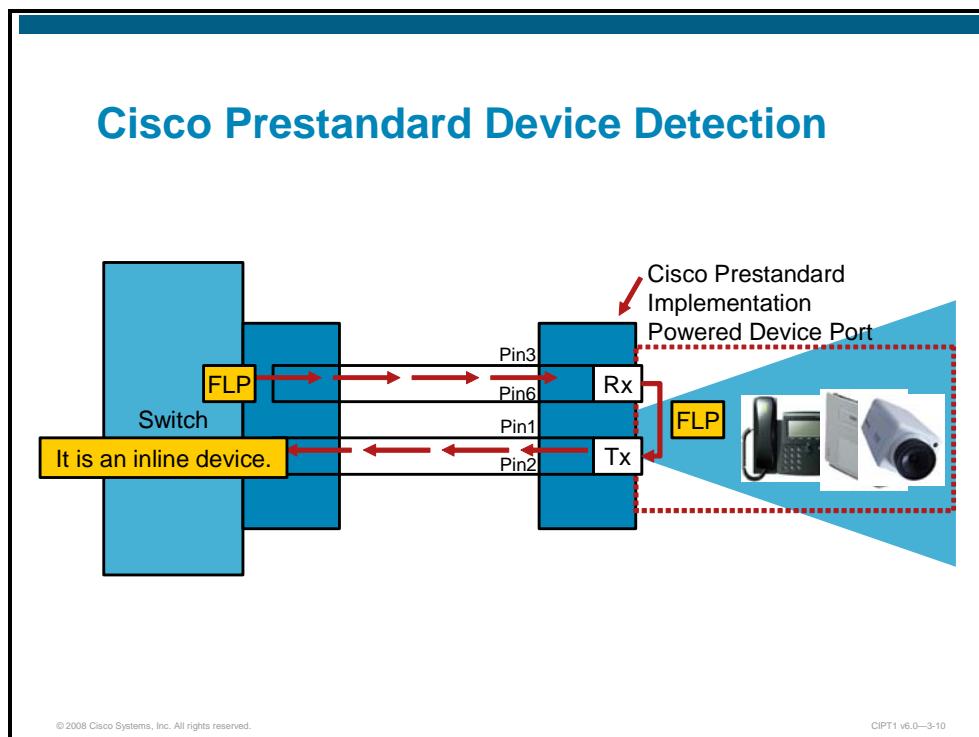
- **0 (default):** 15.4W reserved
- **1:** 4W
- **2:** 7W
- **3:** 15.4W
- **4:** Reserved for future expansion

All Cisco 802.3af-compliant switches support power classification.

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

Cisco Prestandard Device Detection

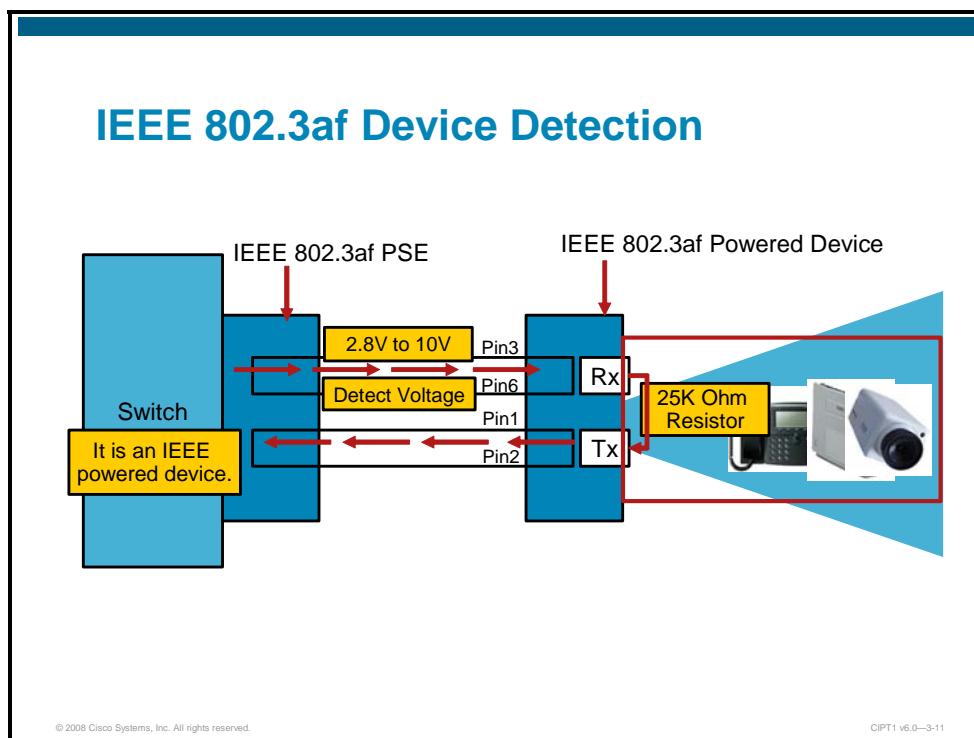
The figure illustrates how a Cisco Catalyst switch with prestandard PoE support detects a Cisco IP phone, wireless access point, or other inline power-capable device.



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

IEEE 802.3af Device Detection

The figure illustrates how a Cisco Catalyst 802.3af-compliant switch detects a Cisco IP phone, wireless access point, or other inline power-capable device.



The PSE (Cisco Catalyst switch) detects a powered device by applying a voltage in the range of -2.8V to -10V on the cable and then looks for a 25kOhm signature resistor. Compliant powered devices must support this resistance method. If the appropriate resistance is found, the Cisco Catalyst switch delivers power.

Configuring Cisco LAN Switches to Provide Power to IP Phones

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

Cisco Catalyst Switch: Configuring PoE

Cisco Catalyst Operating System:

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

Native Cisco IOS Software:

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

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-13

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

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

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

Cisco Catalyst Switch: Show Inline Power Status

The figure shows how to display the status of inline power on a Cisco Catalyst switch.

Cisco Catalyst Switch: Show Inline Power Status

```
show port inline power 7
Default Inline Power allocation per port: 10.000 Watts (0.23 Amps @42V)
Total inline power drawn by module 7: 75.60 Watts (1.80 Amps @42V)

Port      InlinePowered    PowerAllocated
        Admin     Oper       Detected      mWatt      mA @42V
        -----  -----  -----
7/1        auto      off       no           0          0
7/2        auto      on        yes         6300        150
7/3        auto      on        yes         6300        150
7/4        auto      off       no           0          0
7/5        auto      off       no           0          0
7/6        auto      off       no           0          0
7/7        auto      off       no           0          0
```



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

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-14

Use the command shown in the figure to display a view of the power allocated on Cisco Catalyst switches. The switch shows the default allocated power as 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.

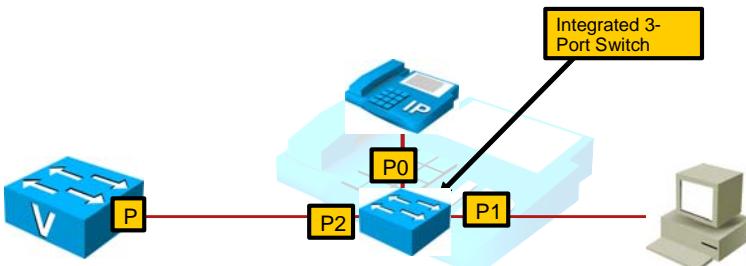
Inline Power Syntax Descriptions

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

Voice VLAN Support in Cisco IOS LAN Switches

This topic describes voice VLAN support in Cisco IOS LAN switches.

Cisco IP Phone Connected to the Network



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-16

The Cisco IP phone contains an integrated three-port 10/100 switch. The ports provide dedicated connections to these devices:

- Port 0 is an internal 10/100 interface that carries the Cisco IP phone traffic.
- Port 1 connects to a PC or other device.
- Port 2 connects to the access switch or other network devices. Inline power PSE can be obtained at port 2.

The voice VLAN feature allows voice traffic from the attached IP phone and data traffic from a daisy-chained PC to be transmitted on different VLANs. This capability provides flexibility and simplicity in IP address allocation and the prioritization of voice over data.

If Cisco Discovery Protocol is enabled on the switch port, the switch instructs an attached Cisco IP phone to treat Layer 2 CoS priority value of the attached PC in one of the following ways (based on the extended priority configured at the switch port):

- **Trusted:** The IP phone allows the PC to send IEEE 802.3 frames (with no CoS priority value) as well as IEEE 802.1p frames with any CoS priority value.
- **Untrusted (default):** The IP phone changes the CoS priority value to 0 if 802.1p is used by the PC.
- **Configured CoS priority level:** The IP phone sets an 802.1p header with a CoS priority value of x if the PC uses 802.1p with a different CoS priority level than x, or if the PC did not use 802.1p at all but sent 802.3 frames.

The traffic that is sent by the IP phone is trusted. It can be one of the following:

- **802.1Q:** In the voice VLAN, tagged with a Layer 2 CoS priority value
- **802.1p:** In the access VLAN, tagged with a Layer 2 CoS priority value
- **Untagged:** In the access VLAN, untagged with no Layer 2 CoS priority value

If Cisco Discovery Protocol is enabled on the switch port, the switch instructs the IP phone to use one of the three listed options, based on the **voice vlan** command.

Voice VLAN Support

This subtopic describes the voice VLAN support provided by a Cisco Catalyst switch.

Voice VLAN Support

- A Cisco Catalyst switch can be configured to support voice traffic in various ways:
 - Single VLAN access port
 - Multi-VLAN access port
 - Trunk port
- Considerations:
 - Security
 - Cisco IP phones/non-Cisco IP phones/IP softphones
 - Spanning tree
 - QoS

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-17

There are various methods of configuring the Cisco Catalyst switch to support voice traffic, including the following:

- Single VLAN access port
- Multi-VLAN access port
- Trunk port

Various factors have to be taken into considerations, including the following:

- Security
- Cisco IP phones/other IP phones/IP softphones (IP softphone is used here as a generic term for all software-based IP phones installed on a workstation.)
- Spanning tree
- QoS

Single VLAN Access Port

This subtopic describes a single VLAN access port and how you can use it to connect to an IP phone.

Single VLAN Access Port

- An **access** port configured for one VLAN only
- Typically used for non-Cisco IP phones or softphones
 - Non-Cisco IP phones: Use voice VLAN for access port
 - Softphones: Use data VLAN for access port and allow required IP communication to voice VLAN (IP ACLs)
- If used with Cisco IP phones:
 - Not recommended with PC attached
 - If no PC attached: Use voice VLAN for access port
- Voice can be tagged with 802.1p (VLAN ID=0) or untagged

The diagram illustrates a single VLAN access port configuration. On the left, a blue switch icon labeled 'Access Port' has two outgoing ports. The top port connects to a blue IP phone icon with a red double-headed arrow labeled 'Untagged or 802.1p'. The bottom port connects to a computer icon (monitor and keyboard) with a blue double-headed arrow labeled 'Untagged 802.3'. A small note at the bottom left says '© 2008 Cisco Systems, Inc. All rights reserved.' and a note at the bottom right says 'CIPT1 v6.0—3-18'.

A single VLAN access port is the default state when an IP phone is connected to an unconfigured Cisco Catalyst switch. It is typically used for non-Cisco IP phones, IP softphones, or when Cisco IP phones or other Cisco voice devices (such as the Cisco VG248 Analog Phone Gateway) do not support PCs to be connected to them.

When using the port for such a device, the access VLAN ID should be the ID of the voice VLAN, that is, the VLAN containing the phones. If a softphone is used on a PC, the device itself, the PC, cannot be in different VLANs per application (phone software versus data applications). Therefore, the access port is usually configured for the data VLAN and the IP address (or subnet) of the PC is allowed to access VLANs with voice devices (Cisco Unified Communications Manager servers, IP phones, and so on).

If a Cisco IP phone has a PC attached, it is not recommended to put both into the same VLAN, because voice and data services should be separated.

Features of a single VLAN access port include the following:

- It can be configured as a secure port.
- It allows physical separation of voice and data traffic using different physical ports.
- It works with both Cisco and other IP phones.
- The IP phone can use 802.1p (with VLAN ID set to 0) for CoS.

Switches other than Cisco switches are typically configured in this way because they do not usually support the voice VLAN feature.

Multi-VLAN Access Port

This subtopic describes a multi-VLAN access port and how it can be used to connect to an IP phone.

Multi-VLAN Access Port

- An **access** port able to handle two VLANs
 - Access (data) VLAN and voice (auxiliary) VLAN
- Voice traffic is tagged with 802.1Q VLAN ID
 - Data traffic is untagged and is forwarded by IP to and from PC port.
 - Phone can be hardened to prevent PC from seeing the voice traffic (by default, phone acts like a hub).
 - Best choice with Cisco IP phones.
 - Voice VLAN does not need to be configured on IP phone but can be learned from Cisco Discovery Protocol messages sent out by the switch.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-19

Multi-VLAN access ports are supported by all Cisco Catalyst switches. All data devices typically reside on data VLANs in the traditional switched scenario. A separate voice VLAN may be needed when combining the voice network into the data network. Cisco Catalyst switches using Catalyst Operating System refer to the voice VLAN as the auxiliary VLAN. The new voice VLAN can be used to represent Cisco IP phones. Although it is a voice VLAN, in the future, other types of non-data devices will reside in the voice VLAN.

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

You can implement multiple VLANs on the same port by configuring an access port. A tagging mechanism distinguishes among VLANs on the same port. 802.1Q is the IEEE standard for tagging frames with a VLAN ID number. The IP phone sends tagged 802.1Q frames. The PC sends untagged frames and the switch puts the frame into the configured access VLAN. When the switch receives a frame from the network destined for the PC, it removes the access VLAN tag before forwarding the untagged frame to the PC.

These are some advantages of implementing dual VLANs:

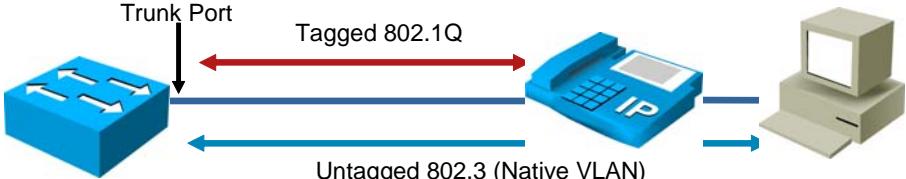
- A multi-VLAN access port can be configured as a secure port.
- A voice VLAN ID is discovered using Cisco Discovery Protocol or it is configured on the IP phone.
- Dual VLANs allow for the scalability of the network, from an addressing perspective. IP subnets usually have more than 50 percent (often more than 80 percent) of their IP addresses allocated. A separate VLAN (separate IP subnet) to carry the voice traffic allows the introduction of a large number of new devices, such as IP phones, into the network without extensive modifications to the IP addressing scheme.
- Dual VLANs allow for the logical separation of data and voice traffic, which allows the network to handle these two traffic types individually.
- Implementing dual VLANs allows you to connect two devices that are in different VLANs to a single switch port.

Trunk Ports

This subtopic describes trunk ports and how you can use them to connect to an IP phone.

Trunk Ports

- A **trunk** port is able to handle multiple VLANs.
- Usually data traffic is untagged and put into a native VLAN.
- Data traffic can be tagged with any 802.1Q VLAN ID if supported by PC (and permitted by IP phone).
- A voice VLAN does not need to be configured on IP phone but can be learned from Cisco Discovery Protocol messages sent out by the switch.
- Security considerations:
 - Cannot be configured as secure port
 - If allowed VLANs are not limited, PC has access to all VLANs of the switch



© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-20

Rather than a dual VLAN access port, you can use a trunk port for connecting a switch to an IP phone. Because a Cisco Catalyst switch supports multi-VLAN access ports, a trunk port is not commonly used to connect a switch to a Cisco IP phone. However, a trunk port can also be a way to connect a Cisco IP phone to switch other than Cisco. Some of the first Cisco switches supported voice VLAN features, allowing the voice VLAN ID to be used by a phone via Cisco Discovery Protocol only on trunk ports.

When an IEEE 802.1Q trunk port is used, frames of the native VLAN are always transmitted untagged and should be received untagged. In other words, a PC, which usually does not send 802.1Q frames but rather untagged Ethernet frames, is part of the native VLAN, while the Cisco IP phone tags its frames with 802.1Q. However, a PC could send and receive tagged frames and thus access all VLANs configured in the switch.

On trunk ports, tagged frames are permitted by default. Therefore, the only function of this command is to allow the IP phone to learn the VLAN ID that should be used for its traffic by Cisco Discovery Protocol (although not required because it can be manually configured at the phone). Some of the considerations when implementing a trunk port to support Cisco IP phones are as follows:

- On some end-of-life (EOL) Cisco IOS and Catalyst switches, PortFast cannot be enabled on a trunk port.
- The port cannot be configured as a secure port.
- The PC can access all VLANs if it supports 802.1Q.

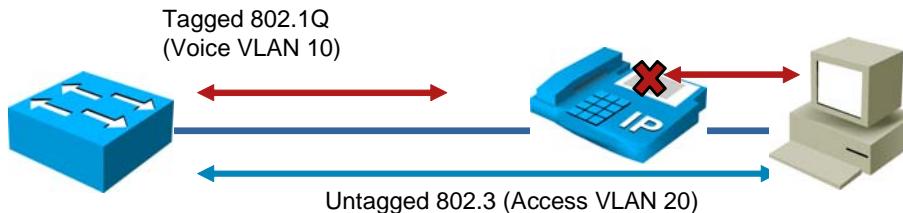
Limiting VLANs on Trunk Ports

This topic describes the need to block traffic to the voice VLAN on the PC port.

Blocking PC VLAN Access at IP Phones

With default configuration on a trunk port, if PC sends 802.1Q tagged frames, all VLANs can be accessed from PC.

- Disable voice VLAN access at phone
 - Prevent PC from sending and receiving data tagged with voice VLAN ID
 - Other VLAN IDs are permitted on some IP phones
- Disable span to PC port (on supported IP phones)
 - Prevent PC from sending and receiving any 802.1Q tagged frames



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-22

When a PC is connected to an IP phone, there are two potential security issues:

- If the switch port is configured as a trunk, the PC has access to all VLANs.
- If the switch port is configured as an access port, the PC has access to the voice VLAN. The reason for this is that, by default, the IP phone forwards all frames received from the switch to the PC and vice versa.

You can configure Cisco IP phones to block access by the PC to the voice VLAN. If configured, the IP phone will not forward frames tagged with the voice VLAN ID. This solves PC VLAN access issues with dual VLAN access ports, because the PC is limited to using the access VLAN (untagged frames). Newer IP phones have an additional setting (“span to PC port”) which allows blocking all frames with an 802.1Q header. This solves PC VLAN access issues with trunk ports, but this feature is not available on all phones—it is only supported on type B Cisco IP phones.

Limits VLANs on Trunk Ports at the Switch

This subtopic describes limiting VLANs on trunk ports.

Limits VLANs on Trunk Ports at the Switch

- VLANs allowed on a trunk port can be configured at the switch.
- Recommendation is to only allow native VLAN and voice VLAN.
 - Blocks PC access to all other VLANs, independent of IP phone configuration and model
 - Access to voice VLAN, can only be prevented by IP phone configuration but is supported on all IP phone models with PC ports
 - Improves performance
 - Improves stability – Minimizes STP issues

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-23

Trunk ports on Cisco Catalyst switches should be configured to allow only the necessary VLANs. In case of a Cisco IP phone with an attached PC, these are the voice VLAN and the native VLAN. Denying all other VLANs provides the following advantages:

- **Increased security:** The attached PC cannot access VLANs other than the voice VLAN. This limitation can also be achieved by IP phone configuration, but only with type B IP phone models. When using other IP phone models, access to the VLANs can only be blocked at the switch. An attacker could unplug the cable from the IP phone and plug it directly into the PC in order to bypass the VLAN access control feature of the IP phone. You can stop this kind of attack by disallowing unnecessary VLANs at the switch.
- **Increased performance:** Reducing the number of VLANs cuts down unnecessary broadcast traffic.
- **Increased stability:** Limiting the number of VLANs will also minimize potential Spanning Tree Protocol (STP) issues and increase network stability.

Configuring Voice VLANs in Cisco IOS LAN Switches

This topic describes how to configure voice VLANs on Cisco Catalyst switches using native Cisco IOS Software.

Configuring Voice VLANs in Access Port Using Native Cisco IOS Software

Example 1 (single VLAN access port):

```
Console(config)#interface FastEthernet0/1
Console(config-if)#switchport mode access
Console(config-if)#switchport voice vlan dot1p
Console(config-if)#switchport access vlan 261
```

Example 2 (multi-VLAN access port):

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

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-25

Use the commands shown in the figure to configure voice and data VLANs on the single port interface of a switch that is running native Cisco IOS Software.

The first example shows the configuration of a single VLAN access port. The switch is configured to transmit Cisco Discovery Protocol packets to enable the Cisco IP phone to transmit voice traffic in 802.1p frames, tagged with VLAN ID 0 and a Layer 2 CoS value. The switch puts the 802.1p voice traffic into the configured access VLAN, VLAN 261, which is used for voice traffic.

The second example shows a multi-VLAN access port configuration in which the voice traffic is sent to VLAN 261 and the data is using the access VLAN 262.

Note	The multi-VLAN access port is the recommended configuration for Cisco IP phones that have a PC port.
-------------	--

Catalyst Switch Voice Interface Commands

Command	Description
switchport mode access	Configures the switchport to be an access (non-trunking) port.
spanning-tree portfast	Causes a port to enter the spanning-tree forwarding state immediately, bypassing the listening and learning states. You can use PortFast on switch ports that are connected to a single workstation or server (as opposed to another switch or network device) to allow those devices to connect to the network immediately.
switchport access vlan data_VLAN_ID	Configure the interface as a static access port with the access VLAN ID (262 in this example); the range is 1 to 4094.
switchport voice vlan {voice_vlan_ID dot1p none untagged}	<p>When configuring the way in which the Cisco IP phone transmits voice traffic, note the following syntax information:</p> <ul style="list-style-type: none"> ■ Enter a voice VLAN ID to send Cisco Discovery Protocol v2 packets that configure the Cisco IP phone to transmit voice traffic in 802.1Q frames, tagged with the voice VLAN ID and a Layer 2 CoS value (the default is 5). Valid VLAN IDs are from 1 to 4094. The switch puts the 802.1Q voice traffic into the voice VLAN. ■ Enter the dot1p keyword to send Cisco Discovery Protocol v2 packets that configure the Cisco IP phone to transmit voice traffic in 802.1p frames, tagged with VLAN ID 0 and a Layer 2 CoS value (the default is 5 for voice traffic and 3 for voice control traffic). The switch puts the 802.1p voice traffic into the access VLAN. ■ Enter the untagged keyword to send Cisco Discovery Protocol v2 packets that configure the Cisco IP phone to transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN. ■ Enter the none keyword to allow the Cisco IP phone to use its own configuration and transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.

Configuring Trunk Port Using Native Cisco IOS Software

This topic shows how to configure trunk ports on Cisco Catalyst switches using native Cisco IOS Software.

Configuring Trunk Port Using Native Cisco IOS Software

Example 3 (trunk port):

```
Console(config)#interface FastEthernet0/1
Console(config-if)#switchport trunk encapsulation dot1q
Console(config-if)#switchport mode trunk
Console(config-if)#switchport trunk native vlan 262
Console(config-if)#switchport voice vlan 261
Console(config-if)#switchport trunk allowed vlan 261
```

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-26

Use the commands shown in the figure to configure the trunk interface of a switch that is running native Cisco IOS Software.

In the example, VLAN 261 is used for voice traffic and VLAN 262, which is also the native VLAN, is used for data traffic. All other VLANs are blocked from the trunk interface.

Note The native VLAN does not have to be permitted in the allowed VLAN list.

Catalyst Switch Voice Interface Commands

Command	Description
switchport mode trunk	Configures the switchport to be a trunk port.
Switchport trunk encapsulation dot1q	Configures the switchport trunk encapsulation to 802.1Q instead of leaving it as auto-detect.
switchport trunk native vlan VLAN-ID	Configures the interface native VLAN. When you use an IEEE 802.1Q trunk port, all frames are tagged except those on the VLAN configured as the native VLAN for the port. Frames on the native VLAN are always transmitted untagged and are normally received untagged.
spanning-tree portfast trunk	Causes a port to enter the spanning-tree forwarding state immediately, bypassing the listening and learning states. You can use the portfast command on switch ports that are connected to a single workstation or server (as opposed to another switch or network device) to allow those devices to connect to the network immediately.
Switchport trunk allowed vlan VLAN-ID	Specifies the VLANs that are allowed on the trunk port.

Verifying Voice VLAN Configuration Using Native Cisco IOS Software

This subtopic describes how to verify voice VLAN configuration on Cisco Catalyst switches that use native Cisco IOS Software.

Verifying Voice VLAN Configuration Using Native Cisco IOS Software

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

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-27

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

Configuring Voice VLANs in Cisco Catalyst Operating System LAN Switches

This topic shows how to configure voice VLANs on Cisco Catalyst switches using a Cisco Catalyst operating system.

Configuring Voice VLANs Using Cisco Catalyst Operating System

Example 1 (single VLAN access port):

```
Console>(enable) set port auxiliaryvlan 2/1-3 dot1p  
Console>(enable) set vlan 262 2/1-3  
Console>(enable) set trunk 2/1-3 off
```

Example 2 (multi-VLAN access port):

```
Console>(enable) set port auxiliaryvlan 2/1-3 261  
Console>(enable) set vlan 262 2/1-3  
Console>(enable) set trunk 2/1-3 off
```

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-29

Use the commands shown in the figure to configure voice and data VLANs on the single port interface of a switch that is running native Cisco Catalyst operating system software.

The first example shows the configuration of a single VLAN access port. The switch is configured to transmit Cisco Discovery Protocol packets to enable the Cisco IP phone to transmit voice traffic in 802.1p frames, tagged with VLAN ID 0 and a Layer 2 CoS value. The switch puts the 802.1p voice traffic into the configured access VLAN, VLAN 261, which is used for voice traffic.

The second example shows a multi-VLAN access port configuration, in which the voice traffic is sent to VLAN 261 (Auxiliary VLAN) and the data uses the access VLAN 262.

Catalyst Switch Catalyst Operating System Interface Commands

Command	Description
set port auxiliaryvlan	Configures voice or auxiliary VLAN for the switchport.
set vlan	Configures the access VLAN (untagged) for the switchport. In a trunk port, this will configure the native VLAN for the switchport. When an 802.1Q trunk port is used, all frames are tagged except those on the VLAN configured as the "native VLAN" for the port. Frames on the native VLAN are always transmitted untagged and are normally received untagged.
set trunk	Configures trunk ports and adds VLANs to the allowed VLAN list for existing trunks.

Configuring Trunk Ports Using Cisco Catalyst Operating System

This example shows how to configure trunk ports on Cisco Catalyst switches using a native Cisco Catalyst operating system.

Configuring Trunk Ports Using Cisco Catalyst Operating System

Example 3 (trunk port):

```
Console>(enable) set trunk 2/1-3 on
Console>(enable) clear trunk 2/1-3 1-4096
Console>(enable) set vlan 262 2/1-3
Console>(enable) set port auxiliaryvlan 261 2/1-3
Console>(enable) set trunk 261 2/1-3
```

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-30

In 802.1Q trunking, all VLAN packets are tagged on the trunk link, except the native VLAN packets. The native VLAN packets are sent untagged on the trunk link. Therefore, the native VLAN is used for the data traffic coming in from the workstation attached to the Cisco IP phone. By default, VLAN 1 is the native VLAN on all switches.

In this example, VLAN 262 is set as the native VLAN and is untagged and will be used by the data traffic. VLAN 261 is tagged with 802.1Q tagging and will be used by the voice traffic.

In the Cisco Catalyst operating system, you can change the native VLAN by using the **set vlan vlan-id mod/port** command, in which mod/port is the trunk port. The **set trunk** command can be used to configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks. The voice VLAN is configured with the **set port auxiliaryvlan** command.

Verifying Voice VLAN Configuration Using Cisco Catalyst Operating System

The example shows how to verify voice VLAN configuration on Cisco Catalyst switches that use the Cisco Catalyst operating system.

Verifying Voice VLAN Configuration Using Cisco Catalyst Operating System

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

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

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-31

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

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

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco LAN switches can supply inline power to IP phones.
- Two types of PoE delivery are supported by Cisco LAN switches.
- PoE delivery methods can be configured on Cisco LAN switches.
- Cisco LAN switches can be configured to support voice traffic in 3 different ways: single VLAN access port, multi-VLAN access port, and trunk port.
- Only required VLANs should be allowed on a trunk port.
- Access and trunk ports can be configured to support Cisco IP phones.
- Voice VLAN configuration can be verified using Cisco Catalyst operating system and Cisco IOS commands and tools.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-32

References

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Catalyst 3550 Multilayer Switch Software Configuration Guide, Rel. 12.2(25)SEE – Configuring Voice VLAN
http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3550/software/release/12.2_25_see/configuration/guide/swvoip.html
- Catalyst 3550 Multilayer Switch Software Configuration Guide, Rel. 12.2(25)SEE – Configuring CDP
http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3550/software/release/12.2_25_see/configuration/guide/swcdp.html

Lesson 3

Implementing and Hardening IP Phones

Overview

Adding, updating, and deleting phones are important functions in the day-to-day activities of a Cisco Unified Communications Manager administrator. Cisco Unified Communications Manager provides various tools to accomplish these tasks.

This lesson describes how to implement Skinny Client Control Protocol (SCCP) and session initiation protocol (SIP) phones (Cisco and third-party phones) in Cisco Unified Communications Manager (manually, using autoregistration, and with Cisco Unified Communications Manager Bulk Administration Tool [BAT]) and how to harden the Cisco IP phones.

Objectives

Upon completing this lesson, you will be able to implement SCCP and SIP phones (Cisco and third-party phones) in Cisco Unified Communications Manager and harden the Cisco IP phones. This ability includes being able to meet these objectives:

- Identify the endpoint configuration elements and tools for adding phones
- Describe how autoregistration works
- Describe how to enable autoregistration for automatic insertion of new phones to the Cisco Unified Communications Manager configuration database
- Describe how Cisco Unified Communications Manager BAT and Cisco Unified Communications Manager Auto-Register Phone Tool can be used to add IP phones
- Describe how to use Cisco Unified Communications Manager BAT to add phones to Cisco Unified Communications Manager
- Describe how to manually add phones to Cisco Unified Communications Manager
- Describe Cisco IP phone configuration settings that can be used to harden IP phones

Examining Endpoint Configuration Tools and Elements

This topic describes the various endpoint configuration tools and elements for adding phones.

Configuration Methods and Tools

Method for Adding IP Phones	Advantages	Disadvantages
Autoregistration	<ul style="list-style-type: none">▪ Devices automatically added	<ul style="list-style-type: none">▪ Default Settings, random DN▪ Modifications needed
Unified CM BAT	<ul style="list-style-type: none">▪ Bulk add	<ul style="list-style-type: none">▪ MAC addresses required in BAT files
Unified CM Auto-Register Phone Tool	<ul style="list-style-type: none">▪ Very scalable▪ MAC addresses not required	<ul style="list-style-type: none">▪ Cisco CRS required▪ Complex configuration
Manual Configuration	<ul style="list-style-type: none">▪ Simple	<ul style="list-style-type: none">▪ MAC addresses required▪ Time-consuming

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-4

There are basically four methods of adding IP phones to the Cisco Unified Communications Manager:

- Using autoregistration
- Using Cisco Unified Communications Manager BAT
- Using Cisco Unified Communications Manager Auto-Register Phone Tools
- Manual configuration

Autoregistration allows the administrator to add Cisco IP phones to the Cisco Unified Communications Manager without first compiling a list of MAC addresses of the endpoints. Without autoregistration, changes in the configuration must be done manually. Without using Cisco Unified Communications Manager BAT and Cisco Unified Communications Manager Auto-Register Phone Tool, there is no easy way for the phone to be associated with the correct user. If the user has specific requirements, these will have to be updated manually after the device has been registered.

Cisco Unified Communications Manager BAT allows bulk adds of phones, but MAC addresses of IP phones must be known and included in the BAT files.

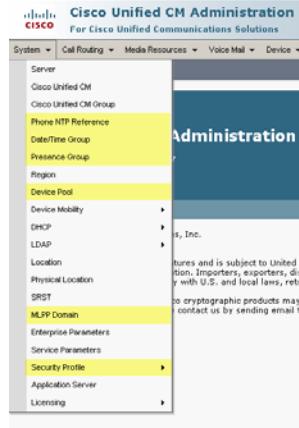
The Cisco Unified Communications Manager Auto-Register Phone Tool is more scalable, but it requires a separate Cisco Customer Response Solutions (CRS) server, and therefore the administrator must be familiar with the installation and configuration of the Cisco CRS server. When using the Cisco Unified Communications Manager Auto-Register Phone Tool, MAC addresses are automatically added and associated with the correct phone configurations that have been added previously using Cisco Unified Communications Manager BAT (with dummy MAC addresses only).

Adding phone devices manually is the easiest way to add IP phones to the Cisco Unified Communications Manager, but has the disadvantage of being tedious and time-consuming. To the administrator must manually compile a list of the MAC addresses of the IP phones and ensure that they are correctly entered when creating device records for the phones.

Regardless of the configuration methods and tools used, the various endpoint-related configuration elements remain the same.

Endpoint Basic Configuration Elements

This subtopic describes the basic configuration elements that are common to endpoints.



The screenshot shows the Cisco Unified CM Administration interface. The left sidebar contains a navigation menu with several items highlighted in yellow: Phone NTP Reference, Device Pool, and Security Profile. The main content area displays a list of configuration elements:

- Phone NTP Reference
- Date / Time Group
- Presences Group
- Device Pool
 - Cisco Unified CM Group
 - Regions
 - Locations
- Security Profile
- Softkey Templates
- Phone Button Templates
- SIP Profile (SIP Phones Only)
- Common Phone Profile

At the bottom of the interface, there is a copyright notice: © 2008 Cisco Systems, Inc. All rights reserved. and a reference: CIPT1 v6.0—3-5.

The figure shows some basic endpoint configuration elements. Some configuration elements can be assigned to the endpoint and some elements are assigned indirectly through a device pool.

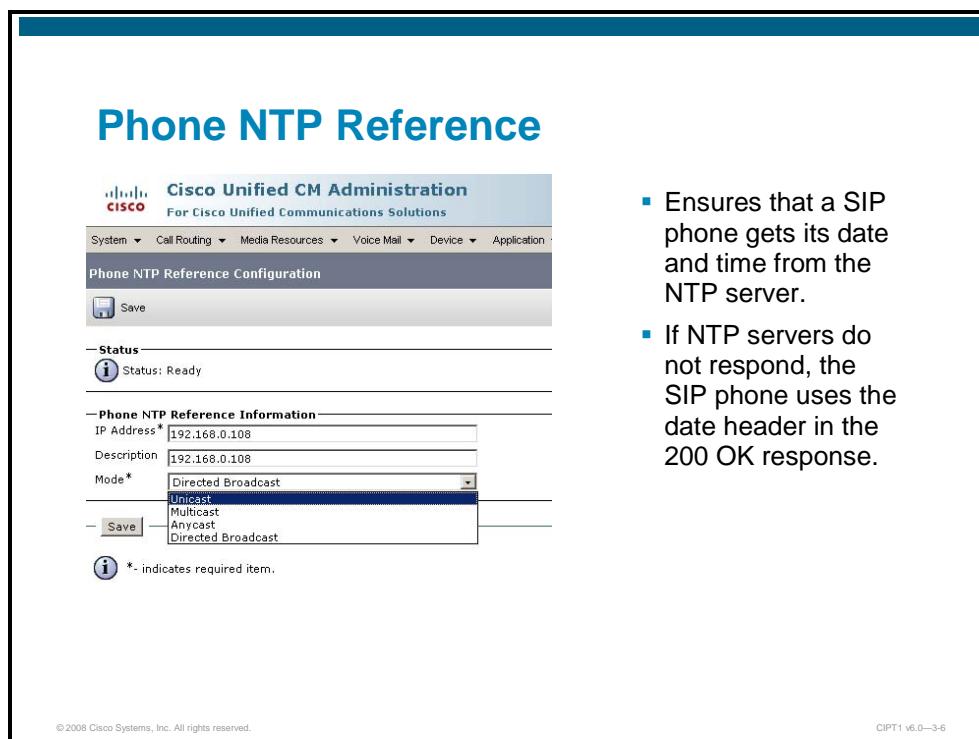
Examples of elements assigned through a device pool are as follows:

- Cisco Unified Communications Manager Group
- Regions
- Locations

Configuration elements can be optional or mandatory. Some mandatory elements have predefined defaults and the administrator can make use of these defaults in basic scenarios.

Phone NTP Reference

This subtopic describes the phone Network Time Protocol (NTP) reference.



The screenshot shows the Cisco Unified CM Administration interface with the title "Phone NTP Reference". The main content area displays the "Phone NTP Reference Configuration" form. It includes fields for "Status" (set to "Ready"), "Phone NTP Reference Information" (IP Address: 192.168.0.108, Description: 192.168.0.108), and "Mode" (set to "Unicast"). A note at the bottom indicates that an asterisk (*) denotes required items. To the right of the screenshot, two bullet points describe the function of NTP references:

- Ensures that a SIP phone gets its date and time from the NTP server.
- If NTP servers do not respond, the SIP phone uses the date header in the 200 OK response.

You can configure phone NTP references in Cisco Unified Communications Manager Administration to ensure that a SIP phone gets its date and time from an NTP server. If no NTP server is reachable, the SIP phone uses the date header in the 200 OK response to the REGISTER message for the date and time. SCCP phones obtain time information within SCCP messages.

After the phone NTP reference has been added to Cisco Unified Communications Manager Administration, it must be added to a date/time group. You can configure priorities of the phone NTP references in the date/time group.

The date/time group configuration is referenced from a device pool, and the device pool is assigned to a device at the device configuration page.

The table describes the Phone NTP Reference Configuration fields.

Phone NTP Reference Field Descriptions

Field	Description
IP Address	Enter the IP address of the NTP server that the SIP phone should use to get its date and time. Cisco Unified Communications Manager cannot be configured for phone NTP references.
Description	Enter a description for the phone NTP reference. Cisco Unified Communications Manager Administration automatically propagates the information in the IP Address field to the Description field, but it can be edited.
Mode	<p>From the drop-down list box, choose the mode for the phone NTP reference. The values available are as follows:</p> <p>Directed Broadcast: This is the default NTP mode, in which the phone accesses date/time information from any NTP server, but gives the listed NTP servers (1st = primary, 2nd = secondary) priority. For example, if the phone configuration contains NTP servers where A = primary NTP server and B = secondary/backup NTP server, the phone uses the broadcast packets (derives the date/time) from NTP server A. If NTP server A is not broadcasting, the phone accesses date/time information from NTP server B. If neither NTP server is broadcasting, the phone accesses date/time information from any other NTP server. If no other NTP server is broadcasting, the phone will derive the date/time from the Cisco Unified Communications Manager 200 OK response to the REGISTER message.</p> <p>Unicast: In this mode, the phone will send an NTP query packet to that particular NTP server. If the phone gets no response, the phone will access date/time information from any other NTP server. If no other NTP servers respond, the phone will derive the date/time from the Cisco Unified Communications Manager 200 OK response to the REGISTER message.</p>

Note	Although selectable, Cisco Unified Communications Manager currently does not support the multicast and anycast modes. If either of these modes is selected, Cisco Unified Communications Manager will default to the directed broadcast mode.
-------------	---

Date/Time Group Configuration

This subtopic describes the Date/Time Group Configuration.

The screenshot shows the Cisco Unified CM Administration interface with the title 'Date/Time Group Configuration'. The window contains fields for 'Group Name' (set to 'Singapore'), 'Time Zone' (set to 'Singapore Standard Time - (GMT+08:00) Kuala Lumpur'), 'Separator' (set to '-' (dash)), 'Date Format' (set to 'D-M-Y'), and 'Time Format' (set to '12-hour'). Below these fields is a section titled 'Phone NTP References for this Date/Time Group' which contains a 'Selected Phone NTP References' list. At the bottom of the window are 'Add Phone NTP References' and 'Remove Phone NTP References' buttons, and a 'Save' button. The status bar at the bottom of the window displays '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—3-7'.

- Date/Time groups define time zones for devices connected to Cisco Unified Communications Manager.
- Date/time group is assigned to device pool.
- Device pool is assigned to device.

Use date/time groups to define time zones for devices that are connected to Cisco Unified Communications Manager. Each device exists as a member of only one device pool, and each device pool has only one assigned date/time group.

Installation of Cisco Unified Communications Manager automatically configures a default date/time group called CMLocal. CMLocal synchronizes to the active date and time of the operating system on the server where Cisco Unified Communications Manager is installed. After installing Cisco Unified Communications Manager, you can change the settings for CMLocal.

Note	CMLocal resets to the operating system date and time whenever the Cisco Unified Communications Manager gets restarted or when the Cisco Unified Communications Manager software is upgraded to a new release. Do not change the name of CMLocal.
-------------	--

The table shows the field descriptions for the Date/Time Group Configuration window.

Date/Time Group Configuration Field Descriptions

Field	Description
Group Name	Enter the name that is assigned to the new date/time group.
Time Zone	In the drop-down list, select the time zone for the group that is being added.
Separator	Choose the separator character to use between date fields.
Date Format	Choose the date format for the date that displays on the Cisco Unified IP phones.
Time Format	Choose a 12-hour or 24-hour time format.
Selected Phone NTP References (ordered by highest priority)	<p>To ensure that a SIP phone gets its date and time configuration from an NTP server, add the phone NTP references to the date/time group by performing the following tasks:</p> <ul style="list-style-type: none"> ■ Click the Add Phone NTP References button. Find the phone NTP reference that needs to be added. ■ Only phone NTP references that exist in the Cisco Unified Communications Manager database display. After the search results display, check the check boxes for the phone NTP references or click Select All. ■ Click Add Selected.

Device Pools

This subtopic describes the device pool configuration.

The screenshot shows the 'Device Pool Configuration' window with the title 'Device Pools'. The window has tabs for 'Device Pool Information' and 'Device Pool Settings'. Under 'Device Pool Information', the device pool is named 'Default' with 15 members. Under 'Device Pool Settings', fields include 'Device Pool Name' (Default), 'Cisco Unified Communications Manager Group' (CUCMGroup), 'Calling Search Space for Auto-registration' (< None >), and 'Reverted Call Focus Priority' (Default). The 'Roaming Sensitive Settings' tab is also visible, containing fields like 'Date/Time Group' (CMLocal), 'Region' (Default), 'Media Resource Group List' (< None >), 'Location' (< None >), 'Network Locale' (< None >), 'SRST Reference' (Disable), 'Connection Monitor Duration' (**), 'Physical Location' (< None >), and 'Device Mobility Group' (< None >). At the bottom, there are buttons for Save, Delete, Copy, Reset, and Add New, along with copyright and version information.

- Device pools define sets of common characteristics for devices.
- The device pool structure supports the separation of user and location information.
- The device pool contains only device- and location-related information.

Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains only device- and location-related information. The Common Device Configuration window records all the user-oriented information such as type of softkey template that is used and locale information. You should ensure that each device is associated with a device pool and with a common device configuration for user-oriented information.

To create a new device pool, these mandatory components must be created, or default settings used where applicable:

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

The device pool combines all of the individual configuration settings that have been created into a single entity. This element can then be assigned to individual devices, such as IP phones. This process will configure these devices with most of the configuration elements that they need to operate efficiently in the IP telephony network.

Complete these steps to create the device pool:

- Step 1** Choose **System > Device Pool**. The Find and List Device Pools window opens.
- Step 2** Click the **Add New** button to open the Device Pool Configuration window.
- Step 3** Choose, at a minimum, the Cisco Unified Communications Manager Group, Date/Time Group, Region, and a Softkey Template.

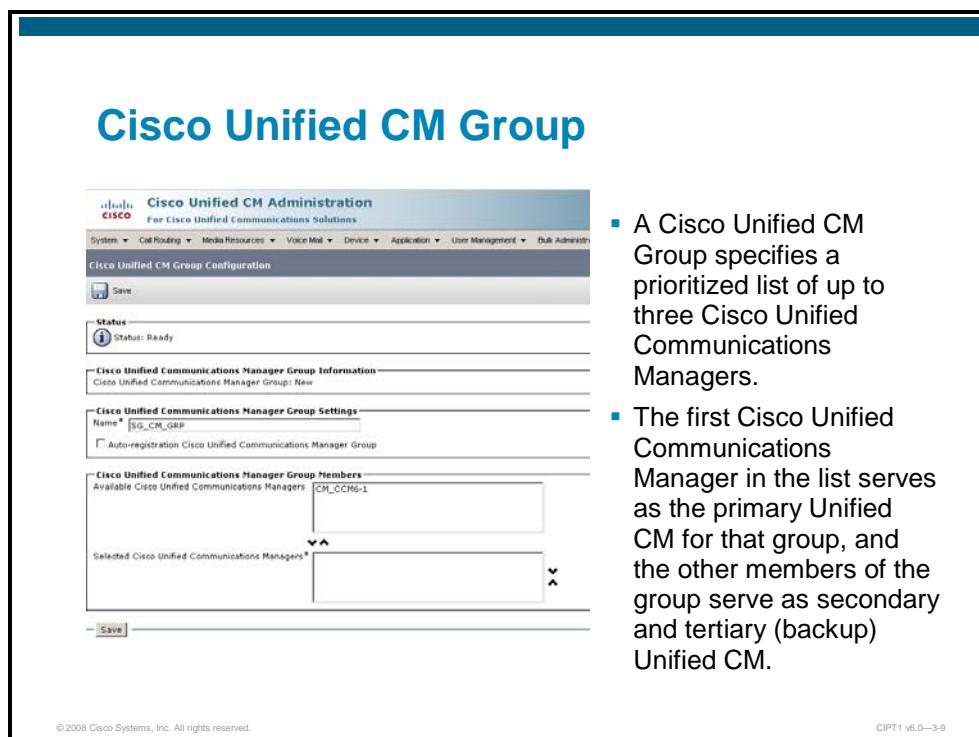
Device Pool Configuration Fields

Field	Description
Device Pool Name*	Describes a name for the device pool.
Cisco Unified Communications Manager Group*	Chooses a redundancy group for the device pool. This redundancy group can contain a maximum of three redundant Cisco Unified Communications Manager servers.
Date/Time Group*	Assigns the correct time zone to the device.
Region*	Determines the coder-decoder (codec) selection used by the device, depending on the end location of the call.
Softkey Template*	Defines the type and order of the softkeys that are displayed on the LCD of a Cisco IP phone.
SRST Reference*	Configures SRST and chooses the gateway that will support the device if the connection to the Cisco Unified Communications Manager is lost.
Calling Search Space for Auto-Registration	Defines who an IP phone is able to call if it autoregisters with the Cisco Unified Communications Manager.
Media Resource Group List	Assigns media resource support to a device for functions such as conferencing, transcoding, or music on hold (MOH).
Network Hold MOH Audio Source	Chooses the audio that Cisco Unified Communications Manager should play when you press the Transfer or Conference button on the Cisco IP phone.
User Hold MOH Audio Source	Chooses the audio that Cisco Unified Communications Manager should play when you press the Hold button on the Cisco IP phone.
Network Locale	Defines the tones and cadences that the device uses.
User Locale	Defines the language that the device uses.
Connection Monitor Duration	Defines the amount of time that the IP phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and reregisters to Cisco Unified Communications Manager. This is to ensure that the registration is stable in case of a flapping link. The default for the enterprise parameter specifies 120 seconds, which can be modified on a device-pool basis or left at the default value.

Note An asterisk (*) Indicates a required field.

Cisco Unified CM Group

This subtopic describes the Cisco Unified CM Group.



The screenshot shows the Cisco Unified CM Administration interface. The title bar reads "Cisco Unified CM Administration" and "Cisco Unified Communications Solutions". The main menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, and Bulk Administration. The current page is "Cisco Unified CM Group Configuration". It displays a form with fields for "Status" (Status: Ready), "Cisco Unified Communications Manager Group Information" (Cisco Unified Communications Manager Group: New), "Cisco Unified Communications Manager Group Settings" (Name: SG_CM_GRP, Auto-registration: Cisco Unified Communications Manager Group checked), and "Cisco Unified Communications Manager Group Members" (Available Cisco Unified Communications Managers: CH_CCM6-1, Selected Cisco Unified Communications Managers: CH_CCM6-1). A "Save" button is at the bottom. The footer includes copyright information: "© 2008 Cisco Systems, Inc. All rights reserved." and "CIPT1 v6.0—3-9".

- A Cisco Unified CM Group specifies a prioritized list of up to three Cisco Unified Communications Managers.
- The first Cisco Unified Communications Manager in the list serves as the primary Unified CM for that group, and the other members of the group serve as secondary and tertiary (backup) Unified CM.

A Cisco Unified CM Group specifies a prioritized list of up to three Cisco Unified Communications Managers.

The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager for that group, and the other members of the group serve as secondary and tertiary (backup) Cisco Unified Communications Managers.

Each device pool has one Cisco Unified Communications Manager Group that is assigned to it. When a device registers, it attempts to connect to the primary (first) Cisco Unified Communications Manager in the group that is assigned to its device pool. If the primary Cisco Unified Communications Manager is not available, the device tries to connect to the next Cisco Unified Communications Manager that is listed in the group, and so on.

Cisco Unified Communications Manager Groups provide these important features for the unified communications system:

- **Redundancy:** This feature allows the administrator to designate a primary and backup Cisco Unified Communications Manager for each group.
- **Call processing load balancing:** This feature allows the administrator to distribute the control of devices across multiple Cisco Unified Communications Managers.

For most systems, there is a need for multiple groups, and a single Cisco Unified Communications Manager can be assigned to multiple groups to achieve better load distribution and redundancy.

Regions

This subtopic describes the regions configuration.

Regions

Region Configuration

Region Information

Name *	HQ_gw
--------	-------

Region Relationships

Region	Audio Codec	Video Call Bandwidth	Link Loss Type
BR_phones	G.729	384	Use System Default
HQ_phones	G.711	384	Use System Default

NOTE: Regions(s) not displayed Use System Default Use System Default Use System Default

Modify Relationship to other Regions

Regions	Audio Codec	Video Call Bandwidth	Link Loss Type
BR_gw	Keep Current Setting	Keep Current Setting	Keep Current Setting
BR_phones	Keep Current Setting	Keep Current Setting	Keep Current Setting
HQ_phones	Keep Current Setting	Keep Current Setting	Keep Current Setting
HQ_gw	Keep Current Setting	Keep Current Setting	Keep Current Setting
HQ_trunks	Keep Current Setting	Keep Current Setting	Keep Current Setting

Keep Current Setting
 Use System Default
 None
 kbps

- Use regions to specify the bandwidth that is used for an audio or video call within a region and between regions by codec type.
- The audio codec determines the type of compression and the maximum amount of bandwidth that is used per audio call.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-10

Regions are used to specify the maximum bandwidth that is used per audio or video call within a region and between regions.

The configured audio codec determines the type of compression and hence the maximum amount of bandwidth that is used per audio call.

The video call bandwidth comprises the sum of the audio and video bandwidth of the video call.

Note The default audio codec for all calls through Cisco Unified Communications Manager specifies G.711. If there is no plan to use any other audio codec, it is not required to change region configuration.

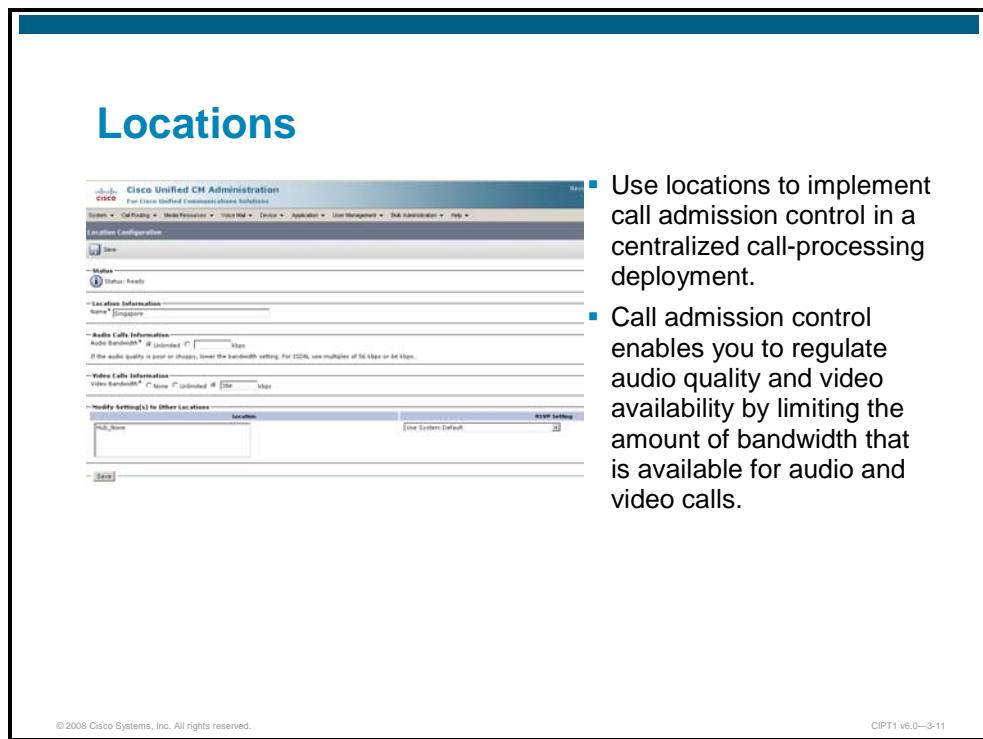
Complete these steps to configure a region:

- Step 1** Choose **System > Region**. The default region that was created during the Cisco Unified Communications Manager installation appears.
 - Step 2** Click **Add New** to configure the regions.
 - Step 3** Give the new region a unique name. Click **Save**.
 - Step 4** Choose the codec and video bandwidth as appropriate between the regions.
-

Note Cisco Unified Communications Manager allows a maximum of 500 regions.

Locations

This subtopic describes the locations configuration.



The screenshot shows the Cisco Unified CM Administration interface for 'Locations Configuration'. The main title is 'Locations'. The page includes sections for 'Media' (with a 'Return-Keystroke' checkbox), 'Location Information' (with a 'Name' field containing 'Corporate'), 'Audio Call Information' (with an 'Audio Bandwidth' dropdown set to 'Unlimited' and a note about audio quality), 'Video Call Information' (with a 'Video Bandwidth' dropdown set to 'None' and a note about bandwidth usage), and a 'Modify Setting(s) to Other Locations' section where 'Poly_Nome' is selected and 'Use System Default' is checked. At the bottom, there is a note about E1/T1 settings and a footer with copyright information and a revision number.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-11

- Use locations to implement call admission control in a centralized call-processing deployment.
- Call admission control enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls.

Use locations to implement call admission control in a centralized call-processing system. Call admission control enables the administrator to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls that go in or out of a location.

Note	If call admission control is not used to limit the audio and video bandwidth on IP WAN links, an unlimited number of calls can be active on that link at the same time. This situation can cause the quality of all audio and video calls to degrade as the link becomes oversubscribed.
-------------	--

In a centralized call-processing system, a single Cisco Unified Communications Manager cluster provides call processing for all locations on the IP telephony network. The Cisco Unified Communications Manager cluster usually resides at the main (or central) location, along with other devices such as phones and gateways. The remote locations contain additional devices, but no Cisco Unified Communications Manager. IP WAN links connect the remote locations to the main location.

Phone Security Profile

This subtopic describes the phone security profile configuration.

Phone Security Profile

The screenshot shows the 'Phone Security Profile Configuration' page in Cisco Unified CM Administration. It includes sections for 'Phone Security Profile Information' (Product Type: Cisco 7960, Device Protocol: SCCP, Name: Cisco 7960 - Standard SCCP Non-Secure Profile, Description: Cisco 7960 - Standard SCCP Non-Secure Profile, Device Security Mode: Non Secure) and 'Phone Security Profile CAPF Information' (Authentication Mode: By Null String, Key Size (bits): 1024). Buttons for Copy, Reset, and Add New are at the bottom.

■ The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (for SIP phones only), and encrypted configuration file settings.

■ You must apply a security profile to each phone that is configured in Cisco Unified Communications Manager Administration.

The Phone Security Profile Configuration window includes security-related settings such as device security mode, Certificate Authority Proxy Function (CAPF) settings, digest authentication settings (for SIP phones only), and encrypted configuration file settings. A security profile must be applied to all phones that are configured in Cisco Unified Communications Manager Administration. The administrator can use existing security profiles that have security disabled.

Device Settings

This subtopic describes the device settings configuration.

The screenshot shows the Cisco Unified CM Administration interface with the title 'Device Settings'. The main menu bar includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Device' menu is expanded, showing options like 'CTI Route Point', 'Gatekeeper', 'Gateway', 'Phone', 'Trunk', 'Remote Destination', and 'Device Settings'. A sub-menu for 'Device Settings' is open, listing 'Device Defaults', 'Firmware Load Information', 'Default Device Profile', 'Device Profile', 'Phone Button Template', 'Softkey Template', 'Phone Services', 'SIP Profile', 'Common Device Configuration', 'Access List', 'Common Phone Profile', 'Remote Destination Profile', and 'Recording Profile'. On the left, there's a search bar for 'Find and List Phones' with a 'Find' button and a 'Clear Filter' button. Below the search bar is a 'Phone' section with a 'Find Phone where [Device Name]' dropdown and an 'Add New' button. The center of the screen contains a large text block: 'Device Settings contain default settings, profiles, templates, and common device configurations that can be assigned to a device or device pool.' At the bottom of the interface, there are copyright and version information: '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—3-13'.

Device settings contain default settings, profiles, templates, and common device configurations that you can assign to the device or device pool.

Device Defaults Configuration

This subtopic describes the device defaults configuration.

Device Defaults Configuration

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Device Defaults Configuration

Save

Status: Ready

Device Defaults Information	Device Type	Protocol	Load Information	Device Pool	Phone Template
7914 14-Button Line Expansion Module SCCP		SCCP	S001050001300	Default	None
Analog Access		Protocol Not Specified		Default	None
Analog Access WS-X6624		Protocol Not Specified	A002H024	Default	None
Analog Phone		SCCP	NONE	Default	Standard Analog
Cisco 12 S		SCCP		Default	Standard 12 S
Cisco 12 SP		SCCP		Default	Standard 12 SP
Cisco 12 SP+		SCCP		Default	Standard 12 SP+
Cisco 30 SP+		SCCP		Default	Standard 30 SP+
Cisco 30 VP		SCCP		Default	Standard 30 VP
Cisco 3951		SIP	SIP3951.B-0-1	Default	Standard 3951 SIP
Cisco 7902		SCCP	CFC7902B0000021CCP00	Default	Standard 7902
Cisco 7905		SIP	005080001151P040412A	Default	Standard 7905 SIP
Cisco 7905		SCCP	S0000035C9P07049A	Default	Standard 7905 SCCP
Cisco 7906		SCCP	SCCP11.B-0-1S	Default	Standard 7906
Cisco 7906		SIP	SIP11.B-0-1S	Default	Standard 7906 SIP

Use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified Communications Manager.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-14

Use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified Communications Manager. The device defaults for a device type apply to all autoregistered devices of that type within a Cisco Unified Communications Manager cluster. You can set the following device defaults for each device type to which they apply:

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

When a device autoregisters with Cisco Unified Communications Manager, it inherits the default settings for its device type.

Complete these steps to update the device defaults:

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Device Defaults** to open the Device Defaults Configuration window.
- Step 2** In the Device Defaults Configuration window, modify the appropriate settings for the device.
- Step 3** Click **Save** to save the changes in the Cisco Unified Communications Manager configuration database.

Phone Button Template

This subtopic describes the phone button template configuration.

The screenshot shows the Cisco Unified CM Administration interface with the title "Phone Button Template". The main area displays a table titled "Button Information" with 15 rows, each representing a button number (1 through 15) and its assigned function. A context menu is open over the first few rows, showing options like "Edit", "Hold", "Transfer", "Forward All", "Line", "Priority", "Service URL", "Call Park", "Call Park BLF", and "Intercom". To the right of the table, there is a column labeled "Label" with corresponding icons for each button assignment. At the bottom left of the interface, it says "© 2008 Cisco Systems, Inc. All rights reserved." and at the bottom right, "CIPT1 v6.0—3-15".

Creating and using templates provides a fast way to assign a common button configuration to a large number of Cisco Unified IP phones.

Cisco Unified Communications Manager includes several default phone button templates. When adding phones, one of these templates can be assigned to the phones or a new template can be created.

Make sure that all phones have at least one line assigned, which is normally button 1. Additional lines to a phone depend on the model of Cisco Unified IP phone. Phones generally have several features, such as speed dial and call forward, which are assigned to the remaining buttons.

Before adding any IP phones to the system, you should create phone button templates for all IP phone models used.

Softkey Template

This subtopic describes the softkey template configuration.

Softkey Template

Softkey template configuration allows the administrator to configure softkey layouts which are assigned to Cisco Unified IP phones.

Softkey template configuration allows the administrator to manage softkeys on Cisco IP phones. Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Applications that support softkeys can have one or more standard softkey templates that are associated with them; for example, Cisco Unified Communications Manager has the standard feature and the standard user softkey templates that are associated with it. Standard softkey templates cannot be modified or deleted. To create a new softkey template, copy one of the templates, edit it, and save it with a new name or create a new one from scratch.

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

SIP Profile

This subtopic describes the SIP profile configuration.

The screenshot shows the 'SIP Profile Configuration' screen in the Cisco Unified CM Administration interface. The top navigation bar includes links for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled 'SIP Profile Configuration' and contains sections for 'Status' (Status: Ready), 'SIP Profile Information' (Name: Standard SIP Profile, Description: Default SIP Profile, Default RTP Telephony Event Payload Type: ILOI), and 'Parameters used in Phone' (Timer Invite Expires (seconds): 180, Timer Register Delta (seconds): 5, Timer Register Expires (seconds): 3600, Timer T1 (msec): 5000, Timer T2 (msec): 40000, Retry INVITE: 5, Retry Non-INVITE: 10, Start Media Port: 16304, Stop Media Port: 32766). A note at the bottom states: 'A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on.'

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks or SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup Uniform Resource Identifier (URI), and so on. The profiles contain some standard entries that cannot be deleted or changed.

Note A SIP URI consists of a call destination configured with a user@host format, such as xten3@CompB.cisco.com or 2085017328@10.21.91.156:5060.

A default SIP profile, called the Standard SIP Profile, can be assigned to SIP phones on the SIP phone configuration page. The Standard SIP Profile cannot be deleted or modified. To create a new SIP profile, copy the default SIP profile, edit it, and save it with a new name, or create a new profile.

Common Phone Profile

This subtopic describes the common phone profile configuration.

Common Phone Profile

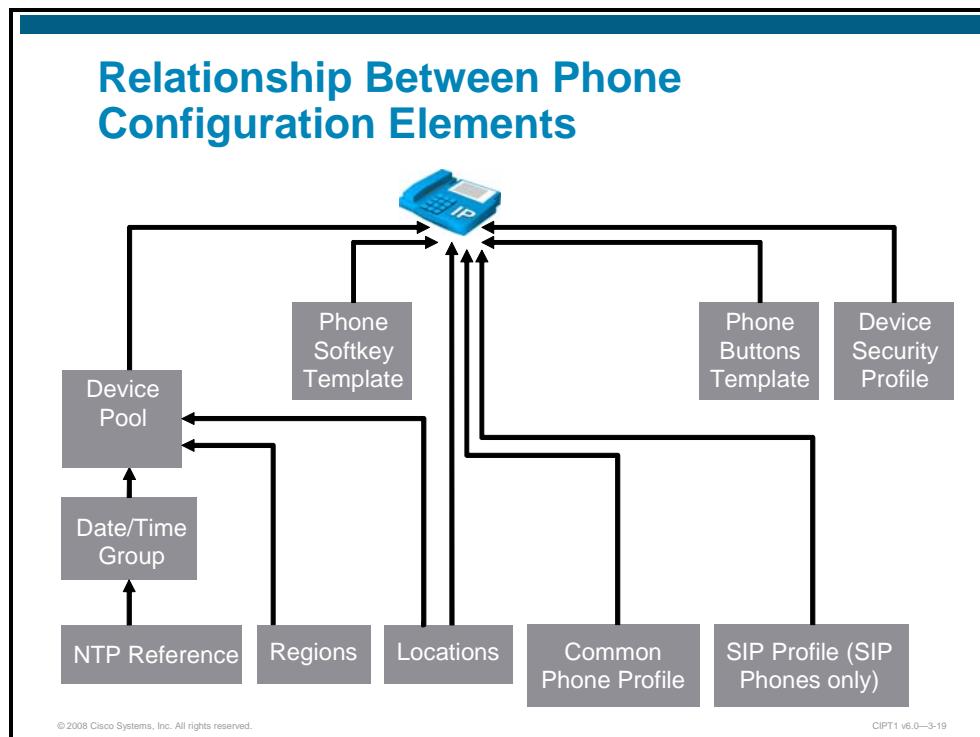
The screenshot shows the Cisco Unified CM Administration interface for configuring a Common Phone Profile. The window title is "Common Phone Profile Configuration". The "Status" field indicates "Status: Ready". The "Common Phone Profile Information" section contains fields for "Name*", "Description", "Local Phone Unlock Password", "DND Option*", "DND Incoming Call Alert*", and "Phone Personalization*". A checkbox for "Enable End User Access to Phone Background Image Setting" is checked. A "Save" button is at the bottom left. Below the window, a note states: "Common phone profiles include phone configuration parameters and are assigned to IP phones." The footer includes copyright information: "© 2008 Cisco Systems, Inc. All rights reserved." and "CIPT1 v6.0—3-18".

Common phone profiles include phone configuration parameters such as the phone password (for supported Cisco IP phones), Do Not Disturb (DND), and personalization settings, including end user access to background images. After a common phone profile has been configured, use the Common Phone Profile Configuration window to associate an SCCP or SIP phone with it.

The administrator can choose to use the default standard common phone profile which is created when Cisco Unified Communications Manager is installed, if no specific settings are required.

Relationship Between Phone Configuration Elements

The figure illustrates the relationship between different phone configuration elements.



The arrows show the assignment of elements. For example, “NTP Reference” is applied as an element to the “Date/Time Group” and the “Date/Time Group” is applied as an element of the “Device Pool” configuration. The Device Pool is one of the elements in the device record of an IP phone, allowing the IP phones to inherit or acquire settings that have been defined in the various elements.

In some cases, such as “Locations”, the element can be applied to both the “Device Pool” and the phone configuration, in which case, the value applied to the phone configuration will have higher priority.

Some of the elements apply to only specific device types. For example, SIP Profile applies only to a SIP phone.

IP Phone Autoregistration

This topic describes how autoregistration works.

Autoregistration

- Supported by all Cisco IP phones.
- Existing endpoints are not affected.
- Automatically adds Cisco IP phones not found in database (based on MAC addresses).
- An autoregistration directory number range is configured and each phone added by autoregistration is assigned with the next available directory number of the configured range.
- Cisco Unified Communications Manager BAT can be used to make bulk changes after autoregistration.
- Cisco Unified Communications Manager Auto-Register Phone Tool can be used to associate phones with specific directory numbers.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-21

Autoregistration allows Cisco Unified Communications Manager to issue extension numbers to new IP phones, which is similar to the way in which the DHCP server issues IP addresses.

With autoregistration configured and enabled, when a new IP phone boots and attempts to register with Cisco Unified Communications Manager for the first time, Cisco Unified Communications Manager issues an extension number from a configured range. After Cisco Unified Communications Manager issues the extension, it adds the phone to its configuration database with the used device ID (MAC address) and the assigned extension.

After the phone is added, the assigned extension usually has to be modified because a specific extension is intended to be used for a given phone.

Therefore, autoregistration only slightly simplifies registration when you add a large number of IP phones. The MAC addresses of the phones are automatically added to the Cisco Unified Communications Manager configuration database. The extensions per phone must still be modified.

Some phone settings, such as device pools, need to be globally changed from their default values. You can use Cisco Unified Communications Manager BAT after phones have been autoregistered.

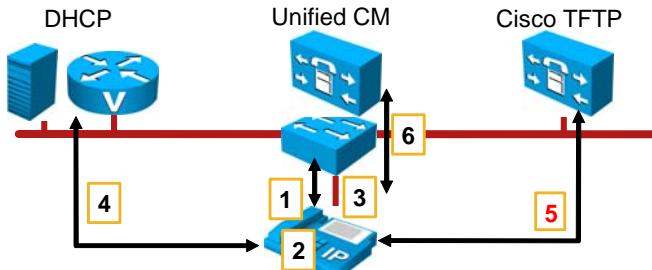
For large deployments, you can use the Cisco Unified Communications Manager Auto-Register Phone Tool, which allows specific extensions to be assigned to individual phones based on user input.

Autoregistration is supported by all Cisco IP phones and does not affect IP phones that are already configured.

Autoregistration Process

This section describes how autoregistration works.

Autoregistration Process



Autoregistration may occur as part of the IP phone startup process when the IP phone tries to download its configuration file from the TFTP server.

The Cisco IP phone with MAC address 0015C5AABBDD attempts to download configuration from TFTP server:

1. If TFTP server does not contain IP phone configuration file (e.g., SEP0015C5AABBDD.cnf.xml), the TFTP server returns “Read Error” to the IP phone.
2. IP phone will then download XmlDefault.cnf.xml from the TFTP server.
3. IP phone will update its firmware based on the phone load information defined in the configuration file.

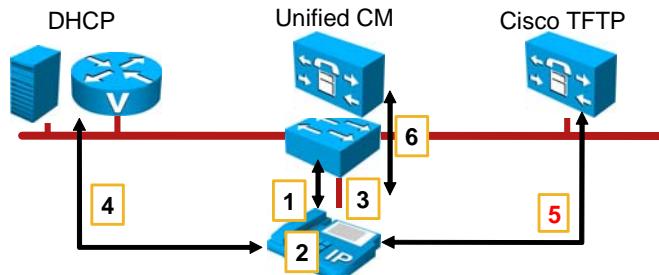
© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-22

Autoregistration occurs as part of the IP phone startup process—when the IP phone tries to download its configuration file from the TFTP server. Assuming the IP phone has a MAC address of 0015C5AABBDD, the following steps will occur when the Cisco IP phone attempts to download the configuration from the TFTP server:

- Step 1** If the TFTP server does not contain a configuration file for this phone (such as SEP0015C5AABBDD.cnf.xml), the TFTP server will return “Read Error” to the IP phone TFTP request.
- Step 2** The IP phone will then download the XmlDefault.cnf.xml file from the TFTP server.
- Step 3** The IP phone will update its firmware based on the phone load information defined in the configuration file.

Autoregistration Process (Cont.)



4. IP phone will then register to the Cisco Unified Communications Manager server configured for autoregistration defined in the XmlDefault.cnf.xml.
5. Cisco Unified Communications Manager will automatically create a phone device record in the database and assign a DN from the configured autoregistration range to the first line of the device and then create the configuration file (SEP0015C5AABBDD.cnf.xml).
6. IP phone will then download the configuration file (SEP0015C5AABBDD.cnf.xml) and register to the Cisco Unified Communications Manager.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-23

- Step 4** The IP phone registers to the Cisco Unified Communications Manager server configured for autoregistration and specified in the file XmlDefault.cnf.xml.
- Step 5** Cisco Unified Communications Manager automatically creates a phone device record in the configuration database and assigns a directory number to the first line of the device based on the autoregistration directory number range. A configuration file (SEP0015C5AABBDD.cnf.xml) is created and added to the TFTP server.
- Step 6** The IP phone downloads its configuration file (SEP0015C5AABBDD.cnf.xml) and registers to the Cisco Unified Communications Manager.

Considerations for Autoregistration

This subtopic describes some of the factors that you must consider when you use autoregistration.

Considerations for Autoregistration

- Only one directory number can be assigned.
- Directory number is assigned out of a pool; no control which phone gets which directory number.
- Autoregistration protocol (SCCP or SIP) is set globally within the cluster.
- Autoregistration is enabled per Cisco Unified Communications Manager Group but can be activated selectively on group members.
- Endpoints that support both SIP and SCCP firmware will be converted between SIP or SCCP automatically.
- Only Cisco IP phones are supported.
- Manual configuration changes are typically required, but process of adding phones is speeded up and MAC address typing errors are eliminated.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-24

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

A range of directory numbers must be configured on Cisco Unified Communications Manager for autoregistration, and Cisco Unified Communications Manager assigns the next available directory number from that range. Only a single directory number is assigned per IP phone, and you cannot control which device will get which directory number.

The default protocol for autoregistered IP phones is set globally within the cluster and can be set to either SIP or SCCP. For endpoints that are SIP- and SCCP-capable, the endpoint firmware is automatically converted to match the default autoregistration protocols. Endpoints that support only one protocol will still be able to autoregister, even if autoregistration protocol is set to the other protocol.

Autoregistration only works for Cisco IP phones.

After autoregistration, additional manual configuration changes will probably be required.

Configuring Autoregistration

This topic describes how to enable autoregistration for automatic insertion of new phones to the Cisco Unified Communications Manager configuration database.

Steps for Configuring Autoregistration

1. Verify (or change) the autoregistration phone protocol.
2. Ensure that autoregistration is enabled on one Cisco Unified CM Group.
3. For each Cisco Unified CM of the Cisco Unified CM Group, enable or disable autoregistration and, if enabled, configure a range of DNs to be assigned.
4. Manual reconfiguration or Cisco Unified Communications Manager BAT may be used to personalize autoregistered devices.

© 2008 Cisco Systems, Inc. All rights reserved.

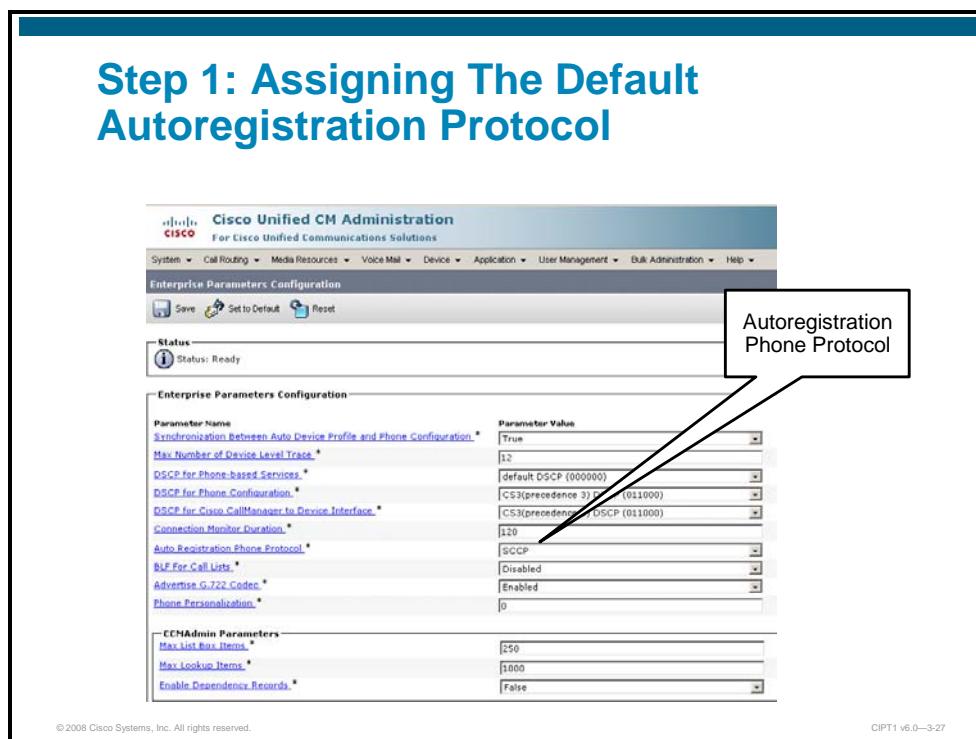
CIPT1 v6.0—3-26

There are four steps involved in configuring autoregistration; the fourth step is optional although commonly required:

- Step 1** Verify that the desired autoregistration default protocol is selected.
- Step 2** Ensure that autoregistration is enabled on one Cisco Unified Communications Manager Group.
- Step 3** Configure Cisco Unified Communications Manager member servers of that group selectively to be used for autoregistration and, if enabled on a particular server, set this server directory number range.
- Step 4** Reconfigure the automatically added phones, applying the individually required configuration settings. This can be done using Cisco Unified Communications Manager BAT for groups of phones that share some settings, or manually for each phone.

Step 1: Assigning the Default Autoregistration Protocol

The figure shows the first step in configuring autoregistration.

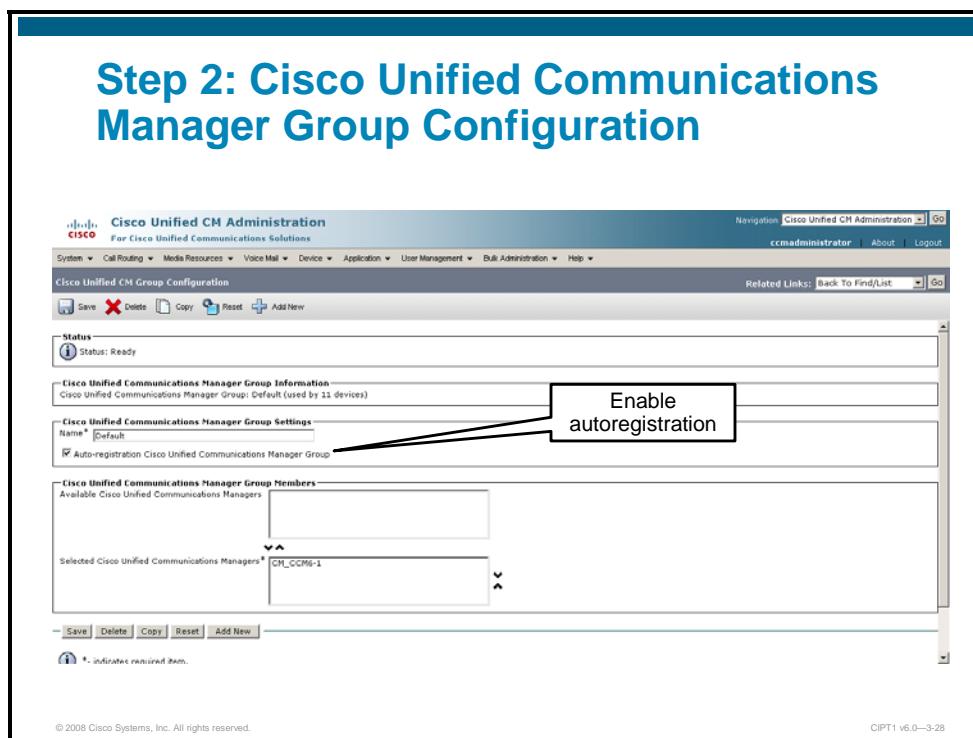


The default autoregistration protocol is an enterprise parameter, configured under **System > Enterprise Parameters**. This parameter specifies the protocol that should be used on Cisco IP phones that support SCCP and SIP.

The default autoregistration protocol is SCCP. Restart all services for the parameter change to take effect.

Step 2: Cisco Unified CM Group Configuration

This diagram shows the second step of configuring autoregistration, which is to enable autoregistration for one Cisco Unified Communications Manager group.



First, go to **System > Cisco Unified CM Group** and choose the group you want to configure. At the Cisco Unified Communications Manager group that should provide the autoregistration service, click the Auto-registration Cisco Unified Communications Manager Group checkbox.

You can only enable autoregistration on one Cisco Unified Communications Manager group. Activating autoregistration on one Cisco Unified Communications Manager group automatically disables the checkbox on the group that had autoregistration enabled before (if applicable).

Step 3: Cisco Unified CM Configuration

This step describes how to enable autoregistration on the members of the Cisco Unified Communications Manager group for which autoregistration has been enabled.

Step 3: Cisco Unified Communications Manager Configuration

The screenshot shows the 'Cisco Unified CM Configuration' page. At the top, there's a status message: 'Status: Ready'. Below it, under 'Cisco Unified Communications Manager Information', it says 'Cisco Unified Communications Manager: CM_CCM6-1 (used by 11 devices)'. The 'Server Information' section includes fields for CTI ID (1), Cisco Unified Communications Manager Server (CCM6-1), Cisco Unified Communications Manager Name (CM_CCM6-1), and Description (CCM6-1). The 'Auto-registration Information' section contains fields for Starting Directory Number (1000), Ending Directory Number (1999), Partition (< None >), and External Phone Number Mask. A checkbox labeled 'Auto-registration Disabled on this Cisco Unified Communications Manager' is present. The 'Cisco Unified Communications Manager TCP Port Settings for this Server' section shows Ethernet Phone Port (2000) and MGCP Listen Port (2427). A note at the bottom states: '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—3-29'.

Complete these steps to enable autoregistration on a specific Cisco Unified Communications Manager server: (This server has to be a member of the Cisco Unified Communications Manager group that is configured for autoregistration.)

- Step 1** From Cisco Unified Communications Manager Administration, choose **System > Cisco Unified Communications Manager**.
- Step 2** Click **Find** and choose the server that should be configured for autoregistration.
- Step 3** Under the Auto-Registration Information section, enter the appropriate directory number range in the Starting Directory Number and Ending Directory Number fields.
- Step 4** Ensure that the Auto-Registration Disabled on this Cisco Unified Communications Manager check box is unchecked.
- Step 5** Click **Save**.

Note	Specifying a valid range of directory numbers in the Starting Directory Number and Ending Directory Number fields automatically clears the Auto-Registration Disabled check box.
-------------	--

Cisco Unified Communications Manager BAT and Auto-Register Phone Tool

This topic describes how you can add IP phones with Cisco Unified Communications Manager BAT and Cisco Unified Communications Manager Auto-Register Phone Tool.

Using Cisco Unified Communications Manager BAT To Add IP Phones

Cisco Unified Communications Manager BAT allows for bulk update, add, or delete of records:

- Can also be used to add phones
- BAT file has to include MAC addresses of IP phones and directory numbers
- Alternative to manually putting MAC addresses into BAT files:
 - Use autoregistration to add phones (and their MAC addresses) automatically
 - Export phone records using Cisco Unified Communications Manager BAT
 - Edit directory numbers in exported files, replacing the directory numbers assigned with autoregistration by the desired directory numbers
 - Use edited file to bulk update phone directory numbers
- Both methods do not scale for large deployments

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-31

Cisco Unified Communications Manager BAT allows for bulk update, addition, or deletion of records, including the capability to add phone records to the configuration database.

When using Cisco Unified Communications Manager BAT to add phones, you must specify the MAC addresses of the IP phones along with the respective directory numbers in the BAT files.

Note	The MAC address is printed in text and Universal Product Code (UPC) form on both the shipping box of the IP phone and on the IP phone itself, which allows you to use bar code scanners rather than manually typing MAC addresses into BAT files.
-------------	---

Alternatively, you can use autoregistration first, so that Cisco Unified Communications Manager includes all phones with their MAC addresses and the directory numbers that were assigned by autoregistration. The administrator can then modify the directory numbers in the exported files by replacing the directory numbers that were assigned by autoregistration with those that are actually desired for the individual phones. These edited files can then be used by Cisco Unified Communications Manager BAT to update the phone records in the database.

However, both methods do not scale for large deployments.

Cisco Unified Communications Manager Auto-Register Phone Tool

This subtopic describes how the Cisco Unified Communications Manager Auto-Register Phone Tool allows phone additions in large deployments.

Cisco Unified Communications Manager Auto-Register Phone Tool

- A set of Cisco CRS scripts and application that has to be installed onto a Cisco CRS server
- Allows automated phone adds for large deployments
- Desired phones and their directory numbers are added with dummy MAC addresses using Cisco Unified Communications Manager BAT
- Autoregistration is enabled so that new phones can be used to call an IVR application, which *allows users to enter their directory number*
- Application updates phone with that directory number. Dummy MAC address is replaced by the address of the calling phone
- Scales to large deployments because:
 - MAC addresses are automatically added
 - MAC address-to-phone configuration association is done automatically based on user input

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-32

Cisco Unified Communications Manager Auto-Register Phone Tool is a set of Cisco CRS scripts and an application that has to be installed on a Cisco CRS server.

With Cisco Unified Communications Manager Auto-Register Phone Tool, new phones and their directory numbers are added with dummy MAC addresses (any arbitrary MAC addresses), so that you only have to specify those settings that cannot be automated. Usually Cisco Unified Communications Manager BAT is used for that purpose. After you add these phone records to Cisco Unified Communications Manager with Cisco Unified Communications Manager BAT, you must apply the appropriate MAC address to each individual phone record.

The process is automated by enabling autoregistration in order to enable newly added IP phones to place a call to an interactive voice response (IVR) application running on Cisco CRS. When a phone user calls into that application, the user is prompted to enter the desired directory number.

The system knows which of the prepared phone records (with dummy addresses) the calling phone is supposed to use—the record that has the entered directory number configured.

At this stage, the system knows all the required information: the MAC address of *this* phone as well as the phone configuration record to be applied to *this* phone. The Cisco Unified Communications Manager Auto-Register Phone Tool will now update the Cisco Unified Communications Manager configuration database by removing the phone record that was added by autoregistration (to free up the MAC address in the configuration database) and by changing the dummy MAC address of the desired phone record to the one of the phone.

As a result, MAC addresses were learned automatically and were automatically associated with the correct phone record (based on user input).

Cisco Unified Communications Manager Auto-Register Phone Tool Requirements

This subtopic lists the requirements for the Cisco Unified Communications Manager Auto-Register Phone Tool.

Cisco Unified Communications Manager Auto-Register Phone Tool Requirements

- Unified CM Auto-Register Phone Tool Services has to be activated in Unified CM.
- Unified CM Auto-Register Phone Tool has to be downloaded from Cisco Unified Communications Manager plug-in page and installed onto a Cisco CRS/Unified Contact Center 5.0 server.
- Unified CM Auto-Register Phone Tool installation prerequisites:
 - Ensure that the publisher for Unified CM is configured and running.
 - Ensure that the Cisco CRS server is configured.
- Optional Unified CM Auto-Register Phone Tool service parameters may be configured.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-33

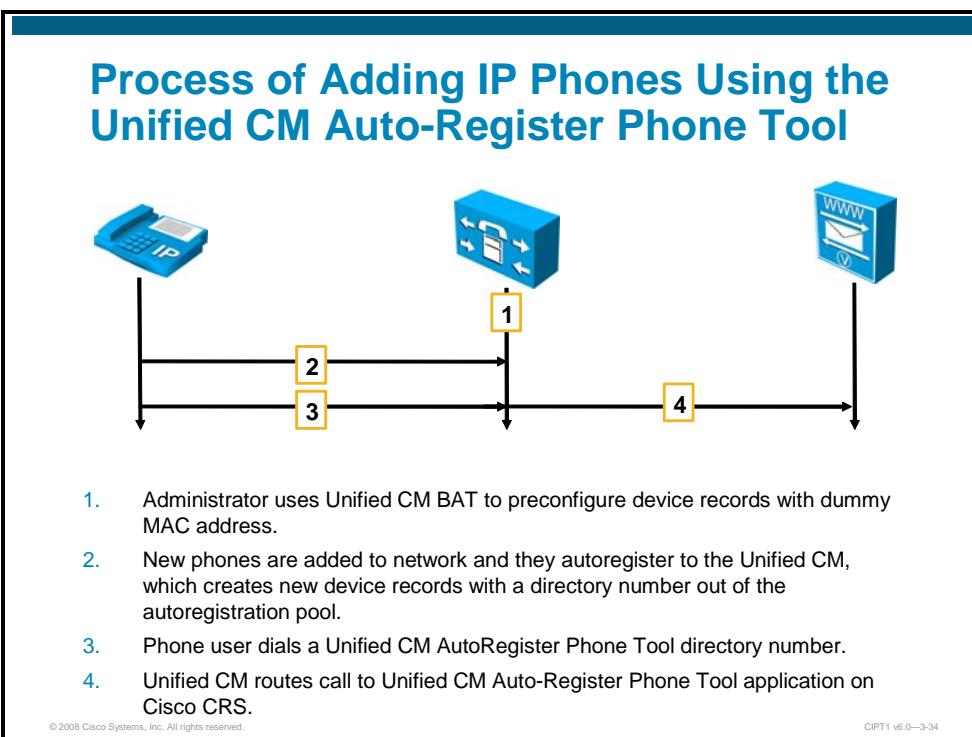
The requirements for the Cisco Unified Communications Manager Auto-Register Phone Tool are as follows:

- The Cisco Bulk Provisioning and Cisco Unified Communications Manager Auto-Register Phone Tool must be activated and running.
- The Cisco Unified Communications Manager Auto-Register Phone Tool has to be downloaded from the Cisco Unified Communications Manager plug-in page and installed onto a Cisco CRS server, for example, the Cisco Unified Contact Center.
- Installation prerequisites for the Cisco Unified Communications Manager Auto-Register Phone Tool are as follows:
 - The Cisco Unified Communications Manager publisher is running and integration with Cisco CRS is configured.
 - The Cisco CRS server is running and integration with Cisco Unified Communications Manager is configured.
- After installation of the Cisco Unified Communications Manager Auto-Register Phone Tool, you can configure optional parameters in Cisco CRS.

Note	Details for installation, configuration and integration of Cisco CRS server are not part of this course and are covered in the course UCXXD 2.0. For instance an AXL admin account needs to be configured for Cisco CRS so that it can access and update the Cisco Unified Communications Manager database. Additional information can also be found at Cisco.com.
-------------	--

Process of Adding IP Phones Using the Cisco Unified Communications Manager Auto-Register Phone Tool

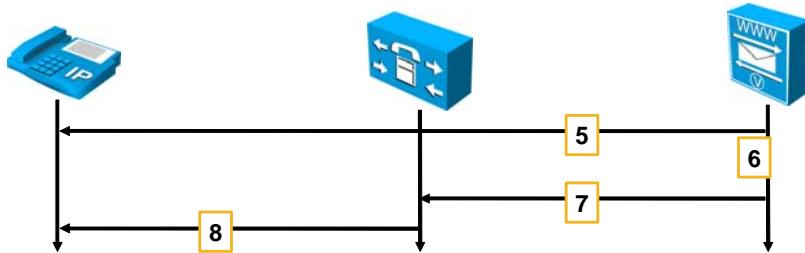
The figure illustrates the process of adding IP phones when using the Cisco Unified Communications Manager Auto-Register Phone Tool.



Follow these steps to add an IP phone using the Cisco Unified Communications Manager Auto-Register Phone Tool:

- Step 1** Use Cisco Unified Communications Manager BAT to preconfigure phone device records with dummy MAC addresses.
- Step 2** A new phone is plugged into the network. It autoregisters to Cisco Unified Communications Manager, which creates a new device record with a directory number from the autoregistration range.
- Step 3** The phone user dials the number of the Cisco Unified Communications Manager Auto-Register Phone Tool CRS application.
- Step 4** Cisco Unified Communications Manager routes the call to Cisco Unified Communications Manager Auto-Register Phone Tool applications on Cisco CRS.

Process of Adding IP Phones Using the Unified CM Auto-Register Phone Tool (Cont.)



5. Cisco CRS prompts user to enter the directory number to be associated with the IP phone and looks up the phone record with that directory number.
6. Cisco CRS updates the dummy MAC address of the found phone record with the MAC address of the actual device.
7. Phone downloads new config from Unified CM/TFTP.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-35

- Step 5** Cisco CRS prompts you to enter a directory number. The number is looked up in the phone configuration records that were previously added using Cisco Unified Communications Manager BAT and which have a dummy MAC address.
- Step 6** Cisco CRS updates the dummy MAC address of the found phone record with the actual MAC address of the phone in the Cisco Unified Communications Manager configuration database.
- Step 7** The IP phone downloads its newly created configuration file from Cisco Unified Communications Manager /TFTP.

Using Cisco Unified Communications Manager BAT for Adding Phones to Cisco Unified Communications Manager

This topic describes the procedure of using Cisco Unified Communications Manager BAT to add phones to Cisco Unified Communications Manager.

Cisco Unified Communications Manager BAT Configuration Procedure

The Cisco Unified Communications Manager BAT configuration process includes these steps:

1. Verify that the Bulk Provisioning Services have been activated.
2. Configure Cisco Unified Communications Manager BAT template.
3. Create the CSV data input file.
4. Validate the data input files.
5. Insert the devices into the Cisco Unified Communications Manager database.

© 2008 Cisco Systems, Inc. All rights reserved.

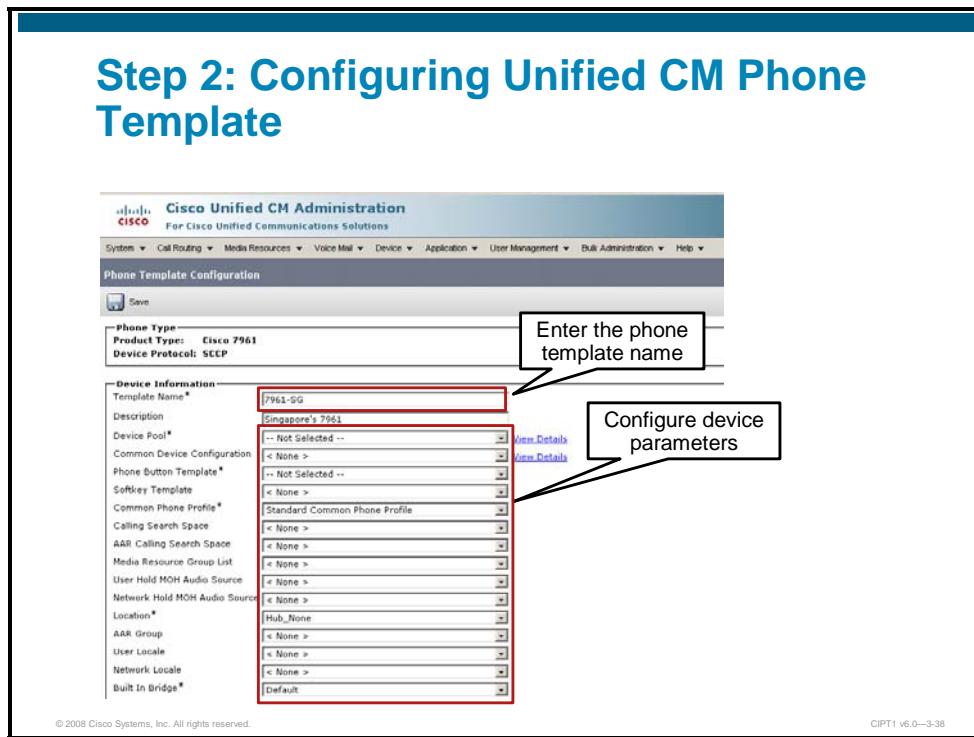
CIPT1 v6.0—3-37

The following procedure for using Cisco Unified Communications Manager BAT to add phones to Cisco Unified Communications Manager is similar to the procedure for using Cisco Unified Communications Manager BAT for adding users:

- Step 1** Verify that the Bulk Provisioning Services have been activated.
- Step 2** Configure the Cisco Unified Communications Manager BAT template.
- Step 3** Create the comma-separated values (CSV) data input file.
- Step 4** Validate the data input file.
- Step 5** Insert the devices into the Cisco Unified Communications Manager database.

Step 2: Configuring Cisco Unified Communications Manager Phone Template

The figure shows an example of configuring a phone template using Cisco Unified Communications Manager BAT.



A template name must be assigned and mandatory device parameters must be configured. Only the common parameters, shared by all phones, are configured through the templates. Individual parameters are entered to the CSV data file.

Prior to creating the template, you should ensure that phone settings such as device pool, location, calling search space, button template, and softkey templates have already been configured in Cisco Unified Communications Manager Administration. These settings cannot be created by Cisco Unified Communications Manager BAT.

Use the following procedure to create a phone template:

- Step 1** Choose **Bulk Administration > Phones > Phone Template** in the menu. The Find and List Phone Templates window displays.
- Step 2** Click the **Add New** button. The Add a New Phone Template window displays.
- Step 3** From the Phone Type drop-down list box, choose the phone model for which the template is to be created. Click **Next**.
- Step 4** Choose the device protocol from the Select the Device Protocol drop-down list box. Click **Next**. The Phone Template Configuration window displays with fields and default entries for the chosen device type.
- Step 5** In the Template Name field, enter a name for the template. The name can contain up to 50 alphanumeric characters (for example: Sales_7960).
- Step 6** In the Device Information area, enter the phone settings that the phones to be added have in common. Some phone models and device types do not use all the attributes which are shown.

- Step 7** After all the settings for this Cisco Unified Communications Manager BAT phone template have been entered, click **Save**.
- Step 8** When the status indicates that the changes are saved, you can add line attributes.
- Step 9** Find the Line Template to add lines to.
- Step 10** In the Line Template Configuration window, click **Line [1] Add a new DN** in the Associated Information area. The Line Template Configuration window displays.

Step 2: Configuring Unified CM Line Template (Cont.)

The screenshot shows the Cisco Unified CM Administration interface for 'Line Template Configuration'. The 'Status' section indicates 'Status: Ready'. The 'Directory Number Information' section has a red box around the 'Line Template Name*' field, which contains '< None >'. A callout box points to this field with the text 'Enter the line template name'. Below it, the 'Route Partition' dropdown also contains '< None >'. The 'Description' and 'Alerting Name' fields are empty. The 'ASCII Alerting Name' field is also empty. The 'Active' checkbox is checked. The 'Directory Number Settings' section contains several dropdown menus for 'Voice Mail Profile', 'Calling Search Space', 'Presence Group*', 'User Hold MOH Audio Source', 'Network Hold MOH Audio Source', and 'Auto Answer*'. A red box surrounds this entire settings group, and a callout box points to it with the text 'Configure line parameters'. At the bottom, there are tabs for 'AAR', 'Voice Mail', and 'AAR Destination Mask', with 'Voice Mail' currently selected.

Now, the next step of the configuration procedure is performed: the line template configuration.

The phone button template that was selected in the previous step determines the number of lines that the administrator can configure in the line template. The administrator can create a master phone template that has multiple lines. Then, the administrator can use the master template to add phones with a single line or up to the number of lines in the master template.

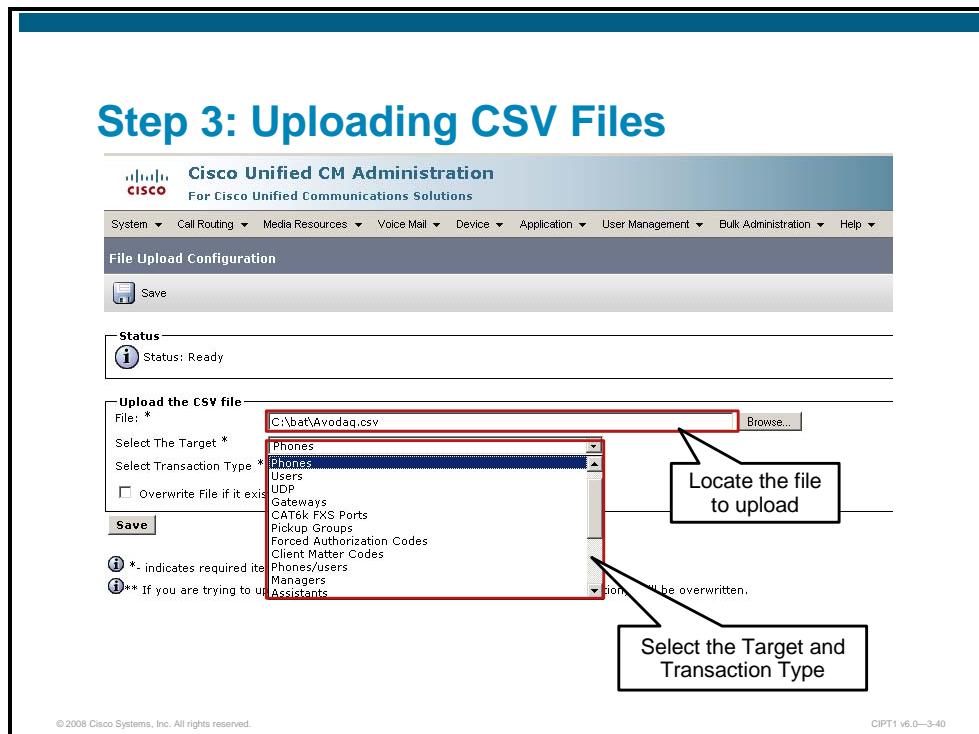
After the administrator clicks **Line [1] Add a new DN**, the Line Template Configuration window appears and must be configured in the following way:

- Step 1** Enter or choose the appropriate values for the line settings, such as Partition, Calling Search Space, Presence, and others. Keep in mind that all phones added by this Cisco BAT job will use the settings that are chosen for this line.
- Step 2** Click **Save**. Cisco Unified Communications Manager BAT adds the line to the phone template configuration.
- Step 3** Repeat the described procedure to add settings for any additional lines.

Note The maximum number of lines that display for a Cisco Unified Communications Manager BAT template depends on model and button template that the administrator chose when the administrator created the Cisco Unified Communications Manager BAT phone template.

Step 3: Uploading CSV Files

This section describes how to upload a data input file containing the individual phone configuration settings.



Use the following procedure to upload the CSV file containing the device data to the Cisco Unified Communications Manager server:

- Step 1** Choose **Bulk Administration > Upload/Download Files**. The Find and List Files window displays.
- Step 2** Click **Add New**. The File Upload Configuration window displays.
- Step 3** In the File text box, enter the full path of the file to be uploaded, or click **Browse** and locate the file.
- Step 4** From the Select the Target drop-down list box, choose the target that the file is to be used for (phones, in this case).
- Step 5** From the Transaction Type drop-down list box, choose the transaction type for the file.
- Step 6** If the file is to overwrite an existing file with the same name, check the **Overwrite File if it Exists** check box.
- Step 7** Click **Save** and wait for updated status information. The status should be Successful.

Step 4: Validating Phones Configuration

The next step is to validate the data input file.

The screenshot shows the 'Cisco Unified CM Administration' interface with the title 'Step 4: Validating Phones Configuration'. The main section is titled 'Validate Phones Configuration'. It includes a 'Status' box showing 'Status: Ready' with an information icon. Below it are two radio button options: 'Validate Phones Specific Details' (selected) and 'Validate Phones All Details'. Under 'Validate Phones Specific Details', there is a 'File Name' dropdown set to 'Not Selected' with a '(View File)' link. Under 'Validate Phones All Details', there is a 'File Name' dropdown set to 'Avodag.csv'. A callout box points to the 'File Name' dropdowns with the text 'Select the file to validate'. To the right of the dropdowns is a 'Phone Template Name' dropdown set to '7961-SG'. A callout box points to this dropdown with the text 'Select the template to be used'. At the bottom left is a red-bordered 'Submit' button, and at the bottom center is a blue-bordered 'Start Validation' button. A callout box points to the 'Start Validation' button with the text 'Validate all details'.

When performing this step, the system runs a validation routine to check that the CSV data file and Cisco Unified Communications Manager BAT phone template have populated all required fields, such as device pool and locations. The validation also checks for discrepancies with the first node database (for instance, an already existing entry with the same MAC address).

To validate the CSV data file phone records, use the following procedure:

- Step 1** Choose **Bulk Administration > Phones > Validate Phones**. The Validate Phones Configuration window displays.
- Step 2** Click either the **Validate Phones Specific Details** radio button to validate phone records that use a customized file format, or **Validate Phones All Details** radio button to validate phone records from an exported phones file that was generated by using the All Details option.
- Step 3** In the File Name drop-down list box, choose the CSV data file that contains the unique details for the phones or other IP telephony devices. This is the file that was uploaded previously.
- Step 4** For the Specific Details option, in the Phone Template Name drop-down list box, the administrator can choose the Cisco Unified Communications Manager BAT phone template that was created for this type of bulk transaction.
- Step 5** To start the verification, click **Submit**.
- Step 6** The job gets submitted and executed immediately.
- Step 7** Check for the status of the verification. Only proceed to the next step if the verification was successful.

Step 5: Inserting IP Phones into Cisco Unified Communications Manager Database

The final step is to submit the BAT job for adding the phones to the Cisco Unified Communications Manager database.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-42

To start the bulk add of the phones listed in the uploaded and verified data file, perform the following steps:

- Step 1** Choose **Bulk Administration > Phones > Insert Phones**. The Phone Insert Configuration window displays.
- Step 2** Click either the **Insert Phones Specific Details** radio button to insert phone records that use a customized file format, or the **Insert Phones All Details** radio button to insert phone records from an exported phones file that was generated by using the All Details option.
- Step 3** In the File Name drop-down list box, the administrator can choose the CSV data file that was created for this specific bulk transaction. Check the Allow Update Phone with Custom File check box to allow updating the phone with the custom file that the administrator chose.
- Step 4** Checking the **Override Configuration Settings** check box overwrites the existing phone settings with the information that is contained in the file that is to be inserted. For the Specific Details option, in the Phone Template Name drop-down list box, choose the BAT phone template that was created for this type of bulk transaction. If an individual MAC address is not entered in the CSV data file, the Create Dummy MAC Address check box must be selected. This is used when the Cisco Unified Communications Manager Auto-Register Phone Tool is used.
- Step 5** In the Job Information area, enter the job description.
- Step 6** Click the **Run Immediately** radio button to insert the phone records immediately, or click **Run Later** to schedule the job for a later time.

- Step 7** Click **Submit** to submit the job for inserting the phone records.
- Step 8** Check for the status of the job. This can be done at any time by browsing to **Bulk Administration > Job Scheduler** and clicking on the appropriate BAT job.

Manually Adding Phones to Cisco Unified Communications Manager

This topic describes how to manually add phones to Cisco Unified Communications Manager.

Cisco IP Phone Configuration Procedure

1. Add the IP phone.
2. Configure phone settings.
3. Add directory number(s).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-44

Manually adding new IP phones to the network is often tedious, but it can constitute a large part of day-to-day voice network management. Provisioning a Cisco SIP phone is just like provisioning an SCCP phone.

The configuration procedure consists of these high-level steps:

- Step 1** Add the IP phone.
- Step 2** Configure the phone.
- Step 3** Configure one or more directory numbers.

Step 1: Adding an IP Phone

The figure illustrates an example of the first step, adding the IP phone.

The screenshot shows the Cisco Unified CM Administration interface. The title bar reads "Cisco Unified CM Administration" and "For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Voice Mail", "Device", "Application", "User Management", "Bulk Administration", and "Help". The current page is "Phone Configuration". The main content area has a heading "Step 1: Adding the IP Phone". It displays a form with the following fields:

- Status: Ready
- Select the type of phone you would like to create:
 - Product Type: Cisco 7960
 - Select the device protocol:
 - SCCP
 - SIP
- A "Next" button at the bottom left.

At the bottom of the page, there is a copyright notice: "© 2008 Cisco Systems, Inc. All rights reserved." and a reference: "CIPT1 v6.0—3-45".

In order to manually add an IP phone to Cisco Unified Communications Manager, go to **Device > Add Phone** and choose the phone type (in the example, a Cisco 7960 IP phone was selected). Then choose the protocol that should be used with the Cisco IP phone (SCCP or SIP), and click **Next** to go to the Phone Configuration page.

Step 2: Phone Configuration

The figure shows the Phone Configuration page, where you configure the parameters for the phone that is to be added.

The screenshot displays the Cisco Unified CM Administration interface. At the top, the title 'Step 2: Phone Configuration' is shown in blue. Below it, the main window is titled 'Cisco Unified CM Administration' with the sub-header 'For Cisco Unified Communications Solutions'. The navigation bar includes links for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The current page is 'Phone Configuration'. A toolbar at the top of the configuration area includes a 'Save' button. The configuration form is titled 'Device Information' and contains the following fields:

MAC Address*	BADB07BACD07
Description	SEPBADB07BACD07
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	Standard 7960 SCCP
SoftKey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAA Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
AAA Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	Default
Privacy*	< None >
Device Mobility Mode*	Default
Owner User ID	Person

Below the configuration form, a note states: '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—3-46'. To the right of the configuration form, a list of 'Required parameters' is provided, followed by a note about default values.

Required parameters:

- MAC Address
- (Device Pool)
- (Phone Button Template)
- (Common Phone Profile)
- (Location)
- (Built-In Bridge)
- (Privacy)
- (Device Mobility Mode)
- Device Security Profile

() = parameters with default values

Each phone in the Cisco Unified Communications Manager configuration database is uniquely identified by a device ID which is built from its MAC address. The MAC address of a Cisco IP phone is printed on a label at the back of the IP phone and can be viewed at the phone itself by pressing the Settings button.

In addition to the MAC address, the following mandatory parameters have to be set:

- MAC Address
- Device Pool
- Phone Button Template
- Common Phone Profile
- Location
- Built-In Bridge
- Privacy
- Device Mobility Mode
- Device Security Profile

Note Not all of these mandatory parameters have to be configured because some of them have default values. Only those that do not have defaults must be configured before the phone can be actually added into the configuration database.

Step 3: Directory Number Configuration

The figure shows the configuration of a directory number to be used by the newly added IP phone.

The screenshot shows the 'Cisco Unified CM Administration' interface with the title 'Step 3: Directory Number Configuration'. The main window is titled 'Directory Number Configuration'. It contains several sections: 'Status' (Status: Ready), 'Directory Number Information' (Directory Number: 23112, Route Partition: <None>, Description: [empty], Alerting Name: [empty], ASCII Alerting Name: [empty], Active checked), 'Directory Number Settings' (Voice Mail Profile: <None>, Calling Search Space: <None>, Presence Group: Standard Presence group, User Hold MOH Audio Source: <None>, Network Hold MOH Audio Source: <None>, Auto Answer: Auto Answer Off), and 'AAR Settings' (AAR: [empty], Voice Mail: [empty], AAR Destination Mask: [empty], Retain this destination in the call forwarding history checked). A note on the right says '() = parameters with default values'. At the bottom, there are copyright and version information: © 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-47.

Required parameters:

- Directory Number
- Presence Group
- Auto Answer
- Visual Message Waiting Indicator Policy
- Ring Setting (Phone Idle)
- Maximum Number of Calls
- Busy Trigger

() = parameters with default values

Follow this procedure to configure a directory number for the manually added IP phone:

- Step 1** At the Phone Configuration window in the left Associated Information column, click on the **Line [x] – Add a new DN** link to configure the first line with a directory number.
- Step 2** When the Directory Number Configuration window appears, enter the directory number of the IP phone in the appropriate field.
- Step 3** Click **Save**.

Note Use the same procedure to configure additional lines if the phone has more than one line.

Verify Endpoint Configuration

After manually adding an IP phone, you can verify the configuration in several ways.

Verify Endpoint Configuration

To verify that the phone configuration is done successfully, do the following:

- Verify that the phone is registered.
- Verify that the correct Cisco Unified Communications Manager is used.
- Verify the IP address of the phone.
- Verify that the lines are associated to the correct phone(s).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-48

To verify phone configuration, do the following:

- Verify the IP address of the IP phone.
- Verify that the IP phone registers with Cisco Unified Communications Manager.
- Verify that the IP phone uses the correct Cisco Unified Communications Manager server.

Note All of the above can be checked at the phone itself by pressing the **Settings** button and navigating to the IP network configuration, or at Cisco Unified Communications Manager by checking the IP phone status in the search list.

- Verifying that the correct directory numbers are assigned to the IP phone lines.

Note The easiest way to verify the directory numbers of a phone is to check at the phone itself or view the phone configuration in Cisco Unified Communications Manager.

Verify Endpoint Configuration (Cont.)

The screenshot shows the Cisco Unified CM Administration interface. The title bar reads "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The menu bar includes "System", "Call Routing", "Media Resources", "Voice Mail", "Device", "Application", "User Management", "Bulk Administration", and "Help". Below the menu is a toolbar with buttons for "Add New", "Select All", "Clear All", "Delete Selected", and "Reset Selected". A status bar at the bottom left says "© 2008 Cisco Systems, Inc. All rights reserved." and "CIPT1 v6.0—3-49". The main content area is titled "Phone (1 - 7 of 7)". It contains a search bar with "Find Phone where Device Name begins with" and a search button. Below is a table with columns: Device Name (Line), Description, Device Pool, Device Protocol, Status, and IP Address. The table lists seven entries:

Device Name (Line)	Description	Device Pool	Device Protocol	Status	IP Address
CTPH_1001	Unified CM Telephony Group #543-1	Default	SCCP	Unregistered	192.168.0.168
CTPH_1002	Unified CM Telephony Group #543-1	Default	SCCP	Unregistered	192.168.0.168
CTPH_1003	Unified CM Telephony Group #543-1	Default	SCCP	Unregistered	192.168.0.168
CTPH_1004	Unified CM Telephony Group #543-1	Default	SCCP	Unregistered	192.168.0.168
CTPH_1005	Unified CM Telephony Group #543-1	Default	SCCP	Unregistered	192.168.0.168
SEPBACB07BAC001	Auto 1000	Default	SCCP	Unregistered	192.168.0.1
SEPBACB07BAC002	SEPBACB07BAC002	Default	SCCP	Unknown	Unknown

At the bottom are buttons for "Add New", "Select All", "Clear All", "Delete Selected", and "Reset Selected".

The figure shows an example of a phone listing (after performing a Find and List Phones procedure from **Device > Phone**). Successful phone configuration can be verified by checking the following items:

- Look at the Status column and verify that the phone is registered.

Note If it is shown as unregistered, it means that the phone has previously registered but is no longer registered. If a phone has been reset, it may be shown as unregistered during the short time until it reregisters with Cisco Unified Communications Manager. If it is shown as unknown, it means that the phone has never successfully registered to the Cisco Unified Communications Manager. If the phone is registered, its IP address will be shown in the Status column.

-
- Look at the IP Address column to verify that the IP phone is registered to the intended Cisco Unified Communications Manager server.

Note If all Cisco Unified Communications Manager servers are up and running, the IP phone should register with the primary server of the IP phone Cisco Unified Communications Manager Group. The Cisco Unified Communications Manager server that the phone registered with is shown by its IP address.

Tip By clicking the device name of a specific phone of the list, the phone configuration page of the corresponding phone is shown. You can then verify line configuration (directory numbers) and other parameters that are not shown on the Find and List phone result page.

Third-Party SIP Phone Configuration Steps

The figure lists the procedure for adding and configuring a third-party SIP phone to Cisco Unified Communications Manager.

Third-Party SIP Phone Configuration Procedure

1. Configure the end user in Cisco Unified Communications Manager.
2. Configure the device in Cisco Unified Communications Manager.
3. Associate the device to the end user.
4. Configure the third-party SIP phone.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-50

The high-level steps for adding a third-party SIP phone are as follows:

- Step 1** Configure the end user in Cisco Unified Communications Manager.
- Step 2** Configure the device in Cisco Unified Communications Manager.
- Step 3** Associate the device to the end user.
- Step 4** Configure the third-party SIP phone to register with Cisco Unified Communications Manager.

Steps 1 to 3: Third-Party SIP Phone Configuration in Cisco Unified Communications Manager

This subtopic describes the steps that are performed in Cisco Unified Communications Manager when you add third-party SIP phones.

Steps 1 to 3: Third-Party SIP Phone Configuration in Unified CM

Step 1: Configure the end user.

Step 2: Add and configure the third-party SIP phone.

Step 3: Select the end user ID in Digest User drop-down list in Phone Configuration.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-51

The steps that are performed in Cisco Unified Communications Manager when you add third-party SIP phones are as follows:

- Step 1** Add an end user in Cisco Unified Communications Manager Administration.
- Step 2** Add the third-party SIP phone:
- When adding a third-party SIP phone, you must specify the type of the phone, basic or advanced.

Note Basic third-party SIP phones support only a single line.

- Configure any dummy MAC address for the third-party phone.
- Verify other phone configuration parameters and change them, if required.
- Configure the lines with directory numbers.

Note Any MAC address that has not been configured with another phone can be configured because third-party SIP phones do not register by MAC address.

- Step 3** In the Protocol Specific Information pane of the Phone Configuration window, choose the end user that was configured in Step 1 from the Digest User drop-down list.

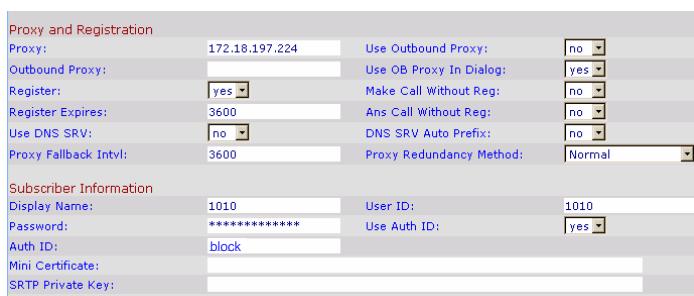
Step 4: Third-Party SIP Phone Configuration

This subtopic describes how to configure a third-party SIP phone to register with Cisco Unified Communications Manager.

Step 4: Third-Party SIP Phone Configuration

The configuration at the third-party SIP phone depends on the third-party product used. The example shows the configuration of a Linksys SPA 942 phone.

The proxy address should be the Cisco Unified Communications Manager IP address or name.



The screenshot shows the configuration interface for a Linksys SPA 942. On the left, a note says "The proxy address should be the Cisco Unified Communications Manager IP address or name." An arrow points from this note to the "Proxy" field in the configuration interface. The configuration interface has two main sections: "Proxy and Registration" and "Subscriber Information". In the "Proxy and Registration" section, the "Proxy" field is set to "172.18.197.224". In the "Subscriber Information" section, the "Display Name" and "User ID" fields are both set to "1010", and the "Auth ID" field is set to "block".

The Auth ID has to match the end user name in Cisco Unified Communications Manager. The User ID has to match the directory number.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—3-52

The final step to add a third-party phone takes place on the third-party phone itself. Therefore, the configuration depends on the product that is used. The example shows the configuration of a Linksys SPA 942 third-party SIP phone.

In the proxy address field of the third-party phone, specify the IP address or fully qualified domain name of Cisco Unified Communications Manager.

The User ID has to be set to the directory number that is assigned to the IP phone in Cisco Unified Communications Manager. The Auth ID has to match the Digest User that was assigned to the phone in Step 3 of Cisco Unified Communications Manager configuration. The password only needs to be set, if the Digest Credentials have been configured in Step 1 when configuring the end user and if the check box Enable Digest Authentication has been activated in the phone security profile.

Note	If the Enable Digest Authentication check box is not activated in the phone security profile, only the username of the digest authentication is verified, but the password (Digest Credentials in Cisco Unified Communications Manager end user configuration) is not checked.
-------------	--

Some third-party SIP phones do not have a separate User ID and Auth ID. In this case, the user ID has to be set to the directory number at the third-party SIP phone, and on the Cisco Unified Communications Manager side, the end user name has to be identical with the directory number of the IP phone. The Linksys phone shown simulates that behavior when the Use Auth ID parameter is set to “No”.

Hardening Cisco IP Phones

This topic describes Cisco IP phone configuration settings that can be used to harden the IP phone.

Phone Hardening Options in Cisco Unified Communications Manager

- PC port
- Settings access
- GARP
- PC voice VLAN access
- Web access

Product Specific Configuration

<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Enabled
Settings Access *	Enabled
Gratuitous ARP *	Enabled
PC Voice VLAN Access *	Enabled
Video Capabilities *	Disabled
Auto Line Select *	Disabled
Web Access *	Enabled

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-54

The IP phone is a target for attacks just like all other components of the network. Often, endpoints, such as IP phones, are not protected—only servers and network infrastructure devices are hardened. This is not a good practice because IP phones have default settings that make them vulnerable to certain attacks. However, there are several options available to harden IP phones and thus protect them against various attack and infiltration methods.

The product-specific configuration parameters of Cisco IP phones are set by default to achieve the greatest functionality but are considered insecure. To secure Cisco IP phones, these settings can be modified:

- **Disable Speakerphone and Disable Speakerphone and Headset:** Disable these features to prevent eavesdropping on conversations in the office by an attacker gaining remote control of the IP phone.
- **PC Port:** Disable the PC port to prevent a PC from connecting to the corporate network via the IP phone PC port.
- **Settings Access:** Disable or restrict access to the IP phone settings to avoid the risk that details about the network infrastructure could be exposed.
- **Gratuitous ARP:** Disable this feature to prevent Gratuitous Address Resolution Protocol (GARP)-based man-in-the-middle attacks.
- **PC Voice VLAN Access:** Disable this feature to stop the IP phone from forwarding voice VLAN traffic to the PC.
- **Web Access:** Disable access to the IP phone from a web browser to avoid the risk that details about the network infrastructure could be exposed.

Disabling PC Port and Settings Access

This subtopic describes reasons to disable the PC port and limit settings access to the IP phone.

Disabling PC Port and Settings Access

- Disable the PC port:
 - Stops attackers from accessing the network through a publicly accessible phone (e.g. lobby phone).
- Disable settings access:
 - Disabled option deactivates the settings button completely.
 - Restricted option grants access to contrast and ringer menu only.
 - Stops attackers from learning your network configuration.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-55

The PC port should be disabled in special areas such as a lobby or area where no additional PC access is allowed. This practice is not common, however, because it entails a major functionality constraint.

Disabling access to settings prevents users (or attackers having physical access to the phone) from gathering information about, for example, DHCP server, TFTP server, default router, and Cisco Unified Communications Manager IP addresses. Knowing such details about the network allows an attacker to place more specific attacks. Cisco Unified Communications Manager Release 4.1 and later releases offer the Restricted option for settings access. With restricted access, the user can modify the contrast and ringer settings but cannot access any other settings.

Disabling IP Phone Web Service

This subtopic describes the reasons for disabling the IP phone web service and for *not* disabling the IP phone built-in web server.

Disabling IP Phone Web Service

- Information provided by the IP phone web service is similar to information provided by the Settings button.
- Discloses information about network infrastructure.
- Disabling web access stops attackers from learning your network configuration from a web browser.

Device Information	MAC Address	000F24A978A7
Network Configuration	Host Name	SEP000F24A978A7
Network Statistics	Phone DN	2017
Ethernet	App Load ID	P00307000200
Port 1 (Network)	Boot Load ID	PC0303010001
Port 2 (Access)	Version	7.0(2.0)
Port 3 (Phone)	Expansion Module 1	
Device Logs	Expansion Module 2	
Debug Display	Hardware Revision	4.2
Stack Statistics	Serial Number	INM08061F9J
Status Messages	Model Number	CP-7940G
Streaming Statistics	Codec	ADLCodec
Stream 1	Amps	5V Amp
	C3PO Revision	2
	Message Waiting	NO

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-56

A web browser can be used to connect to the HTTP server of the IP phone by simply browsing to the IP address of the phone. The HTTP server displays similar information that can be viewed directly on the IP phone using the Settings button, enhanced by some additional statistics.

An attacker can use intelligence gained by discovering the network configuration to direct attacks at the most critical telephony components, such as Cisco Unified Communications Manager and the TFTP server. Therefore, from a security perspective, it is recommended that you disable web access to the phone.

When web access is disabled, the IP phone will not accept incoming web connections and therefore does not provide access to sensitive information.

Note	Disabling web access at the IP phone stops Extensible Markup Language (XML) push applications from working. If you want to use XML push applications on some IP phones (for instance, for an emergency notification application), you cannot disable web access to the IP phone.
-------------	--

Disabling GARP

This section describes why GARP should be disabled on Cisco IP phones.

Disabling GARP

- Usually ARP operates in request-response fashion.
- Learned MAC addresses are added to a local ARP cache.
- GARP packets are ARP packets that have not been requested:
 - Sent by a station that announces its own MAC address.
 - Allow update of ARP caches in receiving devices.
 - Usually sent after MAC address changes.
 - **Can be misused for packet redirection in a man-in-the-middle attack.**

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-57

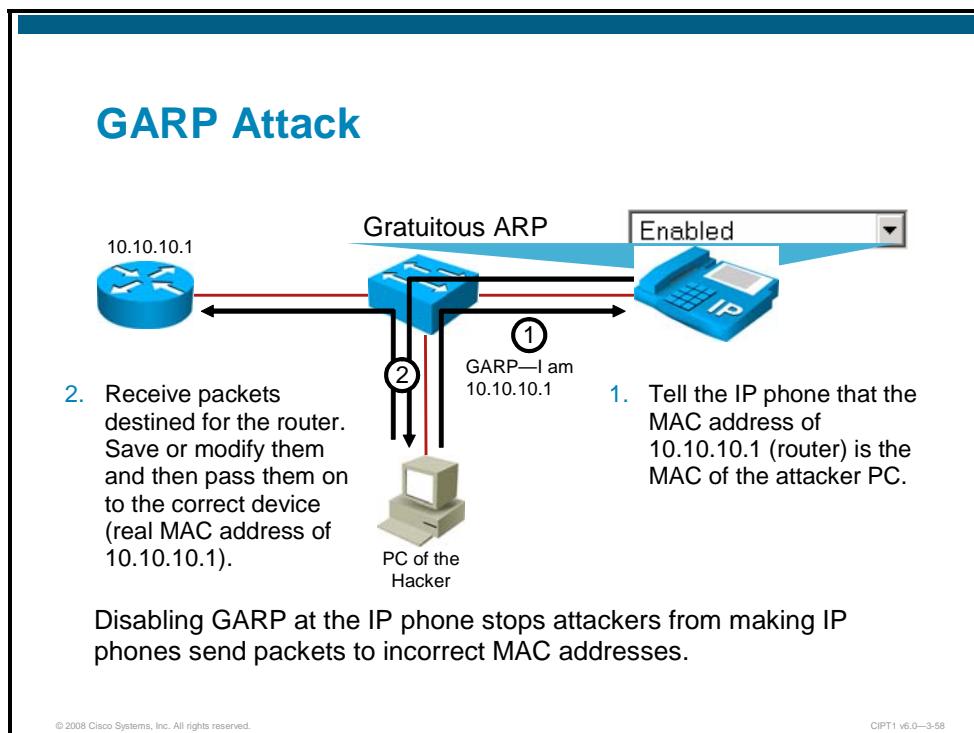
Usually Address Resolution Protocol (ARP) operates in a request-and-response fashion. When a station needs to know the MAC address of a given IP address, it sends an ARP request. The device with the corresponding IP address replies and thus provides its MAC address. All receiving devices update their ARP cache by adding the IP and MAC address pair.

GARP packets are packets that announce the MAC address of the sender even though this information has not been requested. This technique allows receiving devices to update their ARP caches with the information. Usually GARP messages are sent after the MAC address of a device has changed, to avoid packets being sent to the old MAC address, until the related entry has timed out in the ARP caches of the other devices.

GARP, however, can also be used by an attacker to redirect packets in a man-in-the-middle attack and therefore should be disabled.

GARP Attack

The figure illustrates a GARP attack against an IP phone.



Cisco IP phones, by default, accept GARP messages and update their ARP cache whenever they receive a GARP packet.

An attacker located in the VLAN of the IP phone can repeatedly send out GARP packets announcing its MAC address to be the MAC address of the default gateway of the IP phone. The IP phone accepts the information, updates its ARP cache, and forwards all packets meant for the default gateway to the attacker. With tools such as ettercap, the attacker can copy or modify the information and then relay it to the real default gateway. The user does not notice that someone is listening to the data stream as long as the attacker does not significantly increase the delay and does not drop packets.

In this example, only traffic from the IP phone toward the default gateway is sent to the attacker, but if the attacker also impersonates the IP phone toward the router, the attacker could control bidirectional traffic. In this case, the router would also have to listen to GARP packets.

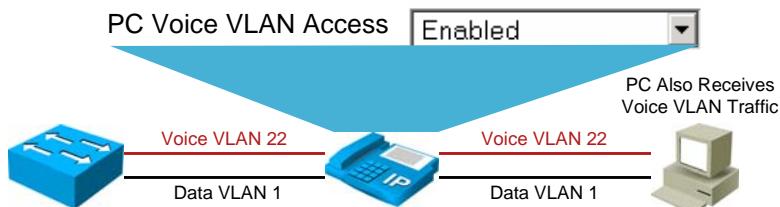
To prevent GARP-based attacks against an IP phone, the GARP feature of the IP phone should be disabled.

Note	There are several methods to prevent GARP attacks. You can disable GARP on end devices, or you can use features such as Dynamic ARP Inspection (DAI) and IP Source Guard at switches. You can find more information about DAI and IP Source Guard in your Cisco IOS Software or Cisco Catalyst operating system software switch configuration guide.
-------------	--

Disabling Voice VLAN Access

This subtopic describes the advantages of disabling voice VLAN access, and when the IP phone should not be blocked from accessing the voice VLAN.

Disabling Voice VLAN Access



By default, the IP phone forwards all frames it receives from the switch to the PC and vice versa:

- Includes voice VLAN traffic
- Includes all other VLANs allowed on the port (if configured as a trunk)
- Allows the PC to sniff phone conversations or other traffic
- Allows the PC to send data to voice and other VLANs

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-59

By default, an IP phone sends all traffic that it receives from the switch out its PC port. This enables the PC to see not only the traffic of the native VLAN (the data VLAN), but also to see the traffic of the voice VLAN. When the PC receives voice VLAN traffic, the traffic can be captured and the conversation can be sniffed.

Further, the PC can also send packets to the voice VLAN if they are tagged accordingly. This ability breaks the separation of voice VLANs and data VLANs, because the PC that is supposed to have access to the data VLAN is only able to send packets to the voice VLAN, bypassing all access-control rules (access control lists [ACLs] in routers or firewalls) that might be enforced between the two VLANs.

Note If the switch port is configured as a trunk, the above also applies to all other VLANs that are allowed on the trunk port in the switch configuration. Note that, by default, all VLANs are allowed on trunk ports.

Usually, the PC does not need access to the voice VLAN, and therefore you should block PC access to the voice VLAN.

Note Some applications, such as call recording or supervisory monitoring in call center applications, require access to the voice VLAN. In such situations, you cannot disable the PC Voice VLAN Access setting.

Blocking PC VLAN Access On Cisco IP Phones

This subtopic describes different ways to block the PC from accessing VLANs.

Blocking PC VLAN Access on Cisco IP Phones

There are two settings that can be used to block the PC from accessing VLANs:

- Disabling PC Voice VLAN Access:
 - The IP phone does not forward voice-VLAN tagged frames received from the switch to the PC and vice versa (voice VLAN traffic is blocked).
 - Setting is available on all phones with PC ports.
- Disabling Span to PC Port:
 - The IP phone does not forward any tagged frames received from the switch to the PC and vice versa (only untagged traffic is permitted).
 - Setting is not available on Cisco Unified IP Phone 7940 and 7960.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-60

Two different settings are available for blocking PC VLAN access:

- **PC Voice VLAN Access:** When this setting is disabled, a phone will not forward voice VLAN-tagged traffic to the PC when it receives such frames from the switch. In addition, the phone will not forward voice VLAN-tagged traffic to the switch if it receives such frames from the PC. Although disabling this setting is recommended for security, it makes troubleshooting more difficult because you cannot analyze voice VLAN traffic from a PC connected to the PC port of the IP phone. When you need to capture voice VLAN traffic to analyze network problems, you will have to sniff the traffic on the network devices.

This setting is supported on all current Cisco IP phones with PC ports.

- **Span to PC Port:** This setting has the same effect as the PC Voice VLAN Access setting, with the difference that it does not only apply to voice VLAN-tagged traffic but also to traffic tagged with any VLAN ID. With Span to PC Port disabled, the IP phone only forwards untagged frames.

This setting is not available on Cisco Unified IP Phones 7940 and 7960.

Note	The Cisco Unified IP Phone 7912, which is end-of-sale, does not support any of the two settings.
-------------	--

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Some IP configuration settings are applied directly to the device, others by referencing configuration elements such as a device pool.
- IP phone autoregistration automatically adds new Cisco IP phones to the configuration database and assigns one directory number to the IP phone.
- Autoregistration configuration includes the configuration of a directory number range and activation of the feature on some servers of a Cisco Unified CM Group.
- Cisco Unified Communications Manager Auto-Register Phone Tool requires a Cisco CRS server on the network.
- Cisco Unified Communications Manager BAT can be used to add and delete IP phones or to change their configuration.
- Manually adding IP phones is time-consuming.
- Harden IP phones by disabling features that are not required.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-61

References

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager Bulk Administration Guide 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/bat/6_0_1/bat-wrapper.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Working with the Cisco Unified Communications Manager Auto-Register Phone Tool
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/bat/6_0_1/t15taps.html

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- Cisco Unified Communications Manager supports a variety of endpoints, including Cisco IP phones and third-party phones. SCCP, SIP, and H.323 can be used as a signaling protocols to these endpoints.
- Cisco Catalyst switches are part of the Cisco Unified Communications solutions and provide endpoints with Power over Ethernet, voice VLAN separation, and Layer 2 QoS.
- Endpoints are configured differently based on protocol and vendor type (Cisco IP phones versus third-party endpoints). Mass endpoint implementation can be simplified using the Cisco Unified Communications Manager BAT or Cisco Unified Communications Manager Auto-Register Phone Tool.

© 2007 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—3-1

This module describes the endpoints supported by Cisco Unified Communications Manager. It explains the differences in the various Cisco IP phone models and third-party phones and how feature support depends on the protocol used. The module describes the LAN infrastructure that provides IP phones with electrical power and separate voice VLANs. The module describes how to implement different endpoints in Cisco Unified Communications Manager manually, using the Cisco Unified Communications Manager Bulk Administration Tool or the Cisco Unified Communications Manager Auto-Register Phone Tool.

References

For additional information, refer to these resources:

- Voice and Unified Communications – Compare Products and Solutions
http://www.cisco.com/en/US/products/sw/voicesw/products_category_buyers_guide.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Catalyst 3550 Multilayer Switch Software Configuration Guide, Rel. 12.2(25)SEE – Configuring Voice VLAN
http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3550/software/release/12.2_25_see/configuration/guide/swvoip.html

- Catalyst 3550 Multilayer Switch Software Configuration Guide, Rel. 12.2(25)SEE – Configuring CDP
http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3550/software/release/12.2_25_see/configuration/guide/swcdp.html
- Working with the Cisco Unified Communications Manager Auto-Register Phone Tool
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/bat/6_0_1/t15taps.html

Module Self-Check

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

- Q1) Which of the following endpoints is not supported by Cisco Unified Communications Manager? (Source: Understanding Endpoints in Cisco Unified Communications Manager)
- A) H.323 phones
 - B) third-party SIP phones
 - C) SCCP phones
 - D) Skype software client
- Q2) Which two of the following protocols provide the highest number of telephony features? (Choose two.) (Source: Understanding Endpoints in Cisco Unified Communications Manager)
- A) SIP (Cisco)
 - B) MGCP
 - C) SIP (Standard)
 - D) SCCP
 - E) H.323
- Q3) Which list of tasks best describes the boot process of a Cisco IP phone? (Source: Understanding Endpoints in Cisco Unified Communications Manager)
- A) configure voice VLAN, obtain power, load configuration file, obtain IP address
 - B) load configuration file, obtain power, obtain IP address, configure voice VLAN
 - C) obtain power, configure voice VLAN, obtain IP address, load configuration file
 - D) obtain power, load configuration file, configure voice VLAN, obtain IP address
- Q4) Which of the following endpoints are identified by their IP address? (Source: Understanding Endpoints in Cisco Unified Communications Manager)
- A) Cisco SIP
 - B) MGCP
 - C) third-party SIP
 - D) H.323
- Q5) Which two items of information are provided by a third-party SIP phone when registering with Cisco Unified Communications Manager? (Choose two.) (Source: Understanding Endpoints in Cisco Unified Communications Manager)
- A) directory number
 - B) MAC address
 - C) username
 - D) X.509 certificate

- Q6) Which two of the following Cisco LAN switch features are used by IP phones? (Choose two.) (Source: Configuring Cisco Catalyst Switches for Endpoints)
- A) VACL
 - B) PoE
 - C) EtherChannel
 - D) voice VLAN
 - E) RSPAN
- Q7) Which two power options, independent of the LAN switch, are supported by Cisco IP phones? (Choose two.) (Source: Configuring Cisco Catalyst Switches for Endpoints)
- A) Power over Ethernet
 - B) midspan power injection
 - C) wall power
 - D) Power over Wi-Fi
- Q8) Which command enables inline power on port 3 of module 2 of a Cisco Catalyst 6500 Series switch that is running Cisco Catalyst software? (Source: Configuring Cisco Catalyst Switches for Endpoints)
- A) **power inline** in global configuration mode
 - B) **power inline auto** in interface configuration mode
 - C) **set port inline power default**
 - D) **set port inline power 3/2 802.3af**
 - E) **set port inline power 2/3 auto**
- Q9) Which VLAN configuration option is *not* supported on Cisco LAN switch ports that connect to Cisco IP phones? (Source: Configuring Cisco Catalyst Switches for Endpoints)
- A) 802.1Q
 - B) 802.1p
 - C) 802.2
 - D) 802.3
- Q10) Which VLANs need to be accessible on a Cisco LAN switch port that is configured in trunk mode and connects to a Cisco IP phone with a PC attached? (Source: Configuring Cisco Catalyst Switches for Endpoints)
- A) data VLAN
 - B) voice VLAN
 - C) native VLAN
 - D) native and voice VLAN
 - E) all VLANs
 - F) no VLANs
- Q11) The command **switchport voice vlan _____** enables an IP phone to send frames with Layer 2 CoS settings on an access port. (Source: Configuring Cisco Catalyst Switches for Endpoints)
- A) **dot1p**
 - B) **802.3p**
 - C) **802.3q**
 - D) **(vlan ID)**

- Q12) Which two of the following commands are *not* used to configure a Cisco LAN switch running the Cisco Catalyst operating system for a multi-VLAN access port? (Choose two.) (Source: Configuring Cisco Catalyst Switches for Endpoints)
- A) **set port auxiliaryvlan 2/1-3 261**
 - B) **set native vlan 262 2/1-3**
 - C) **set trunk 2/1-3 off**
 - D) **set vlan 262 2/1-3**
 - E) **set trunk 261 2/1-3**
- Q13) Which two settings are not configurable at a device pool? (Choose two.) (Source: Implementing and Hardening IP Phones)
- A) Softkey Template
 - B) Media Resource Group List
 - C) Cisco Unified Communications Manager Group
 - D) Date/Time Group
 - E) Phone Button Template
 - F) Region
- Q14) Which two statements do not apply to the autoregistration feature? (Choose two.) (Source: Implementing and Hardening IP Phones)
- A) Each autoregistered phone is added twice: once with SIP and once with SCCP.
 - B) Only one directory number can be assigned per phone.
 - C) Autoregistration is enabled per Cisco Unified Communications Manager Group, but can be activated selectively on group members.
 - D) Autoregistration works for Cisco IP phones and third-party SIP phones.
- Q15) The autoregistration directory number range is configured at the _____. (Source: Implementing and Hardening IP Phones)
- A) device pool
 - B) Cisco Unified Communications Manager server
 - C) Cisco Unified Communications Manager
 - D) default device profile
- Q16) Which two of the following components and features are not used by the Cisco Unified Communications Manager Auto-Register Phone Tool? (Choose two.) (Source: Implementing and Hardening IP Phones)
- A) CRS
 - B) application plugins
 - C) autoregistration
 - D) Cisco Unified Communications Manager BAT
 - E) Cisco Unified Communications Manager Extension Mobility
- Q17) Which of the following is *not* a step in adding phones with the Cisco Unified Communications Manager Bulk Administration Tool? (Source: Implementing and Hardening IP Phones)
- A) Upload a phone template.
 - B) Start a Cisco Unified Communications Manager BAT job to add phones.
 - C) Configure a phone template.
 - D) Upload a CSV data input file.

- Q18) Which three of the following have to be specified when adding a phone manually?
(Choose three.) (Source: Implementing and Hardening IP Phones)
- A) phone model
 - B) protocol
 - C) region
 - D) MAC address
 - E) serial number
 - F) IP address
 - G) location
- Q19) Which of the following features is not used for phone hardening? (Source:
Implementing and Hardening IP Phones)
- A) disabling the PC port
 - B) disabling video capabilities
 - C) disabling GARP
 - D) disabling PC voice VLAN access
 - E) disabling web access

Module Self-Check Answer Key

- Q1) D
- Q2) A, D
- Q3) C
- Q4) D
- Q5) A, C
- Q6) B, D
- Q7) B, C
- Q8) E
- Q9) C
- Q10) D
- Q11) A
- Q12) B, E
- Q13) A, E
- Q14) A, D
- Q15) C
- Q16) B, E
- Q17) A
- Q18) A, B, D
- Q19) B