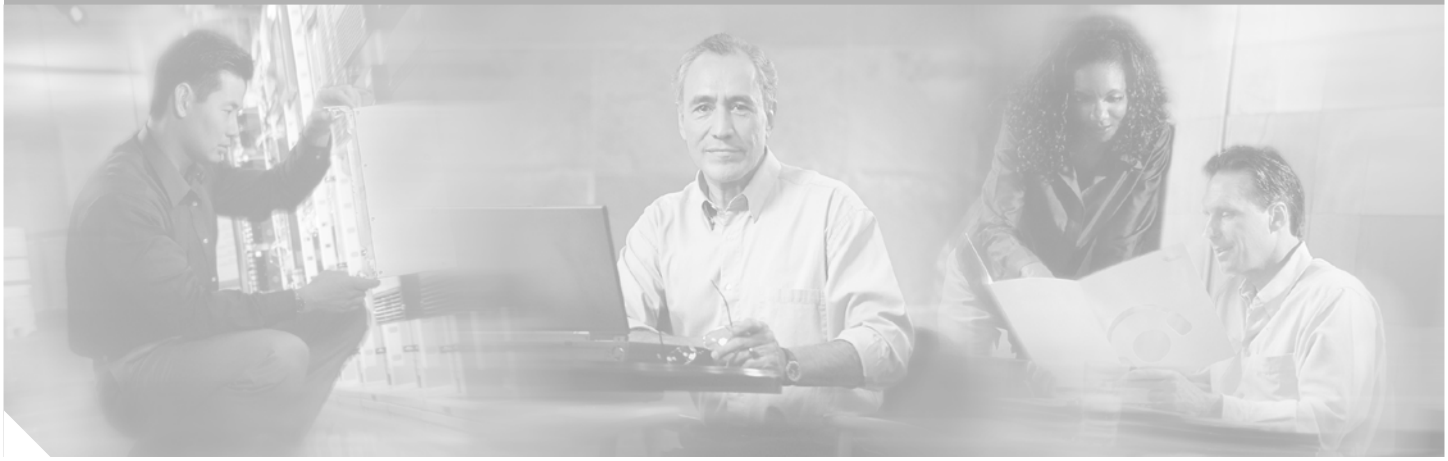


Cisco Unified CME Solution Reference Network Design Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

OL-10621-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and Welcome to the Human Network 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, 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, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, 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. (0711R)

Cisco Unified CallManager Express Solution Reference Network Design (SRND) Guide
Copyright © 2006 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xi

Scope xi

Related Documents and References xii

Document Conventions xvi

Obtaining Documentation xvi

Cisco.com xvi

Product Documentation DVD xvi

Ordering Documentation xvii

Documentation Feedback xvii

Cisco Product Security Overview xvii

Reporting Security Problems in Cisco Products xvii

Product Alerts and Field Notices xviii

Obtaining Technical Assistance xviii

Cisco Technical Support & Documentation Website xviii

Submitting a Service Request xix

Definitions of Service Request Severity xx

Obtaining Additional Publications and Information xx

CHAPTER 1 **Introducing Cisco Unified Communications Express** 1-1

Overview of the Cisco Unified IP Telephony Solution 1-2

Cisco Unified IP Network Infrastructure 1-3

Quality of Service 1-4

Call Processing Agent 1-4

Communication Endpoints 1-5

Applications 1-5

Security 1-6

Network Management Tools 1-7

CHAPTER 2 **IP Telephony Deployment Models** 2-1

Single Site 2-1

Benefits of the Single-Site Model 2-2

Best Practices for the Single-Site Model 2-2

Multisite Implementation with Distributed Call Processing 2-3

Benefits of the Distributed Call Processing Model 2-4

Best Practices for the Distributed Call Processing Model 2-4
Call Processing Agents for the Distributed Call Processing Model 2-5
Design Considerations for Section 508 Conformance 2-6

CHAPTER 3 **Network Infrastructure** 3-1

Cisco Unified CME Network Infrastructure Overview 3-4
  Standalone Network Infrastructure Overview 3-4
  Multisite Network Infrastructure Overview 3-6
LAN Infrastructure 3-9
  LAN Design for High Availability 3-9
    Campus Access Layer 3-9
  Network Services 3-12
    Domain Name System (DNS) 3-12
    Dynamic Host Configuration Protocol (DHCP) 3-12
    Trivial File Transfer Protocol (TFTP) 3-14
    Network Time Protocol (NTP) 3-14
  Power over Ethernet (PoE) 3-15
  Category 3 Cabling 3-16
  IBM Type 1A and 2A Cabling 3-16
  LAN Quality of Service (QoS) 3-17
    Traffic Classification 3-18
    Interface Queuing 3-19
    Bandwidth Provisioning 3-19
    Impairments to IP Communications if QoS is Not Employed 3-20
WAN Infrastructure 3-20
  WAN Design and Configuration Best Practices 3-20
    Deployment Considerations 3-21
    Guaranteed Bandwidth 3-21
    Best-Effort Bandwidth 3-22
  WAN Quality of Service (QoS) 3-22
    Bandwidth Provisioning 3-24
    Traffic Prioritization 3-27
    Link Efficiency Techniques 3-28
    Traffic Shaping 3-31
Wireless LAN Infrastructure 3-33
  WLAN Design and Configuration 3-33
    Wireless Infrastructure Considerations 3-33
    Wireless AP Configuration and Design 3-37
    Wireless Security 3-38

WLAN Quality of Service (QoS) **3-40**
  - Traffic Classification **3-40**
  - Interface Queuing **3-40**
  - Bandwidth Provisioning **3-41**

CHAPTER 4 **Voice Gateways** **4-1**

- Trunk Signaling Systems **4-2**
  - Analog Signaling **4-2**
  - Digital Signaling **4-3**
- Cisco IOS PSTN Telephony Interfaces **4-4**
  - Analog Trunks **4-4**
    - Analog Trunk and Station Hardware **4-5**
    - Configuring Analog Trunks and Stations **4-5**
    - Analog Trunk Features **4-7**
  - Digital Trunks **4-7**
    - Digital Trunk Hardware **4-7**
    - Configuring Digital Trunks **4-8**
    - Digital Trunk Features **4-10**
  - DSP Hardware **4-11**
  - PSTN Trunks Integrated with or Separate from Cisco Unified CME **4-11**
- PSTN Call Switching **4-12**
  - PSTN Call Switching with DID Enabled **4-13**
  - PSTN Call Switching with DNIS (No DID) **4-13**
  - PSTN Call Switching with No DNIS (FXO Trunks) **4-14**
- Digit Manipulation **4-15**
  - Dial Peer Commands **4-15**
  - Cisco IOS Translation Rules **4-16**
  - Cisco Unified CME dialplan-pattern Command **4-17**
- PSTN Trunk Failover **4-18**

CHAPTER 5 **Cisco Unified CallManager Express Call Transfer and Forward** **5-1**

- Call Transfer Methods for VoIP **5-2**
  - H.450 and SIP **5-2**
  - Hairpin Routing **5-3**
  - H.450.12 **5-3**
  - Empty Capabilities Set **5-3**
- Cisco Unified CME VoIP Call Transfer Options **5-4**
- Call Forward Methods for VoIP **5-4**
  - H.450.3 Call Forwarding **5-5**

    - H.323 Facility Message 5-5
    - VoIP Hairpin Call Forwarding 5-5
- Cisco Unified CME VoIP Call Forwarding Options 5-5
- Transfer and Forward Proxy Function 5-6
- Call Transfer and Forward Interoperability with Cisco Unified CallManager 5-7
- Call Transfer and Forwarding with Routed Signaling H.323 Gatekeepers 5-8

CHAPTER 6 **Connecting Multiple Cisco Unified CallManager Express Systems with VoIP** 6-1

- Considerations When Integrating Cisco Unified CME in H.323 and SIP VoIP Networks 6-1
- Integrating Cisco Unified CME in an H.323 Network 6-3
    - A Simple Two-Node Topology with H.323 6-4
    - A Large Multinode Topology with H.323 6-6
    - The Role of an H.323 Gatekeeper 6-8
        - Telephone Address Lookup 6-10
        - Call Admission Control 6-10
        - Billing 6-11
        - Using a Gatekeeper as a Proxy for Additional Services 6-11
    - Public and Internal Phone Numbers in an H.323 Network 6-12
    - Registering Individual Telephone Numbers with a Gatekeeper 6-14
    - Internal and External Callers for VoIP 6-15
- DTMF Relay for H.323 6-16
    - DTMF Digits 6-16
    - Transporting DTMF Digits Reliably Using DTMF Relay 6-17
    - Different Forms of DTMF Relay 6-17
        - H.245 Digit Relay 6-18
        - RTP Digit Relay 6-18
- Call Transfer and Call Forwarding in an H.323 Network Using H.450 Services 6-19
    - H.450.2 Call Transfer 6-20
    - H.450.3 Call Forwarding 6-23
    - H.450.12 Supplementary Services Capabilities 6-24
    - DSP Resources for Transcoding 6-25
    - Configuring H.450.x Services 6-26
    - Cisco Unified CME Local Supplementary Services 6-27
    - H.450.x and Cisco Unified CallManager 6-27
    - H.450.x Proxy Services 6-28
- Integrating Cisco Unified CME in a SIP Network 6-29
    - Two-Node Topology with SIP 6-30
    - SIP Proxy/Registrar/Redirect Server 6-32

- Public and Internal Phone Numbers in a SIP Network **6-33**
- DTMF Relay and RFC 2833 for SIP **6-33**
- SIP Supplementary Services **6-34**
    - MWI Notification **6-34**
    - SIP REFER **6-35**
    - SIP 3XX Response **6-35**
- SIP Interoperability **6-36**

CHAPTER 7 **Integrating Cisco Unified CallManager Express with Cisco Unified CallManager** **7-1**

- Goals of Interoperability **7-1**
- Basic Calls Between Cisco Unified CallManager and Cisco Unified CME **7-2**
- Call Transfer **7-4**
    - H.323 Call Transfer Using an Empty Capabilities Set **7-5**
    - H.323-to-H.323 Call Transfer **7-6**
    - Call Transfer and the Media Termination Point **7-7**
    - Connecting Cisco Unified CallManager with Cisco Unified CME **7-8**
    - Intersite Call Transfer with Multiple Cisco Unified CME Systems **7-9**
- Call Forwarding **7-10**
- Connected Party Name and Number Services **7-12**
- Using H.450.x Cisco IP-to-IP Gateway **7-13**

CHAPTER 8 **Integrating External Applications with Cisco Unified CallManager Express** **8-1**

- Cisco Unified CME External Voice Mail Options **8-2**
    - Cisco Unity Voice Mail **8-2**
        - Standalone Cisco Unified CME System with Cisco Unity **8-3**
        - Multiple Cisco Unified CME Systems with a Centralized Cisco Unity System **8-3**
        - Configuring Cisco Unified CME for Cisco Unity **8-4**
        - MWI **8-6**
        - MWI Relay **8-6**
    - Stonevoice Voice Mail **8-8**
        - Configuring Cisco Unified CME for Stonevoice **8-9**
        - MWI for Stonevoice **8-10**
    - Analog Voice Mail **8-10**
        - Octel **8-11**
        - Active Voice Reception **8-12**
    - PSTN-Based Voice Mail **8-13**
- TAPI and XML Application Architecture **8-14**
- TAPI Applications **8-15**

    Cisco Unified CME TAPI Light 8-15
    Cisco Unified CME TSP Functions 8-16
    Cisco CRM Communications Connector 8-18
  Extensible Markup Language Applications 8-19
    General XML Phone Services 8-19
    Cisco Unified CME XML Phone Services 8-19
    XML Application Example 8-20
    Cisco Unified CME Configuration for XML Applications 8-20

CHAPTER 9 Cisco Unified CallManager Express Dial Plan 9-1
  POTS Dial Peers 9-1
  VoIP Dial Peers 9-2
  Extensions 9-2
  Digit Manipulation Features 9-3
  Other Cisco Unified CME Dial Plan Features 9-3

CHAPTER 10 Cisco Unified CallManager Express Security Best Practices 10-1
  Securing GUI Access 10-1
    System Administrator Account Authentication via AAA 10-2
  Using HTTPS for Cisco Unified CME GUI Management 10-2
  Configuring Basic Cisco Unified CME Access Security 10-3
    Setting Local and Remote System Access 10-3
      Enabling Secret and Encrypt Passwords 10-3
      Creating Multiple Privilege Levels 10-4
      Restrict Access to VTY 10-4
      Using AAA to Secure Access 10-4
      Configuring Accounting and Auditing on AAA 10-4
      Configuring Local User Authentication When AAA Is Not Available 10-5
    Restricting Access to tty 10-5
    Configuring SSH Access 10-5
    Using ACLs for SNMP Access 10-6
    Disabling Cisco Discovery Protocol 10-6
    Configuring COR for Incoming and Outgoing Calls 10-6
    Restricting Outgoing Calling Patterns 10-8
  Cisco Unified CME Security for IP Telephony 10-8
    IP Phone Registration Control 10-9
    Monitoring IP Phone Registration 10-10
    Call Activity Monitoring and Call History Logging 10-10

COR for Incoming/Outgoing Calls to Prevent Toll Fraud 10-10
After-hours Blocking to Restrict Outgoing Calling Pattern-Toll Fraud 10-12
Cisco Unified CME with NAT and Firewall 10-13
Cisco Unified CME with NAT 10-13
Remote Phones with Public IP Addresses 10-14
Remote Phones with Private IP Addresses 10-14
Remote Phones over VPN 10-15
Cisco Unified CME with Cisco IOS Firewall Implementation Considerations 10-16
Overview of Cisco IOS Firewall with Cisco Unified CME 10-16
Previous Problems on Cisco Unified CME with Cisco IOS Firewall 10-17
Cisco Unified CME and Cisco IOS Firewall on the Same Router 10-18
Other Alternatives for Ensuring Cisco Unified CME Security 10-19
Secure SCCP Signaling via TLS 10-19
Troubleshooting and Debugging 10-22
Cisco Unified CME Commonly Used Ports 10-23

CHAPTER 11 **Managing and Monitoring Cisco Unified CallManager Express Systems** 11-1

Configuring and Monitoring via Network Management Systems Using the Cisco Unified CME AXL/SOAP Interface 11-1
Cisco Unified CME 4.0 XML Interface Enhancements 11-2
The Cisco Unified CME AXL/SOAP Interface 11-2
Testing the Cisco Unified CME AXL/SOAP Interface 11-3
Cisco Unified CME 4.0 XML Configuration Example 11-4
Monitoring Cisco Unified CME 11-4
Monitoring IP Phones Using Cisco Unified CME Syslog Messages 11-5
Monitoring Call Activity 11-6
Monitoring Cisco Unified CME Call History 11-6
Logging CDR to External Servers 11-6
Using Account Codes for Billing 11-7
Monitoring Voice Performance Statistics 11-8
Using Cisco Unified CME Supported SNMP MIBs 11-8
Managing Cisco Unified CME Systems 11-10
Cisco Unified CME Management Overview 11-10
Managing a Standalone Cisco Unified CME System 11-10
Cisco Zero Touch Deployment 11-11
Understanding Cisco Zero Touch Deployment Components 11-11
Managing Multisite Cisco Unified CME Networks 11-13
Managing Cisco Unified CME Systems with Cisco Network Management Tools 11-13
Cisco Unified CME Quick Configuration Tool 11-13

Cisco Unified Operations Manager and Cisco Unified Service Monitor 11-14
Managing Cisco Unified CME Systems with Cisco Partner Applications 11-15
NetIQ Vivinet Manager 11-15
Stonevoice 11-21
ISI Telemanagement Solutions Inc. Infortel Select 11-28
Integrated Research Prognosis 11-29

CHAPTER 12 IP Telephony Endpoints for Cisco Unified CallManager Express 12-1
Analog Gateway 12-2
Cisco VG224 Gateway 12-2
Cisco Analog Telephone Adaptor 12-2
Cisco Unified IP Phone 12-3
Low-End Cisco Unified IP Phones 12-3
Cisco Unified IP Phone 7902G 12-3
Cisco Unified IP Phone 7905G 12-3
Cisco Unified IP Phone 7910G and Cisco Unified IP Phone 7910G+SW 12-3
Cisco Unfied IP Phone 7911G 12-4
Cisco Unified IP Phone 7912G 12-4
Mid-Range Cisco Unified IP Phones 12-4
High-End Cisco Unified IP Phones 12-4
Wireless Endpoint 12-4
Site Survey 12-5
Authentication 12-5
Capacity 12-6
Phone Configuration 12-6
Roaming 12-7
AP Call Admission Control 12-8
Cisco Unified IP Conference Station 12-8
QoS Recommendations 12-8
Cisco VG224 12-9
Cisco ATA 186 and Conference Station 12-10
Cisco ATA 188 and Cisco Unified IP Phones 12-10
Cisco Unified Wireless IP Phone 7920G 12-14
Endpoint Features Summary 12-17

INDEX

Preface

This document provides design considerations and guidelines for deploying Cisco Unified CallManager Express (Cisco Unified CME) in the context of standalone or distributed call control environments.

Note Some of the content used in this his publication originated as content in the Cisco Press book entitled *Cisco IP Communications Express: CallManager Express with Cisco Unity Express* (ISBN: 158705180X). See the following Cisco Press summary for a complete table of contents and book description: http://www.ciscopress.com/title/158705180X

Scope

Note This document addresses features available as of Cisco Unified CME 3.1 and later. Features that are associated only with later releases are specifically noted in the body of the publication.

This publication addresses a variety of design considerations associated with deploying Cisco Unified CME. Specific chapters presented in this design guide are as follows:

- Chapter 1, "Introducing Cisco Unified Communications Express"
- Chapter 2, "IP Telephony Deployment Models"
- Chapter 3, "Network Infrastructure"
- Chapter 4, "Voice Gateways"
- Chapter 5, "Cisco Unified CallManager Express Call Transfer and Forward"
- Chapter 6, "Connecting Multiple Cisco Unified CallManager Express Systems with VoIP"
- Chapter 7, "Integrating Cisco Unified CallManager Express with Cisco Unified CallManager"
- Chapter 8, "Integrating External Applications with Cisco Unified CallManager Express"
- Chapter 9, "Cisco Unified CallManager Express Dial Plan"
- Chapter 10, "Cisco Unified CallManager Express Security Best Practices"
- Chapter 11, "Managing and Monitoring Cisco Unified CallManager Express Systems"
- Chapter 12, "IP Telephony Endpoints for Cisco Unified CallManager Express"

Related Documents and References

For more information about topics addressed in this publication, see the Cisco documents listed in Table 1 and external websites listed in Table 2.

Table 1 Related Cisco Content by Chapter

Chapter	Topic	Cisco Public Website Links
Chapter 2	Cisco Unified CME	http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html
	Large scale deployment	http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html
Chapter 3	Cisco 1800 ISR APs	http://www.cisco.com/en/US/products/ps5853/products_data_sheet0900aecd8028a95f.html
	Cisco 870 Integrated Service Routers (ISR) APs	http://www.cisco.com/en/US/products/hw/routers/ps380/products_data_sheet0900aecd8028a976.html
	Campus network design	http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.pdf
	Cisco High-speed WAN Interface Card (HWIC)-AP	http://www.cisco.com/en/US/products/ps5949/products_data_sheet0900aecd8028cc7b.html
	Cisco IOS Wireless LAN configuration	http://www.cisco.com/en/US/docs/ios/wlan/configuration/guide/12_4t/wl_12_4t_book.html
	Cisco Unified Wireless IP Phone 7920	http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html
	Cisco Wireless LAN Services Module (WLSM)	http://www.cisco.com/en/US/products/hw/modules/ps2706/products_implementation_design_guide09186a00807d592c.html
	Integrated Services Router (ISR) implementation limitations	http://www.cisco.com/en/US/products/hw/routers/ps380/products_data_sheet0900aecd8016ef57.html
	Voice-Adaptive Traffic Shaping and Fragmentation	http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541c6.html
Chapter 4	Digital trunks	http://www.cisco.com/en/US/tech/tk652/tk653/technologies_configuration_example09186a008010f05d.shtml
Chapter 6	Cisco Multiservice IP-to-IP Gateway	http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_qanda_item09186a00801da69b.shtml

Table 1 Related Cisco Content by Chapter (continued)

Chapter	Topic	Cisco Public Website Links
Chapter 8	Cisco and Microsoft implementations	http://www.cisco.com/web/partners/pr67/pr41/solutions/index.html
	Cisco Unity Express	*Cisco Unity Express Design Guide* http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/design/design21/cuedg21.html *Excerpts from Cisco IP Communications Express: CallManager Express with Cisco Unity Express* http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/design/CP_CIPExpress/excerpts.html
	CRM Communications Connector	http://www.cisco.com/en/US/products/ps7274/tsd_products_support_series_home.html
	Customer Relations Management (CRM) Express solution specialization	http://www.cisco.com/web/partners/pr11/pr66/crm_express/partners_pgm_concept_home.html
	XML development	http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html
Chapter 10	Cisco Unified CME Command Reference	http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_command_reference_book09186a00805b6c70.html
Chapter 11	XML Provisioning Guide for Cisco CME/SRST	http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_programming_reference_guide09186a00801c5fab.html
	Cisco CallManager Express 3.4 SNMP MIB Support	http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/mib/reference/guide/ccme_mib.html
	Cisco Networking Services Configuration Engine	http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html
	Cisco Unified CME QCT Data Sheet	http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_data_sheet0900aecd802e9be9.html
	Configuring Your System Using Cisco IPC Express Quick Configuration Tool	http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/qct/configuration/guide/qct_usr.html
	Cisco Unified CME QCT software download site	http://www.cisco.com/pcgi-bin/tablebuild.pl/cme-qct
	Cisco Unified Operations Manager data sheets	http://www.cisco.com/en/US/products/ps6535/products_data_sheets_list.html
	Technical documentation for Cisco Unified Operations Manager	http://www.cisco.com/en/US/products/ps6535/tsd_products_support_series_home.html
	Cisco Unified Service Monitor data sheets	http://www.cisco.com/en/US/products/ps6536/products_data_sheets_list.html
	Technical documentation for Cisco Unified Service Monitor	http://www.cisco.com/en/US/products/ps6536/tsd_products_support_series_home.html

Table 1 Related Cisco Content by Chapter (continued)

Chapter	Topic	Cisco Public Website Links
General	Cisco developer support (limited access site)	http://www.cisco.com/cgi-bin/dev_support/access_level/product_support
	Cisco Unified CME configuration examples	http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_configuration_examples_list.html
	Solution Reference Network Design guides	http://www.cisco.com/go/srnd

Table 2 Recommended External Websites References

Organization	External Website Link
IP Blue	http://www.ipblue.com/
NetIQ	http://www.netiq.com/
Stonevoice	http://www.stonevoice.com/
ISI Telemanagement Solutions	http://www.isi-info.com/
Integrated Research	http://www.prognosis.com/

Table 3 Standards and RFCs

Organization	External Website Link
ITU-T H-series standard	http://www.itu.int/rec/T-REC-H/en
RFC 1918	http://www.apps.ietf.org/rfc/rfc1918.html

Document Conventions

This guide uses the following special convention:

Table 4 Document Conventions

Convention	Description
The letter *y* used in a phone number prefix.	Represents the prefix for a telephone number. Example: 506.5yy.1234. This convention is used when phone numbers outside the range of 555-0100 to 555-0199 are required for a given example.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the magazine for Cisco networking professionals. Each quarter, *Packet* delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *Packet* magazine at this URL:

  http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Introducing Cisco Unified Communications Express

Cisco Unified Communications Express is an award-winning IP communications solution that is provided with the Cisco Integrated Services Router portfolio. Cisco Unified Communications Express includes:

- Cisco Unified CallManager Express to provide rich call processing
- Cisco Unity Express to provides integrated messaging with an AIM or NM module
- Full portfolio of IP phones to meet the small medium business needs
- Full-featured voice over IP (VoIP) capability to support H.323 and Session Initiation Protocol (SIP) implementations
- Voice gateways supporting VG224 and analog telephone adaptors (ATA)

Cisco Unified Communications Express provides a complete solution based on Cisco Integrated Services Router. This solution includes:

- Integrated wired and wireless LAN
- Integrated security with VPN, firewall, and encryption
- Cisco routing and switching functionality

Cisco Unified Communications Express encompasses the following solutions:

- Basic Automatic Call Distribution (B-ACD)

  Cisco Unified CallManager Express (Cisco Unified CME) B-ACD provides automatic answering and call distribution for calls through the use of interactive menus and local hunt groups.

- Customer Contact

  Cisco Customer Contact solutions are a combination of strategy and architecture that promote efficient and effective customer communications across a globally capable network by enabling organizations to draw from a broader range of resources to service customers, including access to an unlimited pool of agents and multiple channels of communication as well as customer self-help tools.

- IP Telephony

  IP telephony refers to technology that transmits voice communications over a network using IP standards. The Cisco Unified IP Telephony solution includes a wide array of hardware and software products such as call processing agents, IP phones, video devices, and special applications.

- Rich-Media Conferencing

  Cisco Rich-Media Conferencing solutions enhance the virtual meeting environment with a integrated set of IP-based tools for voice, video, and Web conferencing.
- Third-Party Applications

  We work with leading-edge companies to provide the broadest selection of innovative third-party IP telephony applications and products focused on critical business needs such messaging, customer care, and workforce optimization.
- Unified Communications

  Cisco Unified Communications Express solutions deliver unified messaging (e-mail, voice, and fax messages managed from a single inbox) and intelligent voice messaging (full-featured voicemail providing advanced capabilities) to improve communications, boost productivity, and enhance customer service capabilities across an organization. Cisco Unified Communications Express solutions also enable users to streamline communication processes through the use of features such as rules-based call routing, simplified contact management, and speech recognition.
- Video Telephony

  The Cisco Video Telephony solution enables real-time video communications and collaboration using the same IP network and call processing agent as the Cisco Unified IP Telephony solution. With Cisco Video Telephony, making a video call is now as easy as dialing a phone number.

Note For additional information, see the "Related Documents and References" section on page xii.

Overview of the Cisco Unified IP Telephony Solution

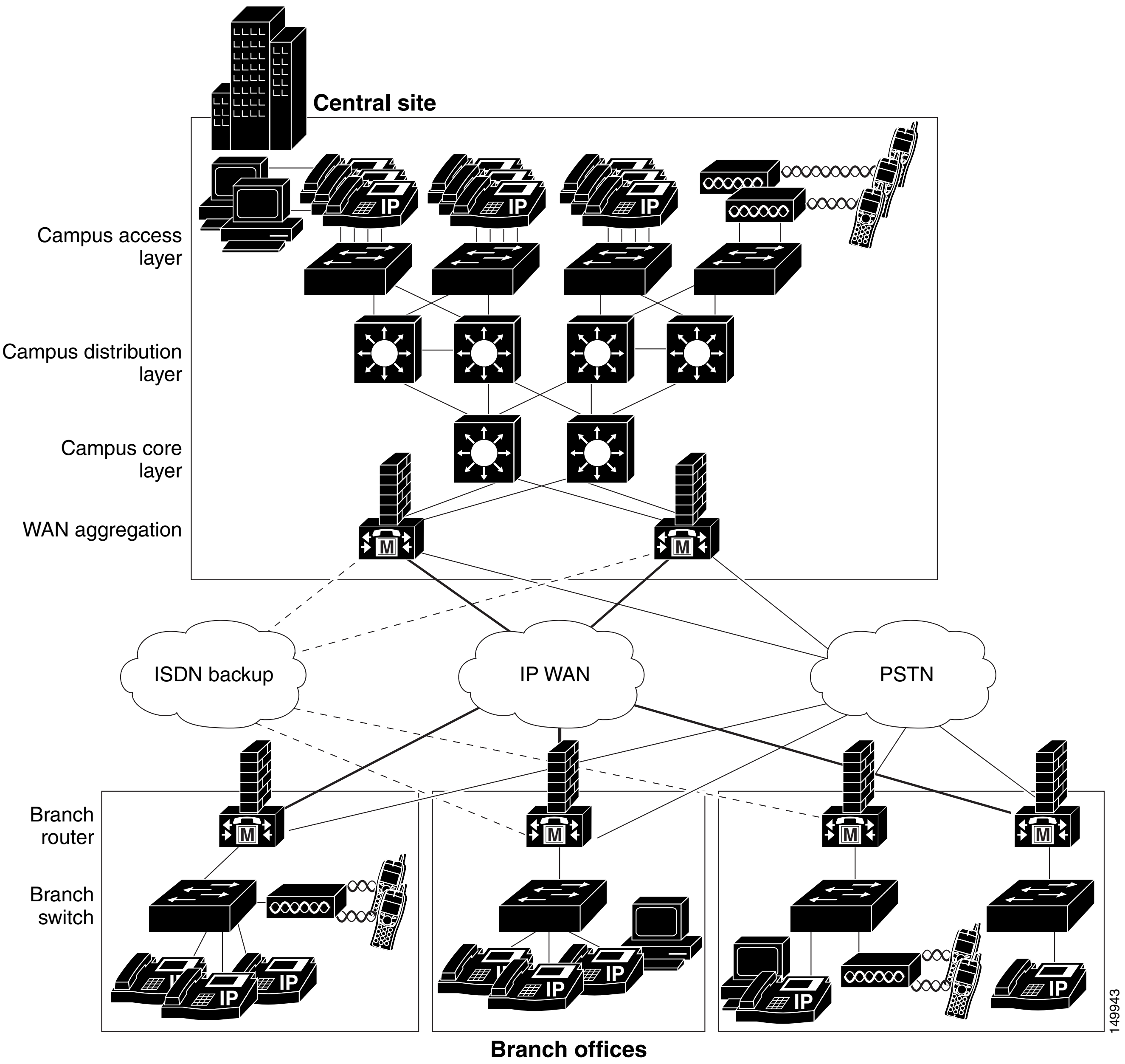
The Cisco Unified IP Telephony solution is the leading converged network telephony solution for organizations that want to increase productivity and reduce the costs associated with managing and maintaining separate voice and data networks. The flexibility and sophisticated functionality of the Cisco Unified IP network infrastructure provides the framework that permits rapid deployment of emerging applications such as desktop Cisco Unified IP Telephony, unified messaging, video telephony, desktop collaboration, enterprise application integration with IP phone displays, and collaborative IP contact centers. These applications enhance productivity and increase enterprise revenues.

Figure 1-1 illustrates a typical IP Telephony solution employing the Cisco Unified IP network infrastructure, with Cisco Unified CME as the call processing agent.

The foundation architecture of the Cisco Unified IP Telephony solution includes of the following major components (see Figure 1-1):

- Cisco Unified IP Network Infrastructure, page 1-3
- Quality of Service, page 1-4
- Call Processing Agent, page 1-4
- Communication Endpoints, page 1-5
- Applications, page 1-5
- Security, page 1-6
- Network Management Tools, page 1-7

Figure 1-1 Typical Enterprise Cisco Unified IP Telephony Environment


Central site
Campus access layer
Campus distribution layer
Campus core layer
WAN aggregation
IP
M
ISDN backup
IP WAN
PSTN
Branch router
Branch switch
Branch offices
149943

Cisco Unified IP Network Infrastructure

The network infrastructure includes public switched telephone network (PSTN) gateways, analog phone support, and digital signal processor (DSP) farms. The infrastructure can support multiple client types such as hardware phones, software phones, and video devices. The infrastructure also includes the interfaces and features necessary to integrate legacy PBX, voicemail, and directory systems. Typical products used to build the infrastructure include Cisco voice gateways (nonrouting, routing, and integrated), Cisco IOS software and Catalyst switches, and Cisco routers.

Quality of Service

Voice, as a class of IP network traffic, has strict requirements concerning packet loss, delay, and delay variation (also known as jitter). To meet these requirements for voice traffic, the Cisco Unified IP Telephony solution includes Quality of Service (QoS) features such as classification, queuing, traffic shaping, compressed Real-Time Transport Protocol (cRTP), and Transmission Control Protocol (TCP) header compression.

The QoS components of the Cisco Unified IP Telephony solution are provided through the rich IP traffic management, queueing, and shaping capabilities of the Cisco Unified IP network infrastructure. Key elements of this infrastructure that enable QoS for IP telephony include:

- Call admission control
- Compressed RTP (cRTP)
- Enhanced queuing services
- Link efficiency
- Link fragmentation and interleaving (LFI)
- Low-latency queuing (LLQ)
- Traffic marking
- Traffic shaping

Call Processing Agent

In the context of a standalone small/medium business application or for distributed call processing designs, Cisco Unified CME is the core call processing software for the Cisco Unified IP Telephony solution. It builds call processing capabilities on top of the Cisco Unified IP network infrastructure. Cisco Unified CME software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, Voice over IP (VoIP) gateways, and multimedia applications.

You can deploy the call processing capabilities of Cisco Unified/ CME according to one of the following models, depending on the size, geographical distribution, and functional requirements of your enterprise:

- Single-site call processing model

  In the single-site model, each site has its own Cisco Unified CME. No voice traffic travels over the IP WAN; instead, external calls or calls to remote sites use the public switched telephone network (PSTN).

- Multisite WAN model with distributed call processing

  In the multisite WAN model with distributed call processing, each site has its own Cisco Unified CME. Communication between sites normally takes place over the IP WAN, with the PSTN serving as a backup voice path. With this model, you can interconnect any number of sites across the IP WAN.

Communication Endpoints

A communication endpoint is a user instrument such as a desk phone or even a software phone application that runs on a PC. In the IP environment, each phone has an Ethernet connection. IP phones have all the functions you expect from a telephone, as well as more advanced features such as the ability to access World Wide Web sites.

In addition to various models of desktop Cisco Unified IP Phones, IP Telephony endpoints include the following devices:

- Software-based IP phones

  Cisco Unified IP Softphone and Cisco IP Communicator are desktop applications that turn your computer into a full-featured IP phone with the added advantages of call tracking, desktop collaboration, and one-click dialing from online directories. Cisco software-based IP phones offer users the great benefit of having a portable office IP phone to use anywhere an Internet connection is available.

- Wireless IP phones

  The Cisco Unified Wireless IP Phone 7920 extends the Cisco family of IP phones from 10/100 Ethernet to 802.11 wireless LAN (WLAN). The Cisco 7920 Wireless IP Phone provides multiple line appearances with functionality similar to existing Cisco 7900 Series IP Phones. In addition, the Cisco 7920 phone provides enhanced WLAN security and Quality of Service (QoS) for operation in 802.11b networks. The Cisco 7920 phone also provides support for XML-based data access and services.

Applications

Voice and video applications build upon the call processing infrastructure to enhance the end-to-end capabilities of the Cisco Unified IP Telephony solution by adding sophisticated telephony and converged network features, such as the following:

- Cisco Unified MeetingPlace Express

  Cisco Unified MeetingPlace Express is a complete rich-media conferencing solution that integrates voice and Web conferencing capabilities to make remote meetings as natural and effective as face-to-face meetings. In a single step, meeting organizers can schedule voice, video, and Web resources through either the Cisco Unified MeetingPlace Express Web interface, an IP phone, or their Microsoft Outlook or Lotus Notes calendars. Meeting invitees automatically receive notification by email or calendar invitation and can attend rich-media conferences with a single click.

- Cisco Unity Express Auto Attendant and Voice Mail

  Cisco Unity Express provides a distributed AA and voice-mail application to an IP Telephony solution where the large offices may have a high-end voice mail solution (such as Cisco Unity) and one or more of the smaller remote offices may use a local or distributed Cisco Unity Express for voice mail. Cisco Unity Express is deployed with one of two call-processing models that are based on either Cisco Unified CME or Cisco Unified CallManager.

  The call processing engine (Cisco Unified CME or Cisco Unified CallManager) manages the IP phones and features such as call-forward-busy (CFB) and call-forward-no-answer (CFNA) to the voice mail pilot number, while Cisco Unity Express provides the AA menus, scripts and voice mail telephony user interface (TUI) sessions for callers retrieving or leaving voice messages. Cisco Unity Express stores the AA scripts and prompts, voice mail subscriber spoken names, greetings and voice mail messages.

Cisco Unity Express interfaces with Cisco Unified CME call control via a Session Initiation Protocol (SIP) interface and to Cisco Unified CallManager via a Java Telephony Applications Programming Interface (JTAPI) interface.

- Unified messaging

  Cisco Unity delivers powerful unified messaging (email, voice, and fax messages sent to one inbox) and intelligent voice messaging (full-featured voicemail providing advanced functionality) to improve communications, boost productivity, and enhance customer service capabilities across your organization. With Cisco Unity Unified Messaging, you can listen to your e-mail over the phone, check voice messages from the Internet, and (when integrated with a supported third-party fax server) send faxes anywhere.

- Web services for Cisco Unified IP Phones

  You can use Cisco Unified IP Phones to deploy customized client services with which users can interact via the keypad and display. You can create applications for Cisco Unified IP Phone services by using the eXtensible Markup Language (XML) Application Programming Interface (API) and deploy them using HTTP from standard web servers, such as Microsoft IIS. Some typical services that can be provided through a Cisco Unified IP Phone include a full conferencing interface, the ability to manage data records even if no PC is available, and the ability to display employee alerts, clocks, stock market information, customer contact information, daily schedules, and so forth.

- Cisco Unified CME B-ACD

  Cisco Unified CME B-ACD provides automatic answering and call distribution for calls through the use of interactive menus and local hunt groups. Each Cisco Unified CME B-ACD application consists of one or more auto-attendant (AA) services and one call-queue service.

Security

The Cisco Unified IP Telephony solution addresses security in the following main areas, among others:

- Physical security for restricting physical access to important application servers and network components
- Network access security to prevent hostile logins or attacks
- Security measures for your Cisco router running Cisco Unified CME
- Mechanisms for defining calling privileges for various classes of users
- Careful network design and management to enhance security

Network Management Tools

The Cisco Unified IP network infrastructure offers a number of network management, QoS, and security management tools that support the IP Telephony solution. Cisco Unified CME offers enhanced software and configuration management tools that leverage the strength and flexibility of IP networks. The Cisco Unified CME user interface simplifies the most common subscriber and telephony configuration tasks by building upon legacy telephony administration systems and adding software and web-based applications.

In addition, CiscoWorks 2000 includes a number of network management tools to manage the operations, administration, and maintenance of IP Telephony networks.

CiscoWorks IP Communications Operations Manager (CiscoWorks IPCOM) provides a suite of applications and tools that facilitate effective management of IP Telephony installations. CiscoWorks IPCOM provides the following major features:

- Problem-focused fault analysis — Provides timely information about the health of IP Telephony environments.
- Confidence testing and monitoring — Permits the use synthetic testing to emulate normal day-to-day operations and to validate operational readiness of the IP infrastructure and the Cisco Unified IP Telephony deployment.
- Intelligent integration with existing management infrastructures — Generates intelligent traps that can be forwarded to other event-management systems installed in the network, sent to email or pager gateways, or displayed on the Alerts and Activities Display (AAD).
- Evaluation and correlation capabilities — Allows for the evaluation of the general health of the IP Telephony environment in the monitored network environment.
- Alerts and activities display (AAD) — Provides a proactive, web-based operations screen for real-time status and alerting of actual and suspected problems in the underlying IP network as well as in the Cisco Unified IP Telephony implementation.
- Cisco Unified IPCOM Multiview — Enables large enterprise customers and managed service providers to partition specific user communities and manage each from a single Cisco Unified IPCOM implementation.

IP Telephony Deployment Models

Last Updated: January 8, 2009

Sections in this chapter address the following topics:

- Single Site, page 2-1
- Multisite Implementation with Distributed Call Processing, page 2-3
- Design Considerations for Section 508 Conformance, page 2-6

Note For additional information, see the "Related Documents and References" section on page xii.

Single Site

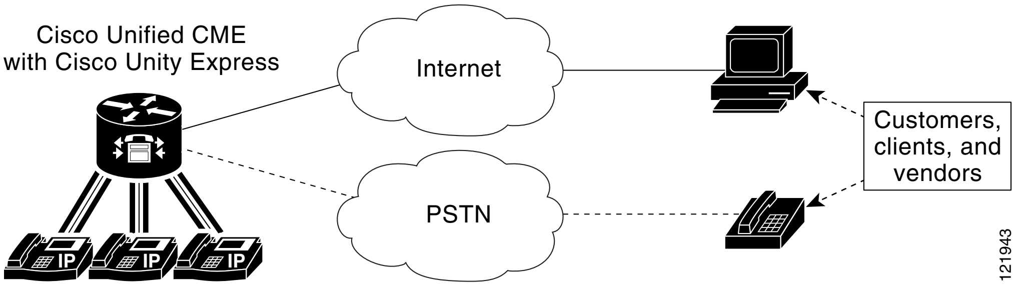
The single-site model for IP telephony consists of a call processing agent located at a single site, or campus, with no telephony services provided over an IP WAN. An SMB would typically deploy the single-site model over single site router running at a single location. In this model, calls beyond the LAN use the PSTN.

The single-site model has the following design characteristics:

- Single Cisco Unified CallManager Express (Cisco Unified CME) router or dual Cisco Unified CME router for redundancy
- Maximum of 240 IP phones
- PSTN for all external calls
- Digital signal processor (DSP) resources for transcoding and PSTN termination.
- Voicemail or unified messaging with AA components
- Only G.711 codecs for all IP phone calls (80 kbps of IP bandwidth per call, uncompressed)
- Capability to integrate with legacy private branch exchange (PBX) and voicemail systems

Figure 2-1 illustrates and example of the model for an IP telephony network within a single campus or site.

Figure 2-1 Single-Site Model



Benefits of the Single-Site Model

A single infrastructure for a converged network solution provides significant cost benefits and enables IP telephony to take advantage of the many IP-based applications in the enterprise. Single-site deployment also allows each site to be completely self-contained. 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:

- Common infrastructure for a converged solution
- Ease of deployment
- No transcoding resources required, due to the use of only G.711 codecs
- Simplified dial plan

Best Practices for the Single-Site Model

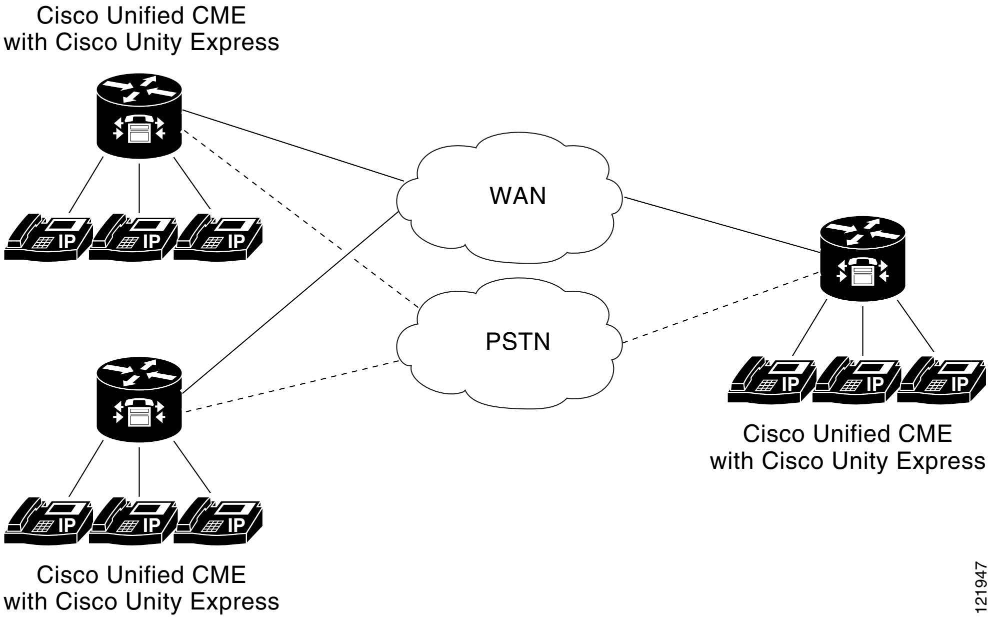
Follow these guidelines and best practices when implementing the single-site model:

- Provide a highly available, fault-tolerant infrastructure based on a common infrastructure philosophy. A sound infrastructure is essential for easier migration to IP telephony, integration with applications such as video streaming and video conferencing, and expansion of your IP telephony deployment across the WAN or to multiple Cisco Unified CallManager clusters.
- Know the calling patterns for your enterprise. Use the single-site model if most of the calls from your enterprise are within the same site or to PSTN users outside your enterprise.
- Use G.711 codecs for all endpoints. This practice eliminates the consumption of digital signal processor (DSP) resources for transcoding, and those resources can be allocated to other functions such as conferencing and Media Termination Points (MTPs).
- Implement the recommended network infrastructure for high availability, connectivity options for phones (in-line power), Quality of Service (QoS) mechanisms, and security. See Chapter 3, "Network Infrastructure."

Multisite Implementation with Distributed Call Processing

The multisite WAN model with distributed call processing consists of multiple independent sites, each with its own call processing agent connected to a PSTN or an IP WAN (or combination including both) that carries voice traffic between the distributed sites. Figure 2-2 illustrates a typical distributed call processing deployment, featuring an IP WAN interconnection and a backup PSTN connection.

Figure 2-2 A Distributed Call Processing Deployment featuring Cisco Unified CME



Each site in a distributed call processing model can be one of the following:

- A single site with its own call processing agent, which can be either:
  - Cisco Unified CME
  - Cisco Unified CallManager
  - Other IP PBX
- A centralized call manager and all of its associated remote sites
- A legacy PBX with Voice over IP (VoIP) gateway
- One or more gatekeepers can be deployed to help with dial plan management.

Note See the following URL related Cisco Unified CME documentation: http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html

An IP WAN interconnects all the distributed call processing sites. Typically, the PSTN serves as a backup connection between the sites in case the IP WAN connection fails or does not have any more available bandwidth. A site connected only through the PSTN is a standalone site and is not covered by the distributed call processing model. (See Single Site, page 2-1.)

Connectivity options for the IP WAN include:

- Leased lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- ATM and Frame Relay Service Inter-Working (SIW)
- Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)
- Voice and Video Enabled IP Security Protocol (IP Sec) VPN (V3PN)

Benefits of the Distributed Call Processing Model

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. 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.
- No loss of functionality during IP WAN failure because there is a call processing agent at each site.
- Scalability to hundreds of sites.

Best Practices for the Distributed Call Processing Model

A multi-site deployment with distributed call processing has many of the same requirements as a single site or a multi-site deployment with centralized call processing. Follow the best practices from these other models in addition to the ones listed here for the distributed call processing model.

Gatekeeper or Session Initiation Protocol (SIP) proxy servers are among the key elements in the multi-site WAN model with distributed call processing. They each provide dial plan resolution, with the gatekeeper also providing call admission control. A gatekeeper is an H.323 device that provides call admission control and E.164 dial plan resolution.

The following best practices apply to the use of a gatekeeper:

- Use a Cisco IOS gatekeeper to provide call admission control into and out of each site.
- To provide high availability of the gatekeeper, use Hot Standby Router Protocol (HSRP) gatekeeper pairs, gatekeeper clustering, and alternate gatekeeper support. In addition, use multiple gatekeepers to provide redundancy within the network.
- Size the platforms appropriately to ensure that performance and capacity requirements can be met.
- Use only one type of codec on the WAN because the H.323 specification does not allow for Layer 2, IP, User Data 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.
- Gatekeeper networks can scale to hundreds of sites, and the design is limited only by the WAN topology.

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

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

- Provide adequate redundancy for the SIP proxies.
- Ensure that the SIP proxies have the capacity for the call rate and number of calls required in the network.
- Planning for call admission control is outside the scope of this document.

Call Processing Agents for the Distributed Call Processing Model

Your choice of call processing agent will vary, based on many factors. The main factors, for the purpose of design, are the size of the site and the functionality required.

For a distributed call processing deployment, each site has its own call processing agent. The design of each site varies with the call processing agent, the functionality required, and the fault tolerance required. For example, in a site with 500 phones, a Cisco Unified CallManager cluster containing two servers can provide one-to-one redundancy, with the backup server being used as a publisher and TFTP (Trivial File Transfer Protocol) server.

The requirement for IP-based applications also greatly affects the choice of call processing agent because only Cisco Unified CallManager provides the required support for many Cisco IP applications.

Table 2-1 lists recommended call processing agents.

Table 2-1 Recommended Call Processing Agents

Call Processing Agent	Recommended Size	Comments
Cisco Unified CME	Up to 240 phones	• For small remote sites. • Capacity depends on Cisco IOS platform; see platform-specific support documentation for more details.
Cisco Unified CallManager	50 to 30,000 phones	• Small to large sites, depending on the size of the Cisco Unified CallManager cluster. • Supports centralized or distributed call processing.
Legacy PBX with VoIP gateway	Depends on PBX	• Number of IP WAN calls and functionality depend on the PBX-to-VoIP gateway protocol and the gateway platform.

Design Considerations for Section 508 Conformance

Regardless of which deployment model you choose, you should consider designing your IP telephony network to make the telephony features more accessible to users with disabilities, in conformance with Section 255 of the Telecommunications Act and U.S. Section 508.

Observe the following basic design guidelines when configuring your IP telephony network to conform to Section 508:

- Enable Quality of Service (QoS) on the network.
- Configure only the G.711 codec for phones that will be connected to a terminal teletype (TTY) device or a Telephone Device for the Deaf (TDD). Although low bit-rate codecs such as G.729 are acceptable for audio transmissions, they do not work well for TTY/TDD devices if they have an error rate higher than one percent Total Character Error Rate (TCER).
- Configure TTY/TDD devices for G.711 across the WAN, if necessary.
- Enable (turn ON) Echo Cancellation for optimal performance.
- Voice Activity Detection (VAD) does not appear to have an effect on the quality of the TTY/TDD connection, so it may be disabled or enabled.
- Connect the TTY/TDD to the IP telephony network in either of the following ways:
  - Direct connection (Recommended method)

    Plug a TTY/TDD with an RJ-11 analog line option directly into a Cisco FXS port. Any FXS port will work, such as the one on the Cisco VG224, Cisco VG248, Catalyst 6000, Cisco ATA 188 module, or any other Cisco voice gateway with an FXS port. We recommend this method of connection.
  - Acoustic coupling

    Place the IP phone handset into a coupling device on the TTY/TDD. Acoustic coupling is less reliable than an RJ-11 connection because the coupling device is generally more susceptible to transmission errors caused by ambient room noise and other factors.
- If stutter dial tone is required, use an analog phone in conjunction with an FXS port on the Cisco VG224 or Cisco ATA 188.

CHAPTER 3

Network Infrastructure

This chapter describes the requirements of the network infrastructure needed to build an IP telephony system in an enterprise environment. Figure 3-1 illustrates the roles of the various devices that form the network infrastructure of a large-scale enterprise network, and Table 3-1 summarizes the features required to support each of these roles.

IP telephony places strict requirements on IP packet loss, packet delay, and delay variation (or jitter). Therefore, you need to enable most of the Quality of Service (QoS) mechanisms available on Cisco switches and routers throughout the network. For the same reasons, redundant devices and network links that provide quick convergence after network failures or topology changes are also important to ensure a highly available infrastructure.

Note In general, this document focuses on standalone and multisite Cisco Unified CallManager Express (Cisco Unified CME) implementations. However, this chapter addresses many issues related to larger enterprise-sized networks. As such, it discusses issues related to Cisco Unified CME deployments featuring centralized call processing. This information is included for context, as Cisco Unified CME is also applicable in larger networks as part of a distributed environment. For more information, see the collection of design guides presentedat: http://www.cisco.com/en/US/netsol/ns656/networking_solutions_program_home.html. The design guides presented there describe deployment and implementation considerations for Cisco Unified CallManager, network infrastructure, and other related topics.

Figure 3-1 Typical Campus Network Infrastructure

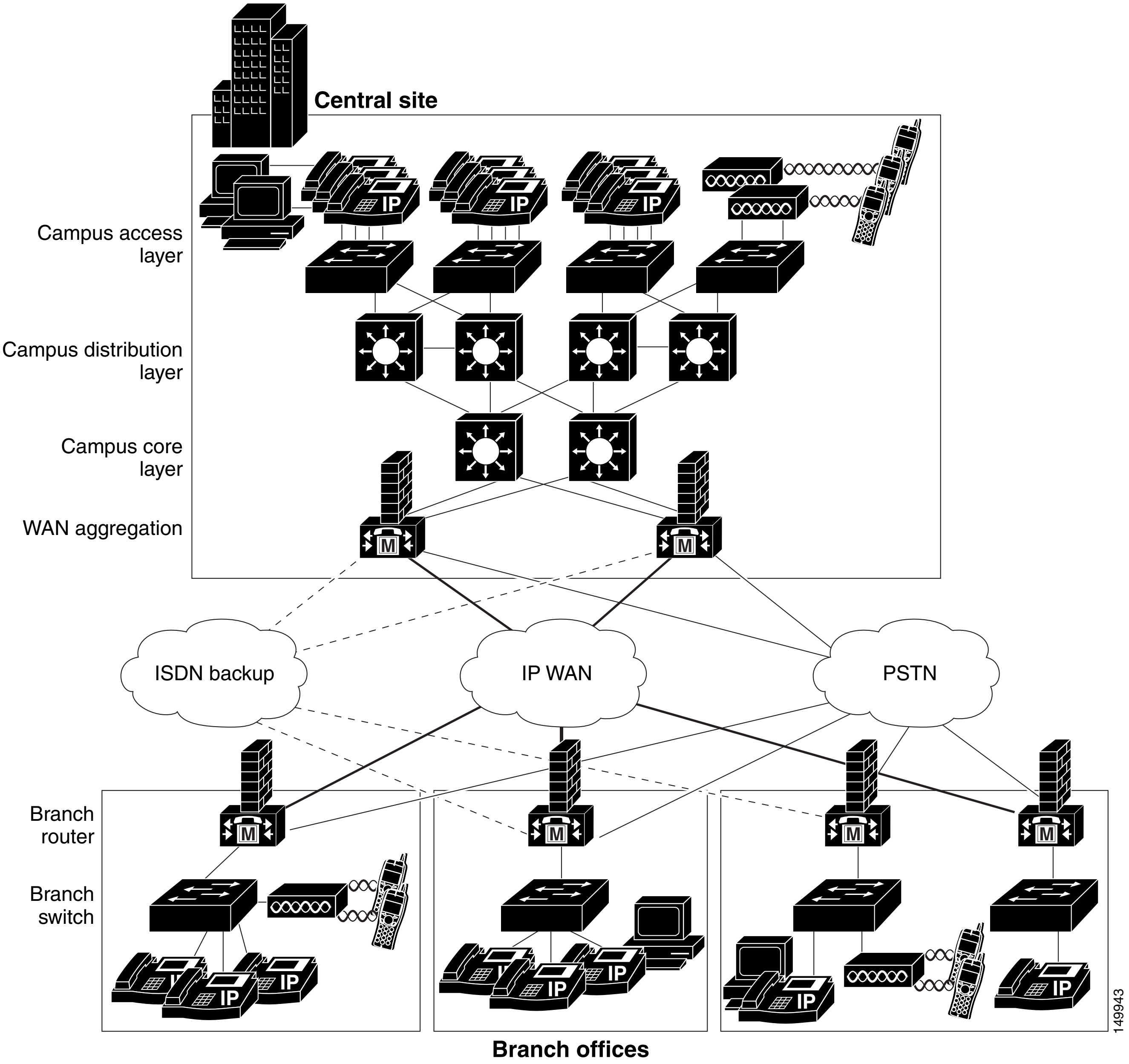

Central site
Campus access layer
Campus distribution layer
Campus core layer
WAN aggregation
ISDN backup
IP WAN
PSTN
Branch router
Branch switch
Branch offices
IP
M
149943

Table 3-1 Required Features for Each Role in the Network Infrastructure

Infrastructure Role	Required Features
Campus Access Switch	• In-Line Power • Multiple Queue Support • 802.1p and 802.1Q • Fast Link Convergence
Campus Distribution or Core Switch	• Multiple Queue Support • 802.1p and 802.1Q • Traffic Classification • Traffic Reclassification
WAN Aggregation Router (Site that is at the hub of the network)	• Multiple Queue Support • Traffic Shaping • Link Fragmentation and Interleaving (LFI) • Link Efficiency • Traffic Classification • Traffic Reclassification • 802.1p and 802.1Q
Branch Router (Spoke site)	• Multiple Queue Support • LFI • Link Efficiency • Traffic Classification • Traffic Reclassification • 802.1p and 802.1Q
Branch or Smaller Site Switch	• In-Line Power • Multiple Queue Support • 802.1p and 802.1Q

The following sections describe the network infrastructure features as they relate to:

- Cisco Unified CME Network Infrastructure Overview, page 3-4
- LAN Infrastructure, page 3-9
- WAN Infrastructure, page 3-20
- Wireless LAN Infrastructure, page 3-33

Note For additional information, see the "Related Documents and References" section on page xii.

Cisco Unified CME Network Infrastructure Overview

This publication focuses on two Cisco Unified CME implementations: standalone and multisite deployments. The general infrastructure considerations for networks supporting Cisco Unified CME are summarized in the following two sections:

- Standalone Network Infrastructure Overview, page 3-4
- Multisite Network Infrastructure Overview, page 3-6

Standalone Network Infrastructure Overview

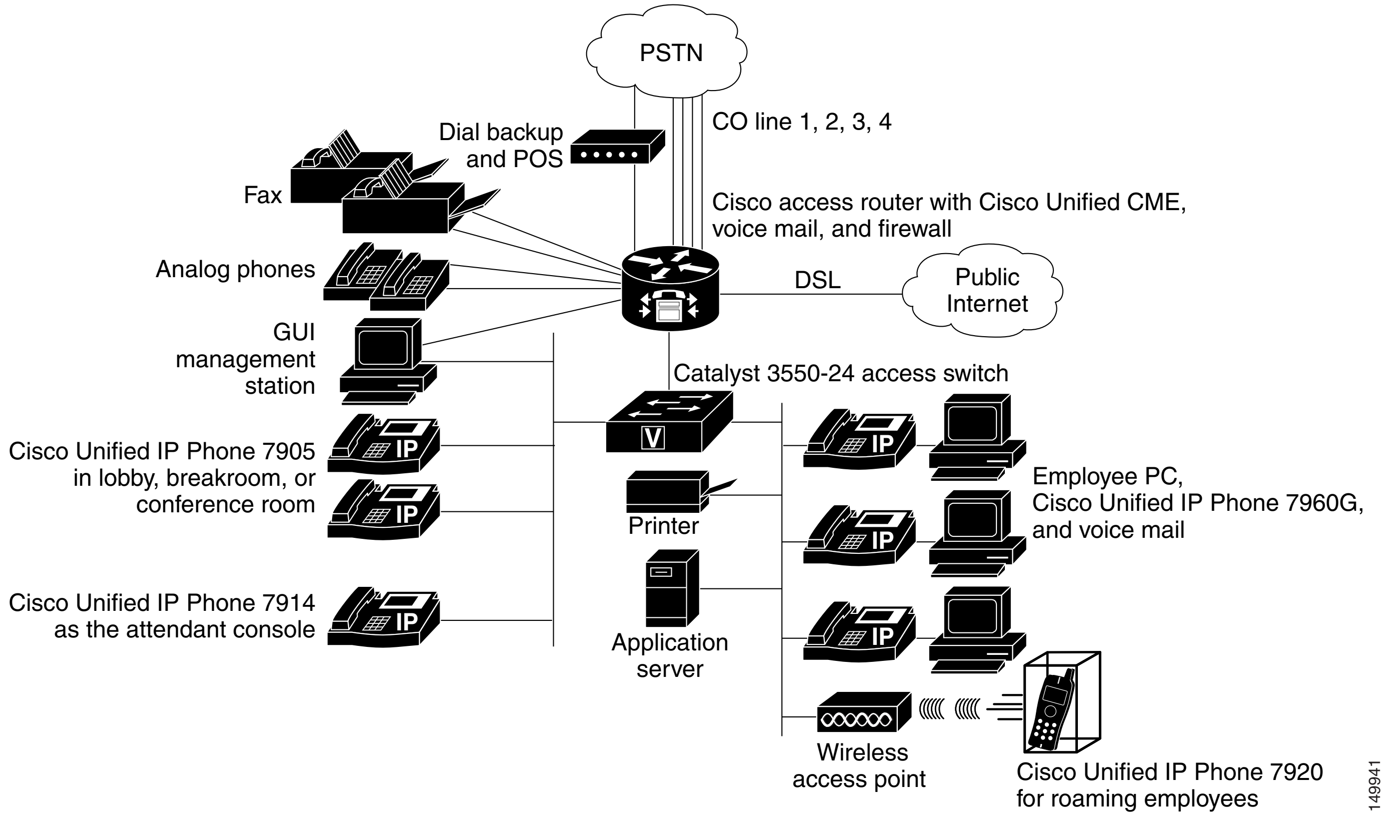
Cisco Unified CME is an excellent choice for a single-site, standalone office. In a world before IP telephony, such an office would have had an onsite router for data services and a separate key system or centrex for voice services. Now the router can be extended to provide converged data and voice services to the office. It also can be managed in the same way as before (either by an ISP or by a VAR or SI). Furthermore, both the business and the SP can realize cost, space, and management savings.

Savings just in wiring of a new office could be enough to make Cisco Unified CME cost-effective. Because the phones and computer equipment are all Ethernet-based, only Ethernet wiring is required in the office. Furthermore, only a single Ethernet wire or jack is required to each employee location or desktop. Computer equipment can be plugged into the back of the phone, and virtual LAN (VLAN) technology can be used to provide virtual separation (and therefore security) of voice from data traffic.

Leading-edge productivity features and improved customer service IP-based applications, such as XML services, can also be deployed easily over this converged infrastructure.

Figure 3-2 shows what such a single-site office's network might look like.

Figure 3-2 Standalone Office Network Topology


PSTN
CO line 1, 2, 3, 4
Dial backup and POS
Fax
Cisco access router with Cisco Unified CME, voice mail, and firewall
Analog phones
DSL
Public Internet
GUI management station
Catalyst 3550-24 access switch
Cisco Unified IP Phone 7905 in lobby, breakroom, or conference room
IP
V
Printer
Employee PC, Cisco Unified IP Phone 7960G, and voice mail
Application server
Cisco Unified IP Phone 7914 as the attendant console
Wireless access point
Cisco Unified IP Phone 7920 for roaming employees
149941

The network inFigure 3-2 has the following components:

- *Employee desktop*—Cisco 7960 IP Phones are provided for employees who work at a desk with a computer. The PC is connected via the phone's Ethernet switch. It also is connected via a single Ethernet cable to a LAN switch that provides inline power to the phones. In Figure 3-2, the LAN switch is a separate component, but a LAN switch that optionally provides inline power can also be integrated into the router chassis for offices requiring 50 or fewer LAN connections. The ability to connect computer equipment via the phone substantially reduces the overall number of switch ports required in the office. However, this might require that an existing LAN switch be upgraded to provide inline power for the IP phones. However, inline power is not a requirement for IPT deployments.
- *Internet connectivity*—This is provided via a DSL or a similar type of uplink to the local ISP, which also might host the company's e-mail services. For larger offices, DSL may not have sufficient bandwidth. Internet connectivity may then be deployed via fractional T1/E1 leased-line services, or even a grouping of multiple DSL or Basic Rate Interface (BRI) lines.
- *PSTN trunks*—These PSTN lines are analog Foreign Exchange Office (FXO) connections to the central office (CO). Each line carries a single incoming or outgoing phone call. Caller ID is typically delivered on such connections, but direct inward dial (DID) operation is not. A variation of this offering from the PSTN offers DID operation; this is technically known as analog DID service. It can have a different cost than the plain FXO service. The trunks can also be on a fractional T1/E1 or a full T1/E1 type of service that runs CAS or PRI services. Small businesses often prefer familiar key system operation. In this system, individual PSTN lines are mapped to buttons on the phones

labeled as Line1, Line2, Line3, and so on up to the number of lines coming in from the PSTN central office. (This arrangement is called key-system or square-keyswitch type of deployment.). These can also be used in the PBX-mode in which a user typically dials an access-code (like 9, commonly used in the US) for gain access to an outside PSTN line.

- *Attendant console*—Many small businesses with more than a handful of employees or considerable front-office customer interaction (such as a doctor's office) prefer that an attendant or receptionist answer incoming calls. Although these businesses might use an automated attendant (AA) for after-hours coverage, the typical preferred customer interaction during normal business hours is person-to-person. Attendant consoles can be a Cisco Unified IP Phone 7960 with one or two Cisco Unified IP Phone 7914s providing a total of 34 extensions that can be monitored. Attendant consoles can also be software based consoles from Cisco-certified third-party vendors.
- *Management station*—This is a web-based GUI management application for daily moves, adds, and changes to the system configuration. This can also be any one of the regular PCs used in the office. The only requirement is that it runs Internet Explorer Version 6 or later.
- *Other voice services*—One or more fax machines are used by almost every type of business. A small number of analog phones may also be used around the office, such as for emergency backup PSTN connectivity if power to the building fails.

Low-end IP phones, such as the Cisco Unified IP Phone 7902 or Cisco Unified IP Phone 7905, are scattered throughout the office in break rooms, health clinic exam rooms, lobbies, and perhaps conference rooms. These are often single-line phones that typically are not used to receive calls from the PSTN (they also do not have PC Ethernet ports). Instead, they are used for calls internal to the office or outgoing calls. Being IP phones, though, they participate in the intercom, paging, and display-based features often useful in a small office environment. Access to features, telephony interfaces, and calling plans can be controlled so that these phones are preventing from having access to outside lines.

The Cisco Unified IP Phone 7920 wireless phone can also be a great productivity enhancer for employees whose responsibilities demand both reachability and mobility, such as a retail floor supervisor, a warehouse supervisor, a bank branch manager, or a restaurant shift manager.

Note For information about wireless design for voice, see the *Cisco Wireless IP Phone 7920 Design and Deployment Guide* at the following location: http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html

However, system installation, initial setup and configuration, software upgrades, and turning on new services are most likely done by the SP or the SI or VAR from whom the system was purchased or leased. If any trouble is experienced, these organizations are responsible for isolating the problem and working with the system's vendor to correct system operation.

Multisite Network Infrastructure Overview

Use Cisco Unified CME there are less than 200 users (so there is some space for growth) and when a centralized provisioning model is not needed. Also Cisco Unified CallManager must be used when implementing certain third-party (and some Cisco) applications that use JTAPI as the control interface. The exact point where a centralized Cisco Unified CallManager starts to make more sense depends on

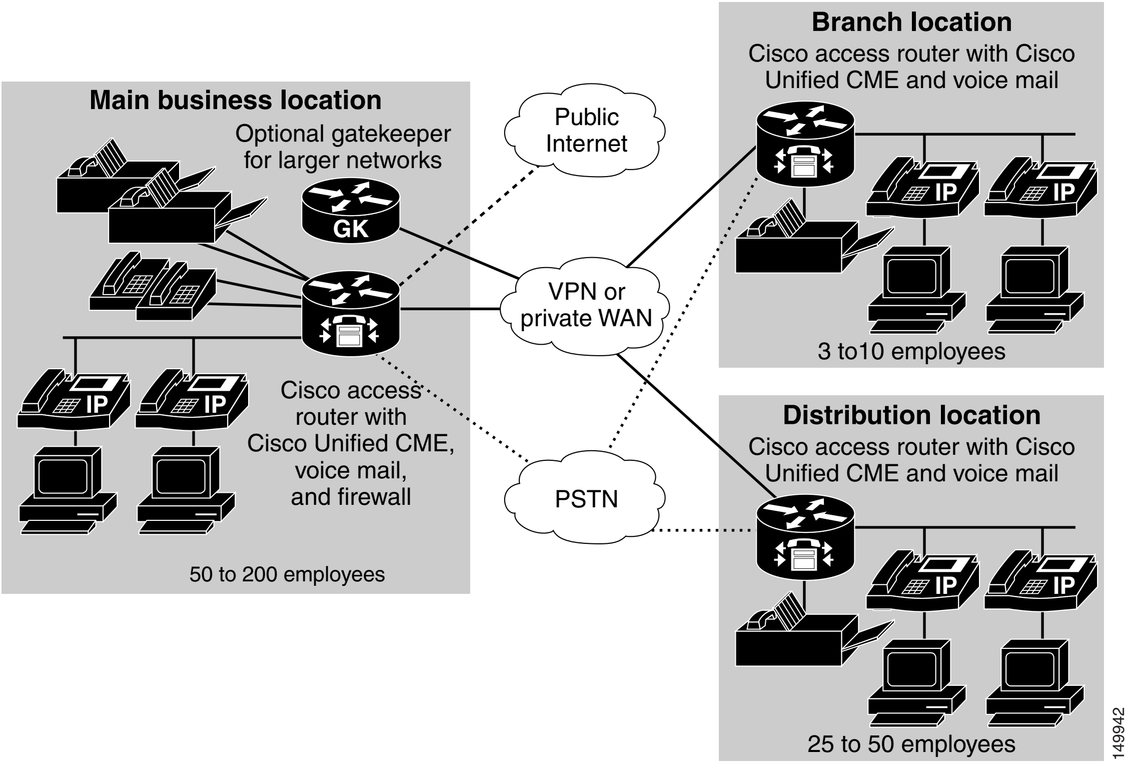
- The individual business
- Its management style
- The QoS readiness of the network between the sites

- The cost basis of the intersite connectivity
- How loosely or tightly coupled the sites are to one another in the normal course of a day's business

A PSTN-based network for voice access is generally recommended for a environment with a loosely coupled operational model and interconnected with only a minimal data network (bandwidth of less than 64 kbps and no QoS deployment). An example of such a business could be a restaurant chain. This network is essentially the same as the standalone model explored in the preceding section. Because the sites have only PSTN calling between them, no VoIP binds the sites together, and the network topology of each location would look like a standalone entity (from a voice traffic perspective). In contrast, a multisite enterprise model that is more tightly coupled (with access to inexpensive QoS) permits consideration of VoIP connectivity between the sites to gain toll savings and other management efficiency advantages. This basic premise of site coupling applies to both Cisco Unified CallManager and Cisco Unified CME solutions.

Figure 3-3 shows a sample network topology of what such an enterprise's branch office network might look like. This representation takes a general view of the branch office.

Figure 3-3 Multisite Distributed Cisco Unified CME Network Topology


Main business location
Optional gatekeeper for larger networks
GK
IP
IP
Cisco access router with Cisco Unified CME, voice mail, and firewall
50 to 200 employees
Public Internet
VPN or private WAN
PSTN
Branch location
Cisco access router with Cisco Unified CME and voice mail
IP
IP
3 to10 employees
Distribution location
Cisco access router with Cisco Unified CME and voice mail
IP
IP
25 to 50 employees
149942

There is significant similarity between the detailed layout of the small enterprise branch office and that of the standalone single-site office discussed earlier. The new or additional considerations are as follows:

- Employee desktop—Depending on the business the company conducts, the percentage of employee desktops varies. A retail organization has comparatively few desk-bound employees, whereas a bank or insurance company has a higher percentage. In each case, though, there is an employee who works on the floor or at a teller location, and these stations are often not equipped with individual phones or computers. Instead, shared resources are deployed for use by these employees. Personal calls are probably made from a public payphone in the break room or from a small number of phones set aside in a shared employee space that employees can access during their breaks.

Desk-bound employees tend to have voice mail, whereas the employees on the retail floor are much less likely to find voice mail productive for their work environment and responsibilities. Sometimes voice mail is still deployed for these employees (again, accessed from a common phone or break room) for human resources or training purposes.

WAN connectivity—The network between the sites is likely to be a private WAN of some type. It could also be a virtual private network (VPN) using the public Internet as the transport, but as such it is not QoS-enabled and, therefore, is not a good fit for deploying VoIP traffic.

A VoIP-capable WAN is most likely either privately owned or provided as a single service to all the sites of the enterprise by a SP. A VPN may still be used on top of the basic network service. Each site's connectivity depends on the site's geographic location and its bandwidth needs. It could be DSL, BRI, fractional T1/E1 access, or even metro-Ethernet. Larger offices may require a full T1/E1 or may bind together multiple DSL or BRI physical access lines to provide larger bandwidth.

- The U.S. offering of integrated access, encompassing both voice and data channels sharing the same physical T1, is a very attractive offering for this type of office. The voice (PSTN) connection could be either T1 in-band signaling (T1 Channel Associated Signaling [T1 CAS]) or fractional PRI. The data connection is most likely Frame Relay.
- PSTN connectivity—PSTN connectivity also depends on the office's size and location. It could be low-density analog (FXO or analog DID) or BRI connections or higher-density fractional T1/E1, perhaps with (fractional) Primary Rate Interface (PRI) service.

  The business model and size of the office dictate whether the office might prefer key system operation (Line1, Line2, and so on appear on the buttons of each phone) or PBX-like operation with typically a single extension per phone and DID service from the CO. Smaller offices more often tend to use key system (shared-line) operation, because that is the traditional voice system they were likely to have had installed before migrating to IP telephony. In larger offices, it becomes impractical to have a button appearance for each incoming CO trunk. These sites tend to be better candidates for DID service. A human or AA provides receptionist services for general incoming business calls and directs clients to the correct department or employee extension.
- Other voice services—When a small number of sites (such as five or fewer) are interconnected, the on-net dial plan is often simple enough to be implemented directly at each site. However, this meshing of sites becomes increasingly complex to manage as the number of sites increases. For this purpose, a gatekeeper (GK) is shown at the main site in Figure 2-5. For enterprises of approximately ten or more locations, centralizing the dial plan management is well worth considering. An H.323 GK is the way to accomplish this when multiple Cisco Unified CME sites are interconnected. This way, the dial plan is administered in a single location and is not duplicated at each site, making changes to the dial plan easy to accomplish.

LAN Infrastructure

LAN infrastructure design is extremely important for proper IP telephony operation on a converged network. Proper LAN infrastructure design requires following basic configuration and design best practices for deploying a highly available network. Further, proper LAN infrastructure design requires deploying end-to-end QoS on the network. The following sections discuss these requirements:

- LAN Design for High Availability, page 3-9
- Network Services, page 3-12
- Power over Ethernet (PoE), page 3-15
- Category 3 Cabling, page 3-16
- IBM Type 1A and 2A Cabling, page 3-16
- LAN Quality of Service (QoS), page 3-17

LAN Design for High Availability

Properly designing a LAN requires building a robust and redundant network from the top down. By structuring the LAN as a layered model (see Figure 3-1) and developing the LAN infrastructure one step of the model at a time, you can build a highly available, fault tolerant, and redundant network. Once these layers have been designed properly, you can add network services such as DHCP and TFTP to provide additional network functionality. The following sections examine the infrastructure layers and network services:

Note For more information on campus design, see the *Gigabit Campus Network Design* white paper at http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.pdf

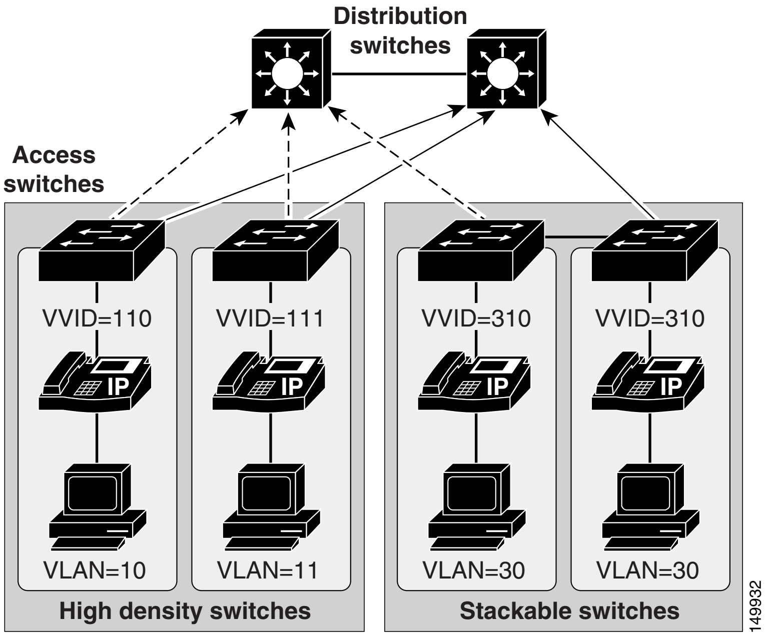
Campus Access Layer

The key layer to consider when implementing a network to support Cisco Unified CME is a the *access layer*. The access layer of the LAN includes the portion of the network from the desktop port(s) to the wiring closet switch.

Note For more information about large scale VoIP deployments, see the following document: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/4x/42nstrct.html#wp1043366

Proper access layer design starts with assigning a single IP subnet per virtual LAN (VLAN). Typically, a VLAN should not span multiple wiring closet switches; that is, a VLAN should have presence in one and only one access layer switch (see Figure 3-4). This practice eliminates topological loops at Layer 2, thus avoiding temporary flow interruptions due to Spanning Tree convergence. However, with the introduction of standards-based IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and 802.1s Multiple Instance Spanning Tree Protocol (MISTP), Spanning Tree can converge at much higher rates. In situations where RSTP and/or MISTP can and have been configured on the access layer switch, there is no need for concern about topological loops. More importantly, confining a VLAN to a single access layer switch also serves to limit the size of the broadcast domain. There is the potential for large numbers of devices within a single VLAN or broadcast domain to generate large amounts of broadcast traffic periodically, which can be problematic. A good rule is to limit the number of devices per VLAN to about 512, which is equivalent to two Class C subnets (that is, a 23-bit subnet masked Class C address). Typical access layer switches include the stackable Cisco Catalyst 2950, Cisco Catalyst 3500XL, Cisco Catalyst 3550, and Cisco Catalyst 3750, and also the larger, higher-density Catalyst 4000 and 6000 switches.

Figure 3-4 Access Layer Switches and VLANs for Voice and Data



When you deploy voice, we recommend that you enable two VLANs at the access layer: a native VLAN for data traffic (VLANs 10, 11, and 30 in Figure 3-4) and a voice VLAN under Cisco IOS software or Auxiliary VLAN under Catalyst Operating System for voice traffic (represented by VVIDs 110, 111, and 310 in Figure 3-4).

Note For implementations with 75 or fewer phones, the voice VLAN should be the same; the data VLAN should not unique for each switch. In the case of a smaller implementation, the VVID and VLAN should be the same.

We recommend separate voice and data VLANs the following reasons:

- Address space conservation and voice device protection from external networks

  Private addressing of phones on the voice or auxiliary VLAN ensures address conservation and ensures that phones are not accessible directly via public networks. PCs and servers are typically addressed with publicly routed subnet addresses; however, voice endpoints should be addressed using RFC 1918 private subnet addresses.

- QoS trust boundary extension to voice devices

  QoS trust boundaries can be extended to voice devices without extending these trust boundaries and, in turn, QoS features to PCs and other data devices.

- Protection from malicious network attacks

  VLAN access control, 802.1Q, and 802.1p tagging can provide protection for voice devices from malicious internal and external network attacks such as worms, denial of service (DoS) attacks, and attempts by data devices to gain access to priority queues via packet tagging.

- Ease of management and configuration

  Separate VLANs for voice and data devices at the access layer provide ease of management and simplified QoS configuration.

To provide high-quality voice and to take advantage of the full voice feature set, access layer switches should provide support for:

- 802.1Q trunking and 802.1p for proper treatment of Layer 2 CoS packet marking on ports with phones connected
- Multiple egress queues to provide priority queuing of RTP voice packet streams
- The ability to classify or reclassify traffic and establish a network trust boundary
- Inline power capability (Although inline power capability is not mandatory, we highly recommend for the access layer switches.)
- Layer 3 awareness and the ability to implement QoS access control lists (These features are required if you are using certain IP telephony endpoints, such as a PC running a softphone application, that cannot benefit from an extended trust boundary.)

Spanning Tree Protocol (STP)

To minimize convergence times and maximize fault tolerance at Layer 2, enable the following STP features:

- PortFast

  Enable PortFast on all access ports. The phones, PCs, or servers connected to these ports do not forward bridge protocol data units (BPDUs) that could affect STP operation. PortFast ensures that the phone or PC, when connected to the port, is able to begin receiving and transmitting traffic immediately without having to wait for STP to converge.

- Root guard or BPDU guard

  Enable root guard or BPDU guard on all access ports to prevent the introduction of a rogue switch that might attempt to become the Spanning Tree root, thereby causing STP re-convergence events and potentially interrupting network traffic flows. Ports that are set to **errdisable** state by BPDU guard must either be re-enabled manually or the switch must be configured to re-enable ports automatically from the errdisable state after a configured period of time.

- UplinkFast and BackboneFast

  Enable these features where appropriate to ensure that, when changes occur on the Layer 2 network, STP converges as rapidly as possible to provide high availability. When using stackable switches such as the Cisco Catalyst 2950, Cisco Catalyst 3550, or Cisco Catalyst 3750, enable Cross-Stack UplinkFast (CSUF) to provide fast failover and convergence if a switch in the stack fails.

- UniDirectional Link Detection (UDLD)

  Enable this feature to reduce convergence and downtime on the network when link failures or misbehaviors occur, thus ensuring minimal interruption of network service. UDLD detects, and takes out of service, links where traffic is flowing in only one direction. This feature prevents defective links from being mistakenly considered as part of the network topology by the Spanning Tree and routing protocols.

Note With the introduction of RSTP 802.1w, features such as PortFast and UplinkFast are not required because these mechanisms are built in to this standard. If RSTP has been enabled on the Catalyst switch, these commands are not necessary.

Network Services

Once a highly available, fault-tolerant, multi-layer campus network has been built, network services such as DNS, DHCP, TFTP, and NTP can be deployed. These topics are addressed in the following individual sections:

- Domain Name System (DNS), page 3-12
- Dynamic Host Configuration Protocol (DHCP), page 3-12
- Trivial File Transfer Protocol (TFTP), page 3-14
- Network Time Protocol (NTP), page 3-14

Domain Name System (DNS)

DNS enables the mapping of host names to IP addresses within a network or networks. DNS server(s) deployed within a network provide a database that maps hostnames to IP addresses. Devices on the network can query the DNS server and receive IP addresses for other devices in the network, thereby facilitating communication between network devices.

Relying on DNS, however, can be problematic. If the DNS server becomes unavailable and a network device is relying on that server to provide a hostname-to-IP-address mapping, communication can and will fail. For this reason, do not rely on DNS for communication between Cisco Unified CME and the IP telephony endpoints.

Configure Cisco Unified CME systems, gateways, and endpoint devices to use IP addresses rather than hostnames. We do *not* recommend configuration of DNS parameters such as DNS server addresses, hostnames, and domain names. If you eliminate DNS configuration within the IP telephony network, telephony devices and applications do not have to rely on the DNS server.

Dynamic Host Configuration Protocol (DHCP)

DHCP is used by hosts on the network to get initial configuration information, including IP address, subnet mask, default gateway, and TFTP server. DHCP eases the administrative burden of manually configuring each host with an IP address and other configuration information. DHCP also provides automatic reconfiguration of network configuration when devices are moved between subnets. The configuration information is provided by a DHCP server located in the network, which responds to DHCP requests from DHCP-capable clients.

You should configure IP telephony endpoints to use DHCP to simplify deployment of these devices. Any RFC 2131 compliant DHCP server can be used to provide configuration information to IP telephony network devices. When deploying IP telephony devices in an existing data-only network, all you have to do is add DHCP voice scopes to an existing DHCP server for these new voice devices. Because IP telephony devices are configured to use and rely on a DHCP server for IP configuration information, you must deploy DHCP servers in a redundant fashion. At least two DHCP servers should be deployed within the telephony network such that, if one of the servers fails, the other can continue to answer DHCP client requests. You should also ensure that DHCP server(s) are configured with enough IP subnet addresses to handle all DHCP-reliant clients within the network.

Note The preceding information applies to large-scale networks. For most Cisco Unified CME deployments, the Cisco IOS router running Cisco Unified CME can also be the DHCP server.

DHCP Option 150

IP telephony endpoints can be configured to rely on DHCP Option 150 to identify the source of telephony configuration information, available from a server running the Trivial File Transfer Protocol (TFTP).

In the simplest configuration, where a single TFTP server is offering service to all deployed endpoints, Option 150 is delivered as a single IP address pointing to the system's designated TFTP server.

We highly recommend using a direct IP address (that is, not relying on a DNS service) for Option 150 because doing so eliminates dependencies on DNS service availability during the phone boot-up and registration process.

DHCP Lease Times

Configure DHCP lease times as appropriate for the network environment. Given a fairly static network in which PCs and telephony devices remain in the same place for long periods of time, we recommend longer DHCP lease times (for example, one week). Shorter lease times require more frequent renewal of the DHCP configuration and increase the amount of DHCP traffic on the network. Conversely, networks that incorporate large numbers of mobile devices, such as laptops and wireless telephony devices, should be configured with shorter DHCP lease times (for example, one day) to prevent depletion of DHCP-managed subnet addresses. Mobile devices typically use IP addresses for short increments of time and then might not request a DHCP renewal or new address for a long period of time. Longer lease times will tie up these IP addresses and prevent them from being reassigned even when they are no longer being used.

Cisco Unified IP Phones adhere to the conditions of the DHCP lease duration as specified in the DHCP server's scope configuration. Once half the lease time has expired since the last successful DHCP server Acknowledgment, the IP phone will request a lease renewal. This DHCP client Request, acknowledged by the DHCP server, will allow the IP phone to retain use of the IP scope (that is, the IP address, default gateway, subnet mask, DNS server (optional), and TFTP server (optional)) for another lease period. If the DHCP server becomes unavailable, an IP phone will not be able to renew its DHCP lease, and as soon as the lease expires, it will relinquish its IP configuration and will thus become unregistered from Cisco CallManager until a DHCP server can grant it another valid scope.

DHCP Network Deployments

There are two options for deploying DHCP functionality within an IP telephony network

- Centralized DHCP Server

  Typically, for a single-site campus IP telephony deployment, the DHCP server should be installed at a central location within the campus. As mentioned previously, redundant DHCP servers should be deployed. If the IP telephony deployment also incorporates remote branch telephony sites, as in a centralized multi-site Cisco CallManager deployment, a centralized server can be used to provide DHCP service to devices in the remote sites. This type of deployment requires that you configure the **ip helper-address** on the branch router interface. If redundant DHCP servers are deployed at the central site, both servers' IP addresses must be configured as **ip helper-address**. Also note that, if branch-side telephony devices rely on a centralized DHCP server and the WAN link between the two sites fails, devices at the branch site will be unable to send DHCP requests or receive DHCP responses.

Note By default, **service dhcp** is enabled on the Cisco IOS device and does not appear in the configuration. Do not disable this service on the branch router because doing so will disable the DHCP relay agent on the device, and the **ip helper-address** configuration command will not work.

- Centralized DHCP Server and Remote Site Cisco IOS DHCP Server

  When configuring DHCP for use in a centralized multi-site Cisco Unified CME deployment, you can use a centralized DHCP server to provide DHCP service to centrally located devices. Remote devices could receive DHCP service from a locally installed server or from the Cisco IOS router at the remote site. This type of deployment ensures that DHCP services are available to remote telephony devices even during WAN failures. The following example lists the basic Cisco IOS DHCP server configuration commands.

```
service dhcp                              ! Activate DHCP Service on the IOS Device

ip dhcp excluded-address <ip-address>|<ip-address-low> <ip-address-high>
                                          !  Specify an IP Address or IP Address Range to
                                          !  be excluded from the DHCP pool

ip dhcp pool <dhcp-pool name>             ! Specify DHCP pool name
   network <ip-subnet> <mask>             ! Specify DHCP pool IP subnet and mask
   default-router <default-gateway-ip>    ! Specify the Default-gateway
   option 150 ip <tftp-server-ip-1> ...   ! Specify TFTP servers (up to four) -
                                          ! IP phones use only the first two addresses in
                                          ! the array.
```

Trivial File Transfer Protocol (TFTP)

Within a Cisco Unified CME system, endpoints (such as IP phones running the SCCP protocol) rely on a TFTP-based process to acquire configuration information. The endpoints request a configuration file whose name is based on the requester's MAC address (for example, for an IP phone with MAC address ABCDEF123456, the filename would be SEPABCDEF123456.cnf.xml). The configuration file includes the version of software that the phone must run and a list of Cisco Unified CME servers that the phone should register with.

If the configuration file instructs the phone to run a software file other than the one it currently uses, the phone will request the new version of software from the TFTP server. The phone goes through this process once per reboot of the phone or router, before registering.

Centralized call processing deployments require remote phones to download configuration files and phone software through the branch's WAN link. When scheduled maintenance involves the downloading of new software, download times are a function of the number of phones requiring upgrades, the file size, and the WAN link's bandwidth and traffic utilization.

Network Time Protocol (NTP)

NTP allows network devices to synchronize their clocks to a network time server or network-capable clock. NTP is critical for ensuring that all devices in a network have the same time. When troubleshooting or managing a telephony network, it is crucial to synchronize the time stamps within all error and security logs, traces, and system reports on devices throughout the network. This synchronization enables administrators to recreate network activities and behaviors based on a common timeline. Billing records and call detail records (CDRs) also require accurate synchronized time.

Cisco Unified CME NTP Time Synchronization

Time synchronization is especially critical on Cisco Unified CME devices. Configure automatic NTP time synchronization on all Cisco Unified CME servers within the network.

Cisco IOS and Catalyst Operating System NTP Time Synchronization

Time synchronization is also important for other devices within the network. Cisco IOS routers and Catalyst switches should be configured to synchronize their time with the rest of the network devices via NTP. This is critical for ensuring that debug, syslog, and console log messages are time-stamped appropriately. Troubleshooting telephony network issues is simplified when a clear timeline can be drawn for events that occur on devices throughout the network.

The following example illustrates the configuration of NTP time synchronization on Cisco IOS and Catalyst Operating System devices.

Cisco IOS software configuration:

```
ntp server 64.100.21.254
```

Catalyst Operating System configuration:

```
set ntp server 64.100.21.254
set ntp client enable
```

To ensure proper NTP time synchronization on routers and switches, it may be necessary to configure time zones using the **clock timezone** command (in Cisco IOS software) and/or **set timezone** command (in Catalyst Operating System).

When an external connection to an NTP server is not available, Cisco IOS software can be used as a reference server for other devices so that all devices including phones use the same time reference. This can be done by using the global Cisco IOS software **ntp master** command in configuration mode. Also set the clock and time zone on the router.

Power over Ethernet (PoE)

PoE (or inline power) is 48 Volt DC power provided over standard Ethernet unshielded twisted-pair (UTP) cable. Instead of using wall power, IP phones and other inline powered devices (PDs) such as the Aironet Wireless Access Points can receive power provided by inline power-capable Catalyst Ethernet switches or other inline power source equipment (PSE). Inline power is enabled by default on all inline power-capable Catalyst switches.

Deploying inline power-capable switches with uninterruptable power supplies (UPS) ensures that IP phones continue to receive power during power failure situations. Provided the rest of the telephony network is available during these periods of power failure, then IP phones should be able to continue making and receiving calls. You should deploy inline power-capable switches at the campus access layer within wiring closets to provide inline-powered Ethernet ports for IP phones, thus eliminating the need for wall power.

Cisco PoE is delivered on the same wire pairs used for data connectivity (pins 1, 2, 3, and 6). If existing access switch ports are not capable of inline power, you can use a power patch panel to inject power into the cabling. (In this case pins 4, 5, 7, and 8 are used.) Additionally, power injectors may be used for specific deployment needs.

Caution The use of power injectors or power patch panels can damage some devices because power is always applied to the Ethernet pairs. PoE switch ports automatically detect the presence of a device that requires PoE before enabling it on a port-by-port basis.

In addition to Cisco PoE inline power, we now support the IEEE 802.3af PoE standard. Not all access switches and phones comply with 802.3af. The Cisco Catalyst 6500, Cisco Catalyst 4500, and Cisco Catalyst 3750 are capable of supporting 802.3af. For information about which Cisco Unified IP Phones support the 802.3af PoE standard, see the information regarding PoE switches provided at the following:

Category 3 Cabling

The use of Category 3 cabling is supported for IP Communications under the following conditions:

- Phones with a PC port and a PC attached to it (Cisco Unified IP Phone 7970, Cisco Unified IP Phone 7960, Cisco Unified IP Phone 7940, and Cisco Unified IP Phone 7910+SW) should be set to 10 Mbps, full-duplex.

  This setting requires hard-coding the upstream switch port, the phone switch and PC ports, and the PC NIC port to 10 Mbps, full-duplex. No ports should be set to AUTO negotiate. If desired, you can hard-code the phone's PC port to 10 Mbps half-duplex, thereby forcing the PC's NIC to negotiate to 10 Mbps half-duplex (assuming the PC's NIC is configured to AUTO negotiate). This configuration is acceptable as long as the uplink between the phone and the upstream switch port is set to 10 Mbps full-duplex.

- Phones with no PC ports and with 10 Mbps switch ports (Cisco Unified IP Phone 7902, Cisco Unified IP Phone 7905, and Cisco Unified IP Phone 7910 IP Phones) should be allowed to auto-negotiate to 10 Mbps, half-duplex.

  Because these phones support only 10 Mbps Ethernet and their ports cannot be manually configured, the upstream switch port should be set to either AUTO negotiate or 10 Mbps, half-duplex. In both cases, these phones will negotiate to 10 Mbps, half-duplex.

- Phones with a PC port but no PC attached to it (Cisco Unified IP Phone 7970, Cisco Unified IP Phone 7960, Cisco Unified IP Phone 7940, Cisco Unified IP Phone 7910+SW, and Cisco Unified IP Phone 7912) can be allowed to negotiate to 10 Mbps, half-duplex.

  If you leave these phones with the default switch port configuration of AUTO negotiate and configure the upstream switch port to 10 Mbps, half-duplex, these phones will revert to 10 Mbps, half-duplex.

Note The Cisco Unified IP Phone 7912 IP Phone should not be used with Category 3 cable when a PC is attached because the switch and PC ports on this phone cannot be forced to 10 Mbps, full duplex.

IBM Type 1A and 2A Cabling

The use of IBM Cabling System (ICS) or Token Ring shielded twisted-pair type 1A or 2A cabling is supported for IP Communications under the following conditions:

- Cable lengths should be 100 meters or less.
- Adapters without impedance matching should be used for converting from universal data connector (UDC) to RJ-45 Ethernet standard.

Note There are only two twisted pairs in the Token Ring cables. Therefore, inline power for IP phones can be supported, but mid-span power insertion cannot (with Cisco Inline Power and 802.3af) because it requires more than two pairs.

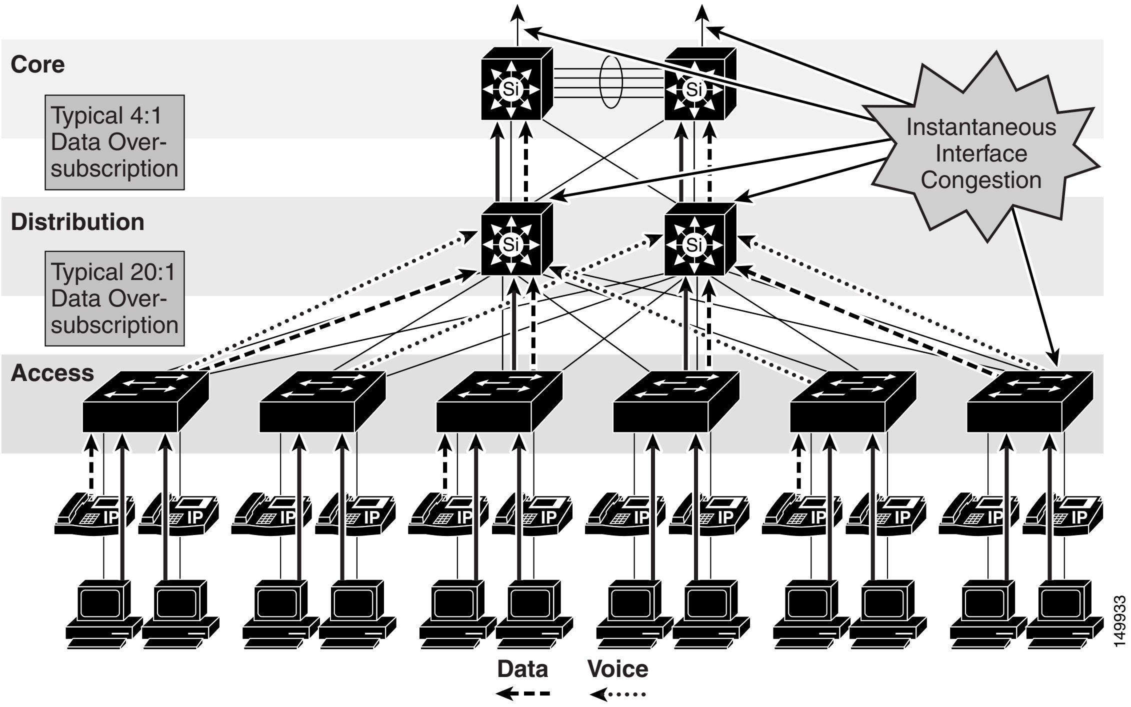
Running data over the network is not always a sufficient test of the quality of the cable plant because some non-compliance issues might not be apparent. Therefore, customers might want to perform a cable plant survey to verify that their type 1A and 2A cabling installation is compliant with Ethernet standards.

LAN Quality of Service (QoS)

Until recently, quality of service was not an issue in the enterprise campus because of the asynchronous nature of data traffic and the ability of network devices to tolerate buffer overflow and packet loss. However, with new applications such as voice and video, which are sensitive to packet loss and delay, buffers and not bandwidth are the key QoS issue in the enterprise campus.

Figure 3-5 illustrates the typical oversubscription that occurs in LAN infrastructures.

Figure 3-5 Data Traffic Oversubscription in the LAN


Core
Typical 4:1 Data Over-subscription
Distribution
Typical 20:1 Data Over-subscription
Access
Si
Si
Si
Si
Instantaneous Interface Congestion
IP
Data
Voice
149933

This oversubscription, coupled with individual traffic volumes and the cumulative effects of multiple independent traffic sources, can result in the egress interface buffers becoming full instantaneously, thus causing additional packets to drop when they attempt to enter the egress buffer. The fact that campus switches use hardware-based buffers, which compared to the interface speed are much smaller than those found on WAN interfaces in routers, merely increases the potential for even short-lived traffic bursts to cause buffer overflow and dropped packets.

Applications such as file sharing (both peer-to-peer and server-based), remote networked storage, network-based backup software, and emails with large attachments, can create conditions where network congestion occurs more frequently and/or for longer durations. Some of the negative effects of recent worm attacks have been an overwhelming volume of network traffic (both unicast and broadcast-storm based), increasing network congestion. If no buffer management policy is in place, loss, delay, and jitter performance of the LAN may be affected for all traffic.

Another situation to consider is the effect of failures of redundant network elements, which cause topology changes. For example, if a distribution switch fails, all traffic flows will be reestablished through the remaining distribution switch. Prior to the failure, the load balancing design shared the load between two switches, but after the failure all flows are concentrated in a single switch, potentially causing egress buffer conditions that normally would not be present.

For applications such as voice, this packet loss and delay results in severe voice quality degradation. Therefore, QoS tools are required to manage these buffers and to minimize packet loss, delay, and delay variation (jitter).

The following types of QoS tools are needed from end to end on the network to manage traffic and ensure voice quality:

- Traffic classification

  Classification involves the marking of packets with a specific priority denoting a requirement for class of service (CoS) from the network. The point at which these packet markings are trusted or not trusted is considered the trust boundary. Trust is typically extended to voice devices (phones) and not to data devices (PCs).

- Queuing or scheduling

  Interface queuing or scheduling involves assigning packets to one of several queues based on classification for expedited treatment throughout the network.

- Bandwidth provisioning

  Provisioning involves accurately calculating the required bandwidth for all applications plus element overhead.

The following sections discuss the use of these QoS mechanisms in a campus environment:

- Traffic Classification, page 3-18
- Interface Queuing, page 3-19
- Bandwidth Provisioning, page 3-19
- Impairments to IP Communications if QoS is Not Employed, page 3-20

Traffic Classification

It has always been an integral part of the Cisco network design architecture to classify or mark traffic as close to the edge of the network as possible. Traffic classification is an entrance criterion for access into the various queuing schemes used within the campus switches and WAN interfaces. The IP phone marks its voice control signaling and voice RTP streams at the source, and it adheres to the values presented in Table 3-2. As such, the IP phone can and should classify traffic flows.

Table 3-2 lists the traffic classification requirements for the LAN infrastructure.

Table 3-2 Traffic Classification Guidelines for Various Types of Network Traffic

Traffic Type	Layer 2 Class of Service (CoS)	Layer 3 IP Precedence	Layer 3 Differentiated Services Code Point (DSCP)	Layer 3 Per-Hop Behavior (PHB)
Voice Real-Time Transport Protocol (RTP)	5	5	46	EF
Voice control signaling[1]	3	3	24	CS3
Video conferencing	4	4	34	AF41
Data	0, 1, 2	0, 1, 2	10 to 22	BE to AF23

[1] The recommended DSCP/PHB marking for voice control signaling traffic has been changed from 26/AF31 to 24/CS3. A marking migration is planned within Cisco to reflect this change, however many products still mark signaling traffic as 26/AF31. Therefore, in the interim, we recommend that both AF31 and CS3 be reserved for call signaling.

Interface Queuing

After packets have been marked with the appropriate tag at Layer 2 (CoS) and Layer 3 (DSCP or PHB), it is important to configure the network to schedule or queue traffic based on this classification, so as to provide each class of traffic with the service it needs from the network. By enabling QoS on campus switches, you can configure all voice traffic to use separate queues, thus virtually eliminating the possibility of dropped voice packets when an interface buffer fills instantaneously.

Although network management tools may show that the campus network is not congested, QoS tools are still required to guarantee voice quality. Network management tools show only the average congestion over a sample time span. While useful, this average does not show the congestion peaks on a campus interface.

Transmit interface buffers within a campus tend to congest in small, finite intervals as a result of the bursty nature of network traffic. When this congestion occurs, any packets destined for that transmit interface are dropped. The only way to prevent dropped voice traffic is to configure multiple queues on campus switches. For this reason, we recommend always using a switch that has at least two output queues on each port and the ability to send packets to these queues based on QoS Layer 2 and/or Layer 3 classification. Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco Catalyst 3750, Cisco Catalyst 35XX, and Cisco Catalyst 2950 switches all support two or more output queues per port.

Bandwidth Provisioning

In the campus LAN, bandwidth provisioning recommendations can be summarized by the motto, *Over provision and under subscribe*. This motto implies careful planning of the LAN infrastructure so that the available bandwidth is always considerably higher than the load and there is no steady-state congestion over the LAN links.

The addition of voice traffic onto a converged network does not represent a significant increase in overall network traffic load; the bandwidth provisioning is still driven by the demands of the data traffic requirements. The design goal is to avoid extensive data traffic congestion on any link that will be traversed by telephony signaling or media flows. Contrasting the bandwidth requirements of a single G.711 voice call (approximately 86 kbps) to the raw bandwidth of a FastEthernet link (100 Mbps) indicates that voice is not a source of traffic that causes network congestion in the LAN, but rather it is a traffic flow to be protected from LAN network congestion.

Impairments to IP Communications if QoS is Not Employed

If QoS is not deployed, packet drops and excessive delay and jitter can occur, leading to impairments of the telephony services. When media packets are subjected to drops, delay, and jitter, the user-perceivable effects include clicking sound, harsh-sounding voice, extended periods of silence, and echo.

When signaling packets are subjected to the same conditions, user-perceivable impairments include unresponsiveness to user input (such as delay to dial tone), continued ringing upon answer, and double dialing of digits due to the user's belief that the first attempt was not effective (thus requiring hang-up and redial). More extreme cases can include endpoint re-initialization, call termination, and the spurious activation of Cisco SRST functionality at branch offices (leading to interruption of gateway calls).

These effects apply to all deployment models. However, single-site (campus) deployments tend to be less likely to experience the conditions caused by sustained link interruptions because the larger quantity of bandwidth typically deployed in LAN environments (minimum links of 100 Mbps) allows for some residual bandwidth to be available for the IP Communications system.

In any WAN-based deployment model, traffic congestion is more likely to produce sustained and/or more frequent link interruptions because the available bandwidth is much less than in a LAN (typically less than 2 Mbps), so the link is more easily saturated. The effects of link interruptions impact the users, whether or not the voice media traverses the packet network.

WAN Infrastructure

Proper WAN infrastructure design is important for proper IP telephony operation on a converged network with two or more Cisco Unified CME systems or Cisco Unified CME systems along with Cisco Unified CallManager systems. If VoIP calls are exchanged between sites, WAN considerations are important.

Proper infrastructure design requires following basic configuration and design best practices for deploying a WAN that is as highly available as possible and that provides guaranteed throughput. Furthermore, proper WAN infrastructure design requires deploying end-to-end QoS on all WAN links. The following sections discuss these requirements:

- WAN Design and Configuration Best Practices, page 3-20
- WAN Quality of Service (QoS), page 3-22

WAN Design and Configuration Best Practices

Properly designing a WAN requires building fault-tolerant network links and planning for the possibility that these links might become unavailable. By carefully choosing WAN topologies, provisioning the required bandwidth, and approaching the WAN infrastructure as another layer in the network topology, you can build a fault-tolerant and redundant network. The following sections examine the required infrastructure layers and network services:

- Deployment Considerations, page 3-21
- Guaranteed Bandwidth, page 3-21
- Best-Effort Bandwidth, page 3-22

Deployment Considerations

WAN deployments for voice networks must follow a hub-and-spoke topology, with a central hub site and multiple remote spoke sites connected into the central hub site. In this scenario, each remote or spoke site is one WAN link hop away from the central or hub site and two WAN link hops away from all other spoke sites.

WAN links should, when possible, be made redundant to provide higher levels of fault-tolerance. Redundant WAN links provided by different service providers or located in different physical ingress/egress points within the network can ensure backup bandwidth and connectivity in the event that a single link fails. In non-failure scenarios, these redundant links may be used to provide additional bandwidth and offer load balancing of traffic on a per-flow basis over multiple paths and equipment within the WAN.

Voice and data should remain converged at the WAN, just as they are converged at the LAN. QoS provisioning and queuing mechanisms are typically available in a WAN environment to ensure that voice and data can interoperate on the same WAN links. Attempts to separate and forward voice and data over different links can be problematic in many instances because the failure of one link typically forces all traffic over a single link, thus diminishing throughput for each type of traffic and in most cases reducing the quality of voice. Furthermore, maintaining separate network links or devices makes troubleshooting and management difficult at best.

When deploying voice in a WAN environment, we recommend that you use the lower-bandwidth G.729 codec for any voice calls that will traverse WAN links because this practice will provide bandwidth savings on these lower-speed links. Furthermore, media resources such as MoH should be configured to use multicast transport mechanism when possible because this practice will provide additional bandwidth savings.

Finally, recommendation G.114 of the International Telecommunication Union (ITU) states that the one-way delay in a voice network should be less than or equal to 150 milliseconds. It is important to keep this in mind when implementing low-speed WAN links within a network. Topologies, technologies, and physical distance should be considered for WAN links so that one-way delay is kept at or below this 150-millisecond recommendation.

Guaranteed Bandwidth

Because voice is typically deemed a critical network application, it is imperative that bearer and signaling voice traffic always reaches its destination. For this reason, it is important to choose a WAN topology and link type that can provide guaranteed dedicated bandwidth. The following WAN link technologies can provide guaranteed dedicated bandwidth:

- Leased Lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- ATM-to-Frame Relay Service Interworking
- Multiprotocol Label Switching (MPLS)
- Cisco Voice and Video Enabled IP Security VPN (IP Sec V3PN)

These link technologies, when deployed in a dedicated fashion or when deployed in a private network, can provide guaranteed traffic throughput. All of these WAN link technologies can be provisioned at specific speeds or bandwidth sizes. In addition, these link technologies have built-in mechanisms that help guarantee throughput of network traffic even at low link speeds. Features such as traffic shaping, fragmentation and packet interleaving, and committed information rates (CIR) can help ensure that packets are not dropped in the WAN, that all packets are given access at regular intervals to the WAN link, and that enough bandwidth is available for all network traffic attempting to traverse these links.

Best-Effort Bandwidth

There are some WAN topologies that are unable to provide guaranteed dedicated bandwidth to ensure that network traffic will reach its destination, even when that traffic is critical. These topologies are extremely problematic for voice traffic, not only because they provide no mechanisms to provision guaranteed network throughput, but also because they provide no traffic shaping, packet fragmentation and interleaving, queuing mechanisms, or end-to-end QoS to ensure that critical traffic such as voice will be given preferential treatment.

The following WAN network topologies and link types are examples of best-effort bandwidth technology:

- The Internet
- DSL
- Cable
- Satellite
- Wireless

In most cases, these link types can provide the guaranteed network connectivity and bandwidth required for critical voice and voice applications. However, these technologies might be suitable for personal or telecommuter-type network deployments. At times, these topologies can provide highly available network connectivity and adequate network throughput; but at other times, these topologies can become unavailable for extended periods of time, can be throttled to speeds that render network throughput unacceptable for real-time applications such as voice, or can cause extensive packet losses and require repeated retransmissions. In other words, these links and topologies are unable to provide guaranteed bandwidth, and when traffic is sent on these links, it is sent best-effort with no guarantee that it will reach its destination. For this reason, we recommend that you do *not* use best-effort WAN topologies for voice-enabled networks that require enterprise-class voice services and quality.

Note There are some new QoS mechanisms for DSL and cable technologies that can provide guaranteed bandwidth; however, these mechanisms are not typically deployed by service providers, and these services are still significantly oversubscribed.

WAN Quality of Service (QoS)

Before placing voice and video traffic on a network, it is important to ensure that there is adequate bandwidth for all required applications. After this bandwidth has been provisioned, voice priority queuing must be performed on all interfaces. This queuing is required to reduce jitter and possible packet loss if a burst of traffic oversubscribes a buffer. This queuing requirement is similar to the one for the LAN infrastructure.

Next, the WAN typically requires additional mechanisms such as traffic shaping to ensure that WAN links are not sent more traffic than they can handle, which could cause dropped packets.

Finally, link efficiency techniques can be applied to WAN paths. For example, link fragmentation and interleaving (LFI) can be used to prevent small voice packets from being queued behind large data packets, which could lead to unacceptable delays on low-speed links.

The goal of these QoS mechanisms is to ensure reliable, high-quality voice by reducing delay, packet loss, and jitter for the voice traffic. Table 3-3 lists the QoS features and tools required for the WAN infrastructure to achieve this goal.

Table 3-3 QoS Features and Tools Required to Support IP Telephony for each WAN Technology and Link Speed

WAN Technology	Link Speed: 56-to-768 kbps	Link Speed: Greater than 768 kbps
Leased Lines	• Multilink Point-to-Point Protocol (MLP) • MLP Link Fragmentation and Interleaving (LFI) • Low Latency Queuing (LLQ) • Optional: Compressed Real-Time Transport Protocol (cRTP)	• LLQ
Frame Relay	• Traffic Shaping • LFI (FRF.12) • LLQ • Optional: cRTP • Optional: Voice-Adaptive Traffic Shaping (VATS) • Optional: Voice-Adaptive Fragmentation (VAF)	• Traffic Shaping • LLQ • Optional: VATS
Asynchronous Transfer Mode (ATM)	• TX-ring buffer changes • MLP over ATM • MLP LFI • LLQ • Optional: cRTP (requires MLP)	• TX-ring buffer changes • LLQ
Frame Relay and ATM Service Interworking (SIW)	• TX-ring buffer changes • MLP over ATM and FR • MLP LFI • LLQ • Optional: cRTP (requires MLP)	• TX-ring buffer changes • MLP over ATM and FR • LLQ
Multiprotocol Label Switching (MPLS)	• Same as above, according to the interface technology • Class-based marking is generally required to remark flows according to service provider specifications	• Same as above, according to the interface technology • Class-based marking is generally required to remark flows according to service provider specifications

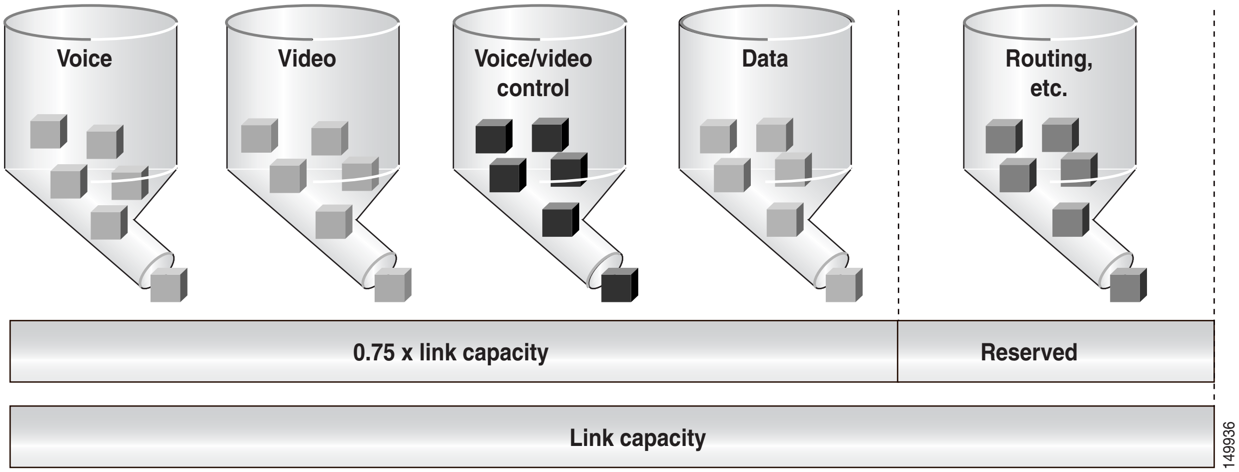
The following sections highlight some of the most important features and techniques to consider when designing a WAN to support both voice and data traffic:

- Bandwidth Provisioning, page 3-24
- Traffic Prioritization, page 3-27
- Link Efficiency Techniques, page 3-28
- Traffic Shaping, page 3-31

Bandwidth Provisioning

Properly provisioning the network bandwidth is a major component of designing a successful IP network. You can calculate the required bandwidth by adding the bandwidth requirements for each major application (for example, voice, video, and data). This sum then represents the minimum bandwidth requirement for any given link, and it should not exceed approximately 75 percent of the total available bandwidth for the link. This 75 percent rule assumes that some bandwidth is required for overhead traffic, such as routing and Layer 2 keepalives. Figure 3-6 illustrates this bandwidth provisioning process.

Figure 3-6 Link Bandwidth Provisioning



In addition to using no more than 75 percent of the total available bandwidth for data, voice, and video, the total bandwidth configured for all LLQ priority queues should typically not exceed 33 percent of the total link bandwidth. Provisioning more than 33 percent of the available bandwidth for the priority queue can be problematic for a number of reasons. First, provisioning more than 33 percent of the bandwidth for voice can result in increased CPU usage. Because each voice call will send 50 packets per second (with 20 ms samples), provisioning for large numbers of calls in the priority queue can lead to high CPU levels due to high packet rates. In addition, if more than one type of traffic is provisioned in the priority queue (for example, voice and video), this configuration defeats the purpose of enabling QoS because the priority queue essentially becomes a first-in, first-out (FIFO) queue. A larger percentage of reserved priority bandwidth effectively dampens the QoS effects by making more of the link bandwidth FIFO. Finally, allocating more than 33 percent of the available bandwidth can effectively starve any data queues that are provisioned. Obviously, for very slow links (less than 192 kbps), the recommendation to provision no more than 33 percent of the link bandwidth for the priority queue(s) might be unrealistic because a single call could require more than 33 percent of the link bandwidth. In these situations, and in situations where specific business needs cannot be met while holding to this recommendation, it may be necessary to exceed the 33 percent rule.

From a traffic standpoint, an IP telephony call consists of two parts:

- The voice carrier stream, which consists of Real-Time Transport Protocol (RTP) packets that contain the actual voice samples.
- The call control signaling, which consists of packets belonging to one of several protocols, according to the endpoints involved in the call (for example, H.323, MGCP, SCCP, SIP, or TAPI). Call control functions are, for instance, those used to set up, maintain, tear down, or redirect a call.

Bandwidth provisioning should include not only the voice stream traffic but also the call control traffic. In fact, in multisite WAN deployments, the call control traffic (and also the voice stream) must traverse the WAN, and failure to allocate sufficient bandwidth for it can adversely affect the user experience.

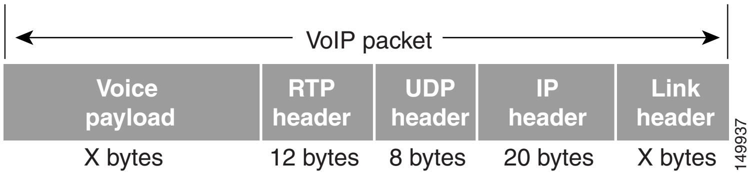
The next three sections describe the bandwidth provisioning recommendations for the following types of traffic:

- Voice bearer traffic in all multisite WAN deployments (see the "Provisioning for Voice Bearer Traffic" section on page 3-25)
- Call control traffic in multi-site WAN deployments with distributed call processing (see the "Provisioning for Call Control Traffic with Distributed Call Processing" section on page 3-26)

Provisioning for Voice Bearer Traffic

As illustrated in Figure 3-7, a voice-over-IP (VoIP) packet consists of the payload, IP header, User Datagram Protocol (UDP) header, Real-Time Transport Protocol (RTP) header, and Layer 2 Link header. At the default packetization rate of 20 ms, VoIP packets have a 160-byte payload for G.711 or a 20-byte payload for G.729. When Secure Real-Time Transport Protocol (SRTP) encryption is used, the payload for each packet is increased by 4 bytes. At the default packetization rate of 20 ms, SRTP VoIP packets have a 164-byte payload for G.711 or a 24-byte payload for G.729. The IP header is 20 bytes, the UDP header is 8 bytes, and the RTP header is 12 bytes. The link header varies in size according to the Layer 2 media used.

Figure 3-7 Typical VoIP Packet



The bandwidth consumed by VoIP streams is calculated by adding the packet payload and all headers (in bits), then multiplying by the packet rate per second (default of 50 packets per second). Table 3-4 details the bandwidth per VoIP flow at a default packet rate of 50 packets per second (pps). Table 3-4 does not include Layer 2 header overhead and does not take into account any possible compression schemes, such as compressed Real-Time Transport Protocol (cRTP).

Table 3-4 lists the bandwidth consumed by the voice payload and IP header only, at a default packet rate of 50 packets per second (pps) and at a rate of 33.3 pps for both unencrypted and encrypted payloads.

Table 3-4 Bandwidth Consumption for Voice Payload and IP Header Only

Codec	Sampling Rate	Voice Payload in Bytes	Packets per Second	Bandwidth per Conversation
G.711	20 ms	160	50.0	80.0 kbps
G.711 (SRTP)	20 ms	164	50.0	81.6 kbps
G.711	30 ms	240	33.3	74.7 kbps
G.711 (SRTP)	30 ms	244	33.3	75.8 kbps
G.729A	20 ms	20	50.0	24.0 kbps
G.729A (SRTP)	20 ms	24	50.0	25.6 kbps

Table 3-4 Bandwidth Consumption for Voice Payload and IP Header Only (continued)

Codec	Sampling Rate	Voice Payload in Bytes	Packets per Second	Bandwidth per Conversation
G.729A	30 ms	30	33.3	18.7 kbps
G.729A (SRTP)	30 ms	34	33.3	19.8 kbps

A more accurate method for provisioning is to include the Layer 2 headers in the bandwidth calculations. Table 3-5 lists the amount of bandwidth consumed by voice traffic when the Layer 2 headers are included in the calculations.

Table 3-5 Bandwidth Consumption with Layer 2 Headers Included

Codec	Header Type and Size						
	Ethernet 14 Bytes	PPP 6 Bytes	ATM 53-Byte Cells with a 48-Byte Payload	Frame Relay 4 Bytes	MLPPP 10 Bytes	MPLS 4 Bytes	WLAN 24 Bytes
G.711 at 50.0 pps	85.6 kbps	82.4 kbps	106.0 kbps	81.6 kbps	84.0 kbps	81.6 kbps	89.6 kbps
G.711 (SRTP) at 50.0 pps	87.2 kbps	84.0 kbps	106.0 kbps	83.2 kbps	85.6 kbps	83.2 kbps	N/A
G.729A at 50.0 pps	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps	28.0 kbps	25.6 kbps	33.6 kbps
G.729A (SRTP) at 50.0 pps	31.2 kbps	28.0 kbps	42.4 kbps	27.2 kbps	29.6 kbps	27.2 kbps	N/A

Provisioning for Call Control Traffic with Distributed Call Processing

In distributed call processing deployments, several sites are connected through an IP WAN. Each site contains a Cisco Unified CME system and can follow either the single-site model or the centralized call processing model. A gatekeeper can be used for keeping dial-plans consistent and easily manageable between sites.

The following considerations apply to this deployment model:

- The signaling protocol used to place a call across the WAN is H.323 or SIP.
- Control traffic is exchanged between the Cisco IOS gatekeeper and the Cisco Unified CME systems at each site, and also between the Cisco Unified CME systems themselves.

Therefore, bandwidth for control traffic must be provisioned on the WAN links between Cisco Unified CME systems and between each Cisco Unified CME and the gatekeeper. Because the topology is limited to hub-and-spoke, with the gatekeeper typically located at the hub, the WAN link that connects each site to the other sites usually coincides with the link that connects the site to the gatekeeper.

The control traffic that traverses the WAN belongs to one of the following categories:

- Quiescent traffic, which consists of registration messages periodically exchanged between each Cisco Unified CME and the gatekeeper

- Call-related traffic, consisting of H.225 or H.245 signaling traffic, exchanged between two Cisco Unified CME systems when a call needs to be set up, torn down, forwarded, and so on

Because the total amount of control traffic depends on the number of calls that are set up and torn down at any given time, it is necessary to make some assumptions about the call patterns and the link utilization. The WAN links that connect each of the spoke sites to the hub site are normally provisioned to accommodate different types of traffic (for example, data, voice, and video). Using a traditional telephony analogy, we can view the portion of the WAN link that has been provisioned for voice as a number of *virtual tie lines*.

Assuming an average call duration of 2 minutes and 100 percent utilization of each virtual tie line, we can derive that each tie line carries a volume of 30 calls per hour. This assumption allows us to obtain the following formula that expresses the recommended bandwidth for call control traffic as a function of the number of virtual tie lines.

Recommended Bandwidth Based on Number of Virtual Tie Lines.

Recommended Bandwidth (bps) = 116 * (Number of virtual tie lines)

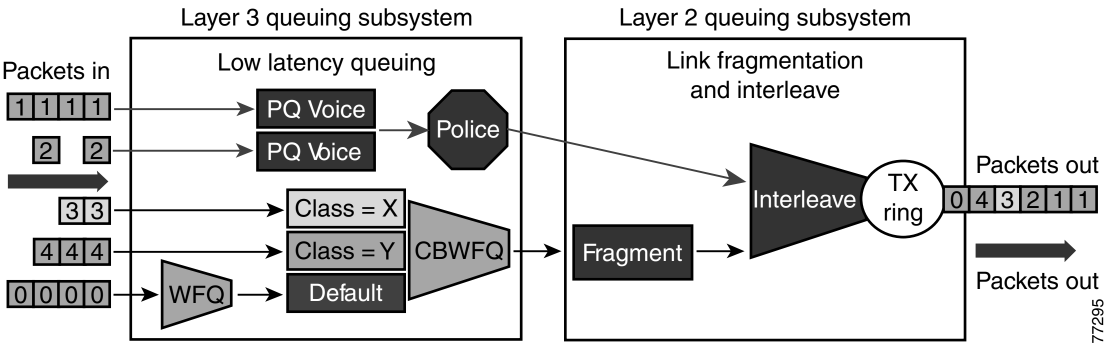
If we take into account the fact that 8 kbps is the smallest bandwidth that can be assigned to a queue on a Cisco IOS router, we can deduce that a minimum queue size of 8 kbps can accommodate the call control traffic generated by *up to 70 virtual tie lines*. This amount should be sufficient for most large enterprise deployments.

Traffic Prioritization

In choosing from among the many available prioritization schemes, the major factors to consider include the type of traffic involved and the type of media on the WAN. For multiservice traffic over an IP WAN, We recommend low-latency queuing (LLQ) for all links. This method supports up to 64 traffic classes, with the ability to specify, for example, priority queuing behavior for voice and interactive video, minimum bandwidth class-based weighted fair queuing for voice control traffic, additional minimum bandwidth weighted fair queues for mission critical data, and a default best-effort queue for all other traffic types.

Figure 3-8 shows an example prioritization scheme.

Figure 3-8 Optimized Queuing for VoIP over the WAN



We recommend the following prioritization criteria for LLQ:

- The criterion for *voice* to be placed into a priority queue is the differentiated services code point (DSCP) value of 46, or a per-hop behavior (PHB) value of EF.

- The criterion for *video conferencing* traffic to be placed into a priority queue is a DSCP value of 34, or a PHB value of AF41. However, due to the larger packet sizes of video traffic, these packets should be placed in the priority queue only on WAN links that are faster than 768 kbps. Link speeds below this value require packet fragmentation, but packets placed in the priority queue are not fragmented, thus smaller voice packets could be queued behind larger video packets. For links speeds of 768 kbps or lower, video conferencing traffic should be placed in a separate class-based weighted fair queue (CBWFQ).

  Note One-way video traffic, such as the traffic generated by streaming video applications for services such as video-on-demand or live video feeds, should always use a CBWFQ scheme because that type of traffic has a much higher delay tolerance than two-way video conferencing traffic.

- As the WAN links become congested, it is possible to starve the *voice control* signaling protocols, thereby eliminating the ability of the IP phones to complete calls across the IP WAN. Therefore, voice control protocols, such as H.323, MGCP, and Skinny Client Control Protocol (SCCP), require their own class-based weighted fair queue. The entrance criterion for this queue is a DSCP value of 24 or a PHB value of CS3.

  Note We have begun to change the marking of voice control protocols from DSCP 26 (PHB AF31) to DSCP 24 (PHB CS3). However many products still mark signaling traffic as DSCP 26 (PHB AF31); therefore, in the interim, we recommend that you reserve both AF31 and CS3 for call signaling.

- In some cases, certain data traffic might require better than best-effort treatment. This traffic is referred to as *mission-critical data*, and it is placed into one or more queues that have the required amount of bandwidth. The queuing scheme within this class is first-in-first-out (FIFO) with a minimum allocated bandwidth. Traffic in this class that exceeds the configured bandwidth limit is placed in the default queue. The entrance criterion for this queue could be a Transmission Control Protocol (TCP) port number, a Layer 3 address, or a DSCP/PHB value.
- All remaining traffic can be placed in a default queue for best-effort treatment. If you specify the keyword **fair**, the queuing algorithm will be weighted fair queuing (WFQ).

Link Efficiency Techniques

The following link efficiency techniques improve the quality and efficiency of low-speed WAN links.

Compressed Real-Time Transport Protocol (cRTP)

You can increase link efficiency by using Compressed Real-Time Transport Protocol (cRTP). This protocol compresses a 40-byte IP, User Datagram Protocol (UDP), and RTP header into approximately two to four bytes. cRTP operates on a per-hop basis. Use cRTP on a particular link only if that link meets *all* of the following conditions:

- Voice traffic represents more than 33 percent of the load on the specific link.
- The link uses a low bit-rate codec (such as G.729).
- No other real-time application (such as video conferencing) is using the same link.

If the link fails to meet any one of the preceding conditions, then cRTP is not effective and you should not use it on that link. Another important parameter to consider before using cRTP is router CPU utilization, which is adversely affected by compression and decompression operations.

cRTP on ATM and Frame Relay Service Inter-Working (SIW) links requires the use of Multilink Point-to-Point Protocol (MLP).

Note that cRTP compression occurs as the final step before a packet leaves the egress interface; that is, after LLQ class-based queueing has occurred. Beginning in Cisco IOS Release 12.(2)2T and later, cRTP provides a feedback mechanism to the LLQ class-based queueing mechanism that allows the bandwidth in the *voice* class to be configured based on the compressed packet value. With Cisco IOS software releases earlier than 12.(2)2T, this mechanism is not in place, so the LLQ is unaware of the compressed bandwidth and, therefore, the *voice* class bandwidth has to be provisioned as if no compression is taking place. Table 3-6 shows an example of the difference in *voice* class bandwidth configuration given a 512-kbps link with G.729 codec and a requirement for 10 calls.

Note that Table 3-6 assumes 24 kbps for non-cRTP G.729 calls and 10 kbps for cRTP G.729 calls. These bandwidth numbers are based on voice payload and IP/UDP/RTP headers only. They do not take into consideration Layer 2 header bandwidth. However, actual bandwidth provisioning should also include Layer 2 header bandwidth based on the type WAN link used.

Table 3-6 LLQ Voice Class Bandwidth Requirements for 10 Calls with 512 kbps Link Bandwidth and G.729 Codec

Cisco IOS Release	With cRTP Not Configured	With cRTP Configured
Before 12.2(2)T	240 kbps	240 kbps[1]
12.2(2)T or later releases	240 kbps	100 kbps

[1] 140 kbps of unnecessary bandwidth must be configured in the LLQ *voice* class.

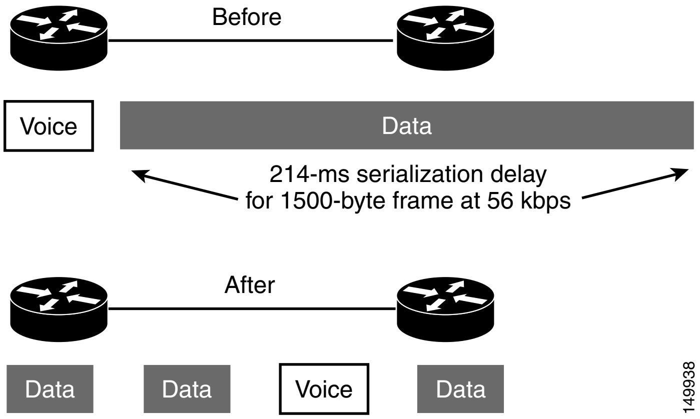
It should also be noted that, beginning in Cisco IOS Release 12.2(13)T, cRTP can be configured as part of the voice class with the Class-Based cRTP feature. This option allows cRTP to be specified within a class, attached to an interface via a service policy. This new feature provides compression statistics and bandwidth status via the **show policy interface** command, which can be very helpful in determining the offered rate on an interface service policy class given the fact that cRTP is compressing the IP/RTP headers.

Note For additional recommendations about using cRTP with a Voice and Video Enabled IP Sec VPN (V3PN), see the V3PN documentation available at http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f2cb.pdf

Link Fragmentation and Interleaving (LFI)

For low-speed links (less than 768 kbps), use of link fragmentation and interleaving (LFI) mechanisms is required for acceptable voice quality. This technique limits jitter by preventing voice traffic from being delayed behind large data frames, as illustrated in Figure 3-9. The two techniques that exist for this purpose are Multilink Point-to-Point Protocol (MLP) LFI (for Leased Lines, ATM, and SIW) and FRF.12 for Frame Relay.

Figure 3-9 Link Fragmentation and Interleaving (LFI)



Voice-Adaptive Fragmentation (VAF)

In addition to the LFI mechanisms mentioned above, voice-adaptive fragmentation (VAF) is another LFI mechanism for Frame Relay links. VAF uses FRF.12 Frame Relay LFI; however, once configured, fragmentation occurs only when traffic is present in the LLQ priority queue or when H.323 signaling packets are detected on the interface. This method ensures that, when voice traffic is being sent on the WAN interface, large packets are fragmented and interleaved. However, when voice traffic is not present on the WAN link, traffic is forwarded across the link unfragmented, thus reducing the overhead required for fragmentation.

VAF is typically used in combination with voice-adaptive traffic shaping (se0 the "Voice-Adaptive Traffic Shaping" section on page 3-32). VAF is an optional LFI tool, and you should exercise care when enabling it because there is a slight delay between the time when voice activity is detected and the time when the LFI mechanism engages. In addition, a configurable deactivation timer (default of 30 seconds) must expire after the last voice packet is detected and before VAF is deactivated, so during that time LFI will occur unnecessarily. VAF is available in Cisco IOS Release 12.2(15)T and later releases.

Traffic Shaping

Traffic shaping is required for multiple-access, non-broadcast media such as ATM and Frame Relay, where the physical access speed varies between two endpoints and several branch sites are typically aggregated to a single router interface at the central site.

Figure 3-10 illustrates the main reasons why traffic shaping is needed when transporting voice and data on the same IP WAN.

Figure 3-10 Traffic Shaping with Frame Relay and ATM

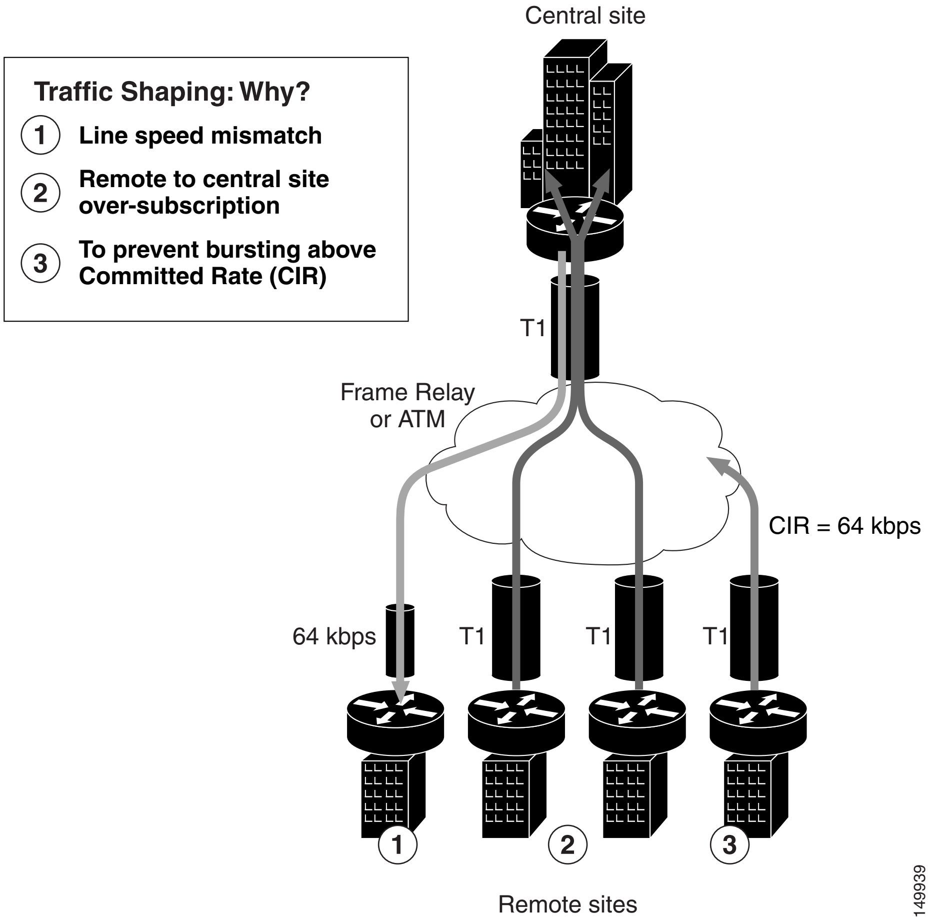

Central site
Traffic Shaping: Why?
① Line speed mismatch
② Remote to central site over-subscription
③ To prevent bursting above Committed Rate (CIR)
T1
Frame Relay or ATM
CIR = 64 kbps
64 kbps
T1
T1
T1
①
②
③
Remote sites
149939

Figure 3-10 shows three different scenarios:

1. Line speed mismatch

   While the central-site interface is typically a high-speed one (such as T1 or higher), smaller remote branch interfaces may have significantly lower line speeds, such as 64 kbps. If data is sent at full rate from the central site to a slow-speed remote site, the interface at the remote site might become congested and degrade voice performance.

2. Oversubscription of the link between the central site and the remote sites

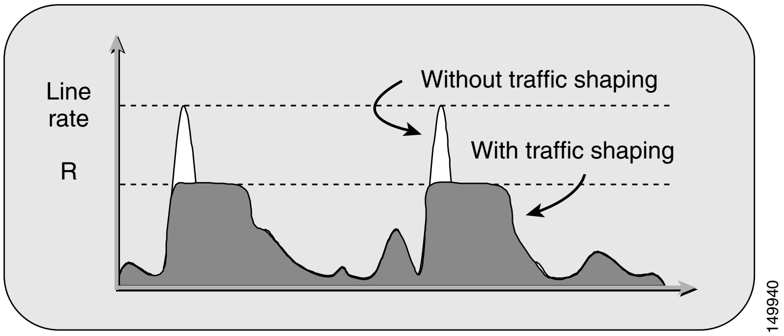
   It is common practice in Frame Relay or ATM networks to oversubscribe bandwidth when aggregating many remote sites to a single central site. For example, there may be multiple remote sites that connect to the WAN with a T1 interface, yet the central site has only a single T1 interface. While this configuration allows the deployment to benefit from statistical multiplexing, the router interface at the central site can become congested during traffic bursts, thus degrading voice quality.

3. Bursting above Committed Information Rate (CIR)

   Another common configuration is to allow traffic bursts above the CIR, which represents the rate that the service provider has guaranteed to transport across its network with no loss and low delay. For example, a remote site with a T1 interface might have a CIR of only 64 kbps. When more than 64 kbps worth of traffic is sent across the WAN, the provider marks the additional traffic as "discard eligible." If congestion occurs in the provider network, this traffic will be dropped with no regard to traffic classification, possibly having a negative affect on voice quality.

Traffic shaping provides a solution to these issues by limiting the traffic sent out an interface to a rate lower than the line rate, thus ensuring that no congestion occurs on either end of the WAN. Figure 3-11 illustrates this mechanism with a generic example, where R is the rate with traffic shaping applied.

Figure 3-11 Traffic Shaping Mechanism



Voice-Adaptive Traffic Shaping

Voice-adaptive traffic shaping (VATS) is an optional dynamic mechanism that shapes traffic on Frame Relay permanent virtual circuits (PVCs) at different rates based on whether voice is being sent across the WAN. The presence of traffic in the LLQ voice priority queue or the detection of H.323 signaling on the link causes VATS to engage. Typically, Frame Relay shapes traffic to the guaranteed bandwidth or CIR of the PVC at all times. However, because these PVCs are typically allowed to burst above the CIR (up to line speed), traffic shaping keeps traffic from using the additional bandwidth that might be present in the WAN. With VATS enabled on Frame Relay PVCs, WAN interfaces are able to send at CIR when voice traffic is present on the link. However, when voice is not present, non-voice traffic is able to burst up to line speed and take advantage of the additional bandwidth that might be present in the WAN.

When VATS is used in combination with voice-adaptive fragmentation (VAF) (see the "Link Fragmentation and Interleaving (LFI)" section on page 3-29), all non-voice traffic is fragmented and all traffic is shaped to the CIR of the WAN link when voice activity is detected on the interface.

As with VAF, exercise care when enabling VATS because activation can have an adverse effect on non-voice traffic. When voice is present on the link, data applications will experience decreased throughput because they are throttled back to below CIR. This behavior will likely result in packet drops and delays for non-voice traffic. Furthermore, after voice traffic is no longer detected, the deactivation timer (default of 30 seconds) must expire before traffic can burst back to line speed. It is important, when using VATS, to set end-user expectations and make them aware that data applications will experience slowdowns on a regular basis due to the presence of voice calls across the WAN. VATS is available in Cisco IOS Release 12.2(15)T and later.

For more information on the voice-adaptive traffic shaping and fragmentation features and how to configure them, see documentation at:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_vats.html

Wireless LAN Infrastructure

Wireless LAN infrastructure design becomes important when IP telephony is added to the wireless LAN (WLAN) portions of a converged network. With the addition of wireless IP telephony endpoints such as the Cisco Wireless IP Phone 7920, voice traffic has moved onto the WLAN and is now converged with the existing data traffic there. Just as with wired LAN and wired WAN infrastructure, the addition of voice in the WLAN requires following basic configuration and design best-practices for deploying a highly available network. In addition, proper WLAN infrastructure design requires understanding and deploying QoS on the wireless network to ensure end-to-end voice quality on the entire network. The following sections discuss these requirements:

- WLAN Design and Configuration, page 3-33
- WLAN Quality of Service (QoS), page 3-40

Note For more information about the Cisco Unified Wireless IP Phone 7920, see the following URLs:
http://www.cisco.com/en/US/docs/wireless/technology/7920/design/guide/7920DG.htmland
http://www.cisco.com/en/USf/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html

WLAN Design and Configuration

Properly designing a WLAN requires, first and foremost, ensuring that the existing wired network is deployed in a highly available, fault-tolerant and redundant manner. Next, an understanding of wireless technology is required. Finally, by configuring and deploying wireless APs and wireless telephony endpoints in an effective way, you can build a flexible, secure, redundant, and highly scalable network.

The following sections examine the WLAN infrastructure layers and network services:

- Wireless Infrastructure Considerations, page 3-33
- Wireless AP Configuration and Design, page 3-37
- Wireless Security, page 3-38

Wireless Infrastructure Considerations

The following sections provide guidelines and best practices for designing the WLAN infrastructure:

- VLANs, page 3-34
- Roaming, page 3-34
- Wireless Channels, page 3-34

- Wireless Interference, page 3-36
- Multicast on the WLAN, page 3-36

VLANs

Just as with a wired LAN infrastructure, when deploying voice in a wireless LAN, you should enable at least two virtual LANs (VLANs) at the Access Layer. The Access Layer in a wireless LAN environment includes the access point (AP) and the first-hop access switch. On the AP and access switch, you should configure both a native VLAN for data traffic and a voice VLAN (under Cisco IOS software) or Auxiliary VLAN (under Catalyst Operating System) for voice traffic. This voice/auxiliary VLAN must be separate from all the other wired voice VLANs in the network. In addition, as with voice endpoints on wired LANs, wireless voice endpoints should be addressed using RFC 1918 private subnet addresses. When deploying a wireless infrastructure, we recommend configuring a separate management VLAN for the management of WLAN APs. This management VLAN should not have a WLAN appearance; that is, it should not have an associated service set identifier (SSID) and it should not be directly accessible from the WLAN.

Roaming

Another very important consideration for wireless infrastructure is wireless endpoint roaming. When wireless devices roam at Layer 2, they keep their IP address and network configuration. For this reason, roaming can occur fairly quickly (in 100 to 400 ms). All that is required is re-authentication, if Cisco LEAP or Extensible Authentication Protocol (EAP) is used, and the passing of Inter-Access Point Protocol (IAPP) messages between the last AP and the new AP to indicate that the endpoint has roamed. Layer 2 roaming is typically unnoticeable to the end user.

When devices roam at Layer 3, they move from one AP to another AP and cross a subnet boundary. With the release of the new Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), the Cisco Unified Wireless IP Phone 7920 now supports call-survivable Layer 3 roaming while using Static WEP. Cisco Centralized Key Management (Cisco CKM) enables the Cisco 7920 phone to achieve full Layer 3 mobility while using LEAP. For details about the Cisco WLSM, see the product documentation available at:
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_implementation_design_guide09186a00807d592c.html

Note If Cisco Catalyst 4000 Series switches are used as Layer 3 devices at the distribution layer, a minimum of a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module is required. The Supervisor Engine 1 or 2 (SUP1 or SUP2) modules can cause roaming delays. The Cisco Catalyst 2948G, 2948G-GE-TX, 2980G, 2980G-A, and 4912 switches are also known to introduce roaming delays. we do not recommend using these switches in a wireless voice network.

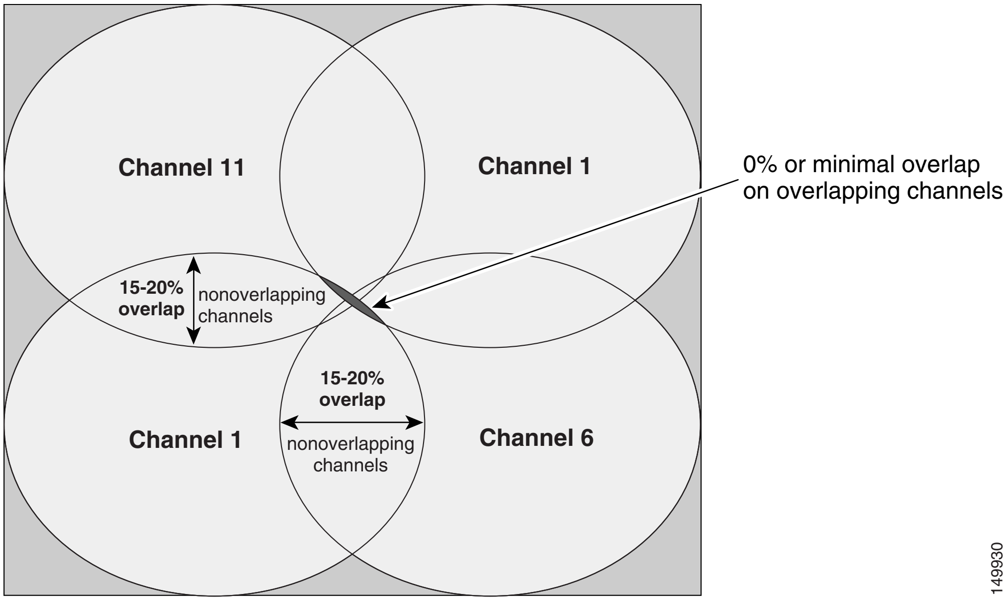
Wireless Channels

Wireless endpoints and APs communicate via radios on particular channels. When communicating on one channel, wireless endpoints typically are unaware of traffic and communication occurring on other nonoverlapping channels. Optimal channel configuration for 2.4 GHz 802.11b requires a five-channel spread to prevent interference or overlap between channels. In North America, channels 1, 6, and 11 are the three usable nonoverlapping channels for APs and wireless endpoint devices. In the European Union, the nonoverlapping usable channels for 802.11b are 1, 6, and 11 or 12 or 13. In Japan these channels are 1, 6, and 11 or 12, 13, or 14.

AP coverage should be deployed so that minimal or no overlap occurs between APs configured with the same channel (for example, see Channel 1 in Figure 3-12). However, proper AP deployment and coverage on *nonoverlapping* channels (1, 6, and 11 in North America) require an overlap of 15 to 20 percent. This amount of overlap ensures smooth roaming for wireless endpoints as they move between

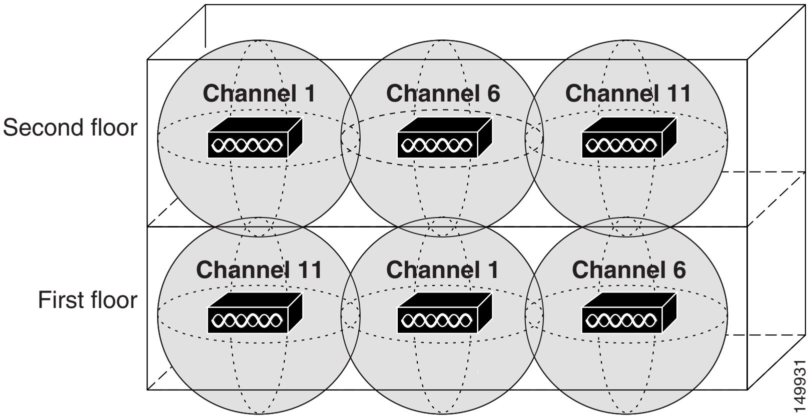
AP coverage cells. Overlap of less than 15 to 20 percent can result in slower roaming times and poor voice quality; while overlap of more than 15 to 20 percent can result in too frequent or constant roaming. Figure 3-12 illustrates appropriate AP overlap for both overlapping and nonoverlapping channels.

Figure 3-12 Wireless 802.11b Channel Overlap


Channel 11
Channel 1
0% or minimal overlap on overlapping channels
15-20% overlap
nonoverlapping channels
15-20% overlap
Channel 1
nonoverlapping channels
Channel 6
149930

Deploying wireless devices in a multistory building such as an office high-rise or hospital introduces a third dimension to wireless AP and channel coverage planning. The 2.4 GHz wave form of 802.11b can pass through floors and ceilings and walls. For this reason, not only is it important to consider overlapping cells or channels on the same floor, but it is also necessary to consider channel overlap between adjacent floors. With only three channels, proper overlap can be achieved only through careful three-dimensional planning. Figure 3-13 shows the potential for channel overlap when considering the three-dimensional aspects of 802.11b wireless coverage.

Figure 3-13 Wireless 802.11b Channel Overlap Considerations (in Three Dimensions)


Second floor
Channel 1
Channel 6
Channel 11
First floor
Channel 11
Channel 1
Channel 6
149931

Note Careful deployment of APs and channel configuration within the wireless infrastructure are imperative for proper wireless network operation. For this reason, we require that a complete and thorough site survey be conducted before deploying wireless networks in a production environment. The survey should include verifying nonoverlapping channel configurations, AP coverage, and required data and traffic rates; eliminating rogue APs; and identifying and mitigating the impact of potential interference sources.

Wireless Interference

Interference sources within a wireless environment can severely limit endpoint connectivity and channel coverage. In addition, objects and obstructions can cause signal reflection and multipath distortion. Multipath distortion occurs when traffic or signaling travels in more than one direction from the source to the destination. Typically, some of the traffic arrives at the destination before the rest of the traffic, which can result in delay and bit errors in some cases. You can reduce the affects of multipath distortion by eliminating or reducing interference sources and obstructions, and by using diversity antennas so that only a single antenna is receiving traffic at any one time. Interference sources should be identified during the site survey and, if possible, eliminated. At the very least, interference impact should be alleviated by proper AP placement and the use of location-appropriate directional or omni-directional diversity radio antennas.

Possible interference sources include:

- Other APs on overlapping channels
- Other 2.4 GHz appliances, such as 2.4 GHz cordless phones, personal wireless network devices, sulphur plasma lighting systems, microwave ovens, rogue APs, and other WLAN equipment that takes advantage of the license-free operation of the 2.4 GHz band
- Metal equipment, structures, and other metal or reflective surfaces such as metal I-beams, filing cabinets, equipment racks, wire mesh or metallic walls, fire doors and fire walls, concrete, and heating and air conditioning ducts
- High-power electrical devices such as transformers, heavy-duty electric motors, refrigerators, elevators, and elevator equipment

Multicast on the WLAN

We do not recommend forwarding multicast traffic on a WLAN with voice devices because of the following reasons:

- Multicast packets are buffered on the AP if devices associated with the AP are in power-save mode.

  When devices such as the Cisco Wireless IP Phone 7920 go into power-save mode, an AP buffers all multicast packets until the next active interval for these devices. This buffering causes packet delay and affects all devices associated with the AP even if they are not in power-save mode. This condition can be extremely problematic for real-time multicast applications such as music on hold and streaming video.

- Multicast packets on the WLAN are unacknowledged and are not retransmitted if lost or corrupted.

  AP and wireless endpoint devices use acknowledgements on the link layer to ensure reliable delivery. When packets are not received or acknowledged, they are retransmitted. This retransmission does not occur for multicast traffic on the WLAN. Given that wireless networks have a higher instance of bit error than wired networks, this lack of retransmission results in a larger number of lost packets when compared to a wired LAN.

Before enabling multicast applications on the wireless network, we recommend testing these applications to ensure that performance and behavior are acceptable.

Wireless AP Configuration and Design

Proper AP selection, deployment, and configuration are essential to ensure that the wireless network handles voice traffic in a way that provides high-quality voice to the end users.

AP Selection

Cisco recommend the following APs for deploying wireless voice:

- Cisco Aironet 350 Series AP
- Cisco Aironet 1100 Series AP
- Cisco Aironet 1200 Series AP

For these APs, Cisco IOS Release 12.2(13)JA3 or later releases should be used. We do *not* recommend the VxWorks operating system for APs when deploying wireless voice because new features are not being added to VxWorks, but some of those new features are required for voice deployments.

The Cisco Integrated Services Routers (ISRs)—including the Cisco 800, Cisco 1800, Cisco 2800, and Cisco 3800 series routers—also support access point functionality. For the fixed Cisco 800s and fixed Cisco 1800s (with a built-in access point), use Cisco IOS Release 12.3(8)YI or later. For the modular Cisco 1841, Cisco 28xx, and Cisco 38xx routers, use a HWIC-AP to provide access point functionality along with Cisco IOS Release 12.4(2)T or later releases. Features supported on the wireless ISR APs are similar to the Aironet APs, with a few exceptions. The following links documents features supported on the wireless ISR APs:

- Cisco 870

  http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps6200/product_data_sheet0900aecd8028a976.html

- Cisco 1800 (fixed hardware configuration)

  http://www.cisco.com/en/US/prod/collateral/routers/ps5853/ps6184/product_data_sheet0900aecd8028a95f_ps5853_Products_Data_Sheet.html

- HWIC-AP

  http://www.cisco.com/en/US/prod/collateral/modules/ps5949/ps6246/product_data_sheet0900aecd8028cc7b.html

- Configuration Guide

  http://www.cisco.com/en/US/docs/ios/wlan/configuration/guide/12_4t/wl_12_4t_book.html

AP Deployment

When deploying Cisco APs, do not associate more than 15 to 25 devices to a single AP at any time. This number will vary depending on usage profiles. The number of devices on an AP affects the amount of time each device has access to the medium. As the number of devices increases, the traffic contention increases. Associating more than 15 to 25 devices to an AP can result in poor AP performance and slower response times for associated devices.

AP Configuration

When deploying wireless voice, observe the following specific AP configuration requirements:

- Enable Address Resolution Protocol (ARP) caching.

  ARP caching is required on the AP because it enables the AP to answer ARP requests for the wireless endpoint devices without requiring the endpoint to leave power-save or idle mode. This feature results in extended battery life for the wireless endpoint devices.

- Match the transmit power on the AP to that on the wireless voice endpoints.

  When possible, the transmit power on the AP and the voice endpoints should match. Matching transmit power on the AP and voice endpoints helps eliminate the possibility of one-way audio traffic. If the transmit power configuration on the APs must vary, the transmit power on all voice endpoints should be configured to match the AP with the highest transmit power.

  Note Beginning with version 1.0(8) of the Cisco Unified Wireless IP Phone 7920 firmware, the phone will take advantage of the Dynamic Transmit Power Control (DTPC) feature by automatically adjusting its transmit power based on the Limit Client Power (mW) setting of the current AP.

- Set the data rate to 11 Mbps.

  Configuring the maximum 11 Mbps data rate ensures the best level of throughput for voice devices and the largest number of active calls per AP.

- Manually configure the RF channel selection. (Do *not* use the option **Search for Least Congested Channel**).

  To control wireless network channels and eliminate channel overlap, it is important to configure a channel number manually on each AP based on its location.

- Assign a Service Set Identifier (SSID) to each VLAN configured on the AP.

  SSIDs enable endpoints to select the wireless VLAN they will use for sending and receiving traffic. These wireless VLANs and SSIDs map to wired VLANs. For voice endpoints, this mapping ensures priority queuing treatment and access to the voice VLAN on the wired network.

- Enable **QoS Element for Wireless Phones** on the AP.

  This feature ensures that the AP will provide QoS Basic Service Set (QBSS) information elements in beacons. The QBSS element provides an estimate of the channel utilization on the AP, and Cisco wireless voice devices use it to help make roaming decisions and to reject call attempts when loads are too high.

- Configure two QoS policies on the AP, and apply them to the VLANs and interfaces.

  Configure a voice policy and a data policy with default classifications for the respective VLANs to ensure that voice traffic is given priority queuing treatment. (See the "Interface Queuing" section on page 3-40 for more information).

Wireless Security

Another important consideration for a wireless infrastructure is security. Wireless endpoints, including wireless phones, can connect to the wireless network using one of the following security mechanisms:

- Cisco LEAP

  Cisco LEAP requires the wireless endpoint to provide a user name and password to authenticate with the network. Once this authentication occurs, a dynamic key is generated, and traffic to and from the wireless device is encrypted. This method requires an EAP-compliant Remote Authentication Dial-In User Service (RADIUS) authentication server such as the Cisco Secure Access Control Server (ACS), which provides access to a user database for authenticating the wireless devices. Cisco LEAP is the recommend security mechanism for use with wireless voice because it requires the highest level of security for access to voice VLANs.

- Static Wire Equivalent Privacy (WEP)

  Static WEP requires the exchange of a statically configured 40-bit or 128-bit character key between the wireless endpoint and the AP. If the keys match, the wireless device is given access to the network. Be aware that there are known weaknesses in the WEP encryption algorithm. These weaknesses, coupled with the complexity of configuring and maintaining static keys, can make this security mechanism undesirable in many cases.

- Open authentication

  This method requires no authentication and provides no security for traffic traveling between the wireless endpoint device and the wireless network. This method requires only that the wireless device be configured with the proper SSID for the wireless VLAN to which the device wishes to connect. We do not typically recommend this method for wireless voice because it requires no authentication for access to voice VLANs and provides no encryption for voice traffic.

Cisco LEAP Authentication and ACS Deployment Models

As indicated previously, Cisco LEAP is the preferred method of wireless device authentication (especially voice devices) because it provides the most secure and robust mechanism for access to the network and voice VLAN(s). Because an EAP-compliant RADIUS server is required, we recommend the use of Cisco Secure ACS for Windows Server Version 3.1 or later releases.

When deploying Cisco LEAP for wireless authentication and encryption, carefully consider the placement of the ACS within the network, and select one of the following ACS deployment models:

- Centralized ACS

  ACS server or servers are located in a centralized place within the network and are used to authenticate all wireless devices and users within the network.

- Remote ACS

  In networks where remote locations are separated from the central site by low-speed or congested WAN links, an ACS server can be located at the remote site and remote wireless devices or users can be authenticated by this server locally, thus eliminating the potential for delayed authentication via a centralized ACS across the WAN link.

- Local and fallback RADIUS server on the Cisco AP

  In networks where remote locations are separated from a central site by low-speed WAN links, local wireless devices can authenticate against local Cisco IOS APs. APs running Cisco IOS Release 12.2(11)JA or later releases can authenticate Cisco LEAP users and devices locally without relying on an external ACS. A single AP can support up to 50 users with this functionality.

  The Cisco integrated services routers (ISR) also support local authentication via LEAP. The number of users supported depends on the platform. Please see the link below for limitations per platform:

  http://www.cisco.com/en/US/prod/collateral/routers/ps5854/product_data_sheet0900aecd8016ef57_ps380_Products_Data_Sheet.html

  This feature can be used in lieu of a centralized or local ACS, or in the case of a WAN or ACS failure in which the remote site users are unable to contact a local ACS or the central site ACS.

When choosing a deployment model for the ACS, it is imperative to make authentication services redundant so that the ACS does not become a single point of failure when wireless devices attempt to access the network. For this reason, each ACS server should replicate its database to a secondary server. Furthermore, it is always a good idea to provide a local ACS or an on-AP RADIUS server at remote sites to ensure that remote wireless devices can still authenticate in the event of a WAN failure.

In addition to ACS server placement, it is also important to consider the implications of user database location in relation to the ACS server. Because the ACS server must access the user database to authenticate wireless devices, the location of the user database affects the amount of time the authentication will take. If the user database is a Microsoft Active Directory (AD) server located on the network, the ACS must send an authentication request to the AD server and wait for a response. To ensure the fastest response times for wireless voice endpoints attempting to authenticate to the network, we recommend defining users locally on the ACS server. Remote databases have unknown response times and can adversely affect authentication times.

WLAN Quality of Service (QoS)

Just as QoS is necessary for LAN and WAN wired network infrastructure in order to ensure high voice quality, QoS is also require for wireless LAN infrastructure. Because of the bursty nature of data traffic and the fact that real-time traffic such as voice is sensitive to packet loss and delay, QoS tools are required to manage wireless LAN buffers, limit radio contention, and minimize packet loss, delay, and delay variation.

However, unlike most wired networks, wireless networks are a shared medium, and wireless endpoints do not have dedicated bandwidth for sending and receiving traffic. While wireless endpoints can mark traffic with 802.1p CoS, DSCP, and PHB, the shared nature of the wireless network means limited admission control and access to the network for these endpoints.

Wireless QoS involves the following main areas of configuration:

- Traffic Classification, page 3-40
- Interface Queuing, page 3-40
- Bandwidth Provisioning, page 3-41

Traffic Classification

As with wired network infrastructure, it is important to classify or mark pertinent wireless traffic as close to the edge of the network as possible. Because traffic marking is an entrance criterion for queuing schemes throughout the wired and wireless network, marking should be done at the wireless endpoint device whenever possible. Marking or classification by wireless network devices should be identical to that for wired network devices, as indicated in Table 3-2.

In accordance with traffic classification guidelines for wired networks, the Cisco Unified Wireless IP Phone 7920 marks voice media traffic or RTP traffic with DSCP 46 (or PHB EF) and voice signaling traffic (SCCP) with DSCP 26 (or PHB AF31). Once this traffic is marked, it can be given priority or better than best-effort treatment and queuing throughout the network. All wireless voice devices should be capable of marking traffic in this manner. All other traffic on the wireless network should be marked as best-effort or with some intermediary classification as outlined in wired network marking guidelines.

Interface Queuing

Once marking has occurred, it is necessary to enable the wired network APs and devices to provide QoS queuing so that voice traffic types are given separate queues to reduce the chances of this traffic being dropped or delayed as it traversed the wireless LAN. Queuing on the wireless network occurs in two directions, upstream and downstream. Upstream queuing concerns traffic traveling from the wireless endpoint up to the AP and from the AP up to the wired network. Downstream queuing concerns traffic traveling from the wired network to the AP and down to the wireless endpoint.

Unfortunately, there is little upstream queuing available in a wireless network. While wireless devices such as the Cisco Unified Wireless IP Phone 7920 can provide queuing upstream as the packets leave the device, there is no mechanism in place to provide queuing among all clients on the wireless LAN because wireless networks are a shared medium. Therefore, although voice media packets might receive priority treatment leaving the wireless endpoint, these packets must contend with all the other packets that other wireless devices may be attempting to send. For this reason, it is extremely important to follow the guideline of no more than 15 to 25 wireless clients per AP. Going beyond the upper limit of this guideline can result in additional voice packet delay and jitter.

As for downstream QoS, Cisco APs currently provide up to eight queues for downstream traffic being sent to wireless clients. The entrance criterion for these queues can be based on a number of factors including DSCP, access control lists (ACLs), and VLAN. Although eight queues are available, we recommend using only two queues when deploying wireless voice. All voice media and signaling traffic should be placed in the highest-priority queue, and all other traffic should be placed in the best-effort queue. This ensure the best possible queuing treatment for voice traffic.

To set up this two-queue configuration, create two QoS policies on the AP. Name one policy **voice** and configure it with the class of service **Voice <10 ms Latency (6)** as the **Default Classification for all packets on the Vlan**. Name the other policy **data** and configure it with the class of service **Best Effort (0)** as the **Default Classification for all packets on the Vlan**. Then assign the **data** policy to the incoming and outgoing radio interface for the data VLAN(s), and assign the **voice** policy to the incoming and outgoing radio interfaces for the voice VLAN(s). With the QoS policies applied at the VLAN level, the AP is not forced to examine every packet coming in or going out to determine the type of queuing it should receive. This configuration ensures that all voice media and signaling are given priority queuing treatment in a downstream direction.

Bandwidth Provisioning

Another QoS requirement for wireless networking is the appropriate provisioning of bandwidth. Bandwidth provisioning involves the bandwidth between the wired and wireless networks as well as the number of simultaneous voice calls that an AP can handle. Wireless APs typically connect to the wired network via a 100 Mbps link to an Access Layer switch port. While the ingress Ethernet port on the AP can receive traffic at 100 Mbps, the maximum throughput on an 802.11b wireless network is 11 Mbps. After taking into account the half-duplex nature of the wireless medium and the overhead of wireless headers, the practical throughput on the 802.11b wireless network is about 7 Mbps. This mismatch in throughput between the wired and wireless network can result in packet drops when traffic bursts occur in the network.

Rather than allowing traffic bursts to send excessive traffic toward the AP only to have it dropped by the AP, it is a good idea to rate-limit or police this traffic to a rate that the wireless network can handle. Forcing the AP to drop excessive traffic causes increased CPU utilization and congestion at the AP. Instead, limiting the traffic rate to 7 Mbps on the link between the wired Access Layer switch and the wireless AP ensures that traffic is dropped at the Access Layer switch, thus removing the burden from the AP. Note that, depending on the wireless network deployment, the practical throughput might be less than 7 Mbps, especially if more than the recommended number of devices are associated to a single AP.

Based on wireless voice network testing, we determined that a single wireless AP can support up to seven (7) G.711 voice calls or eight (8) G.729 voice calls. If these limits are exceeded, voice quality will suffer and voice calls might be dropped. While there is no true call admission control mechanism or method for provisioning wireless bandwidth for voice traffic, Cisco 7920 Wireless IP Phones can provide a simplified version of call admission control or bandwidth provisioning based on channel utilization information received from APs on the network. This information can be sent by the AP to the phone via a beacon that includes the QoS Basic Service Set (QBSS). The QBSS provides an estimation of the percentage of time the RF channel is in use by that AP. The higher the QBSS element value, the higher the channel utilization and the less likely the channel and AP can provide sufficient bandwidth for additional wireless voice devices. If the QBSS element value is 45 or higher, then any calls attempted by the wireless IP phone will be rejected with a "Network Busy" message and/or fast busy tone. In addition, the wireless IP phone considers the QBSS element in its roaming algorithm and will not roam to an AP that is sending beacons with a QBSS element of 45 or higher.

Note The QBSS value is simply an estimation of the channel utilization for a particular AP. The real channel utilization can be much higher than indicated. For this reason, the wireless voice device might still be able to place a voice call on an AP that has already reached the limit of 7 or 8 calls, thus still resulting in dropped calls or poor voice quality.

The QBSS information element is sent by the AP only if **QoS Element for Wireless Phones** has been enable on the AP. (See the "Wireless AP Configuration and Design" section on page 3-37.)

Voice Gateways

Router PSTN connectivity is generically referred to as *voice gateway* functionality, offering a *gateway* for voice over IP (VoIP) calls to, and from, traditional analog or digital PSTN or private branch exchange (PBX) calls. You can use a router voice gateway to connect to PSTN central office (CO) switches, private branch exchanges (PBXs), Key Systems, time-division multiplexing (TDM)-based interactive voice response (IVR) systems, traditional TDM-based voice mail systems, and any other legacy (non-IP) voice processing or telephone equipment.

This chapter explores several aspects of Cisco Unified CallManager Express (Cisco Unified CME) connectivity to the PSTN, including the following:

- Standards-based telephony signaling systems and protocols supported by Cisco IOS, which, in turn, determine what traditional TDM or analog systems to which you can connect and what features you get when using this type of connection
- A brief overview of the Cisco voice gateway hardware choices and the voice port densities and features provided
- Sample Cisco IOS configurations for different types of PSTN connections
- Network design and call switching considerations for connecting to the PSTN from your IP network

Traditional telephony terminology is used throughout this chapter. It has a more precise meaning here than in other chapters, because the topic of discussion is connecting a traditional telephony system, the PSTN.

Voice gateway considerations for Cisco Unified CME deployment are in the following sections:

- Trunk Signaling Systems, page 4-2
- Cisco IOS PSTN Telephony Interfaces, page 4-4
- PSTN Call Switching, page 4-12
- Digit Manipulation, page 4-15
- PSTN Trunk Failover, page 4-18

Note For additional information, see the "Related Documents and References" section on page xii.

Trunk Signaling Systems

Cisco IOS PSTN connectivity complies with the relevant standard signaling systems used by the PSTN and other telephony-switching systems. Cisco IOS routers support most signaling variations in general use. No matter where your business is located, you should be able to connect easily to the PSTN with the analog or digital signaling options described in this section.

Analog Signaling

Low-density PSTN connectivity typically implies an analog connection. In some geographies Basic Rate Interface (BRI) is used instead, as discussed in the"Digital Signaling" section on page 4-3. Analog signaling is also used for connections to analog stations (such as fax machines and traditional analog phones). Table 4-1 summarizes the analog signaling variations supported by Cisco IOS voice gateways.

Table 4-1 Analog Signaling Support by Cisco IOS Software

Signaling	Description	Typical Use
Analog DID	Analog Direct Inward Dial	Used to connect to an analog PSTN line that has DID service for incoming calls on it.
CAMA	Centralized Automatic Message Accounting	Used to connect to the PSTN for emergency services (911 calls) in North America.
E&M	Ear and Mouth	Used to connect to an analog PBX.
FXO	Foreign Exchange Office	Generally used to connect to an analog PSTN line. Also used to connect to a PBX or Key System FXS interface. Can be connected to any interface where a standard analog phone is currently connected.
FXS	Foreign Exchange Station	Used to connect to analog phone sets or fax machines. Occasionally also used to connect to a PBX or Key System if it offers only FXO interfaces.

To connect your Cisco Unified CME system to the PSTN for normal analog business line service, use FXO interfaces. FXO ports, like all the other analog interfaces, carry one call per port, so each RJ-11 port on your Cisco Unified CME router connects to one line from the PSTN and carries a single call at a time. A second call is given a busy tone if it tries to use the same port or line.

Note On voice interface cards, such as the NM-HDA and EVM-HD-8FXS/DID, which contain a single RJ-21 50-pin connector, the individual analog ports carried in the single cable are broken into separate RJ-11 ports by a break-out box.

The FXS and FXO voice interfaces are asymmetric, but most of the other signaling methods are symmetric. This means that if the PSTN offers an FXS interface (a normal business line), your Cisco Unified CME router connects to that with an FXO interface. On the other hand, you might have a Key System with FXO interfaces being used to connect to the PSTN. If you want to connect those same ports to your Cisco Unified CME router, you will require FXS interfaces on the router to connect to these ports.

Asymmetric also means that although you can make calls in both directions across FXS and FXO connections, services typically work in only one direction. For example, caller ID is *sent* on an FXS interface and *received* on an FXO interface, but not the other way around.

Analog trunks all support a single call per physical connection or port, so you need as many ports connected to the PSTN as you require simultaneous calls from your business to the PSTN.

FXO connections do not provide dialed digits (DNIS), introducing challenges in providing automatic call switching. More information about this is provided in the "PSTN Trunk Failover" section on page 4-18. Analog DID is a variation of FXO that provides DNIS on what is, essentially, an FXO interface. Note, though, that these trunks are one-way and can only receive calls from the PSTN (they cannot make calls to the PSTN). If you use analog DID for incoming calls from the PSTN, you still need FXO trunks as well to be able to make outgoing calls to the PSTN.

Digital Signaling

If you require only a small number of simultaneous calls to the PSTN, you will most likely use analog FXO connections. In geographic locations outside North America, ISDN BRI is a likely alternative option for low-density PSTN connectivity. However, if you have a larger office and require more than approximately 10 to 16 simultaneous calls to the PSTN, a digital T1 or E1 trunk might provide a more cost-effective option. Table 4-2 summarizes the digital signaling variations supported by Cisco IOS routers.

Table 4-2 Digital Signaling Support by Cisco IOS Software

Signaling	Description	Typical Use
BRI Q.931	Basic Rate Interface	An ISDN connection to the PSTN or a PBX carrying two simultaneous voice calls. It uses the Q.931 ISDN specification. Calls are controlled via a dedicated channel called the D channel. The term 2B+D is often used for BRI describing two voice channels (or bearer [B] channels) and one signaling channel (or data [D] channel).
BRI QSIG	Basic Rate Interface	Used for PBX ISDN connectivity. It uses the Q Signaling (QSIG) variation of the basic ISDN specification.
T1 CAS	T1 Channel Associated Signaling	Used widely in North America to connect to the PSTN or PBXs. Several variations of this signaling exist, including T1 FXS, T1 FXO, and T1 E&M. T1 FXS and T1 FXO support loop start and ground start signaling.T1 E&M signaling supports delay dial, wink, and immediate dial.
T1 FGD	Feature Group D	The T1 CAS variations generally cannot convey caller ID. T1 FGD can. It is used to connect to the PSTN where caller ID is required and PRI is not an option. T1 FGD is an asymmetric protocol.
T1 and E1 PRI	Primary Rate Interface	An ISDN connection to the PSTN carrying 23 (T1) or 30 (E1) simultaneous voice calls, giving rise to the terms 23B+D and 30B+D. It uses the Q.931 ISDN specification. Calls are controlled via a dedicated signaling channel (D channel).

Table 4-2 Digital Signaling Support by Cisco IOS Software

Signaling	Description	Typical Use
T1 PRI NFAS	Nonfacility Associated Signaling	A variation of PRI available only on T1 that uses a single D channel to control multiple spans of T1s with only B channels (voice calls).
T1 and E1 QSIG	Primary Rate Interface	Used for PBX ISDN connectivity. It uses the QSIG variation of the basic ISDN specification.
E1 R2	The Regional System 2 (R2) CAS protocol	Used in South America and Asia for PSTN connectivity. Numerous country-specific variations of the R2 protocol exist.
J1	Japan interface	PBX connectivity in Japan. Japan also uses the T1 standard.

BRI connectivity on the Cisco IOS routers is supported only for switch (PSTN, PBX, or key system) connectivity—not for ISDN BRI phones.

All ISDN variations listed in Table 4-2 support both DID and caller ID, which is implicitly supported in the ISDN protocol. The CAS protocols (T1 CAS and E1 R2) might or might not support caller ID. Typically T1 CAS does not, but T1 FGD is a variation that does. All digital trunk types support DNIS and DID.

Cisco IOS PSTN Telephony Interfaces

You can add numerous modular cards to your Cisco Unified CME router to support PSTN connections of the types discussed in the preceding section. These technologies and hardware cards are not particular to Cisco Unified CME. They can be used on any Cisco router that supports the card in question—independent of whether Cisco Unified CME is enabled on the router. For example, you can choose to have two separate routers in your office—one configured for Cisco Unified CME and the other as the PSTN voice gateway—as an alternative, or you can combine both functions in the same router.

The following sections cover these hardware choices in greater detail:

- Analog Trunks, page 4-4
- Digital Trunks, page 4-7
- DSP Hardware, page 4-11
- PSTN Trunks Integrated with or Separate from Cisco Unified CME, page 4-11

Analog Trunks

Voice interfaces range from two- and four-port FXO/FXS/E&M/DID cards up to 96/120-channel quad T1/E1 interfaces. The physical telephony interface for analog and BRI ports is provided by a plug-in voice interface card (VIC) and for a T1/E1 port by a voice or WAN interface card (VWIC).

Using various combinations of VICs and VWICs on a Cisco IOS router, you can build a Cisco Unified CME system that includes a range of physical telephone interfaces. You can assemble a small analog telephony system with a few FXO ports used to connect to PSTN subscriber lines, or you can use digital telephony interfaces such as T1/E1 and ISDN BRI/PRI, or any combination of these. The specific hardware cards offering analog trunk and station (analog phone or fax machine) interfaces are discussed next.

Analog Trunk and Station Hardware

The analog interface cards listed in Table 4-3 are used to provide low-density analog PSTN interfaces. VICs are placed in a Voice Interface Card (VIC) or WAN interface card (WIC) slot (supported on the Cisco 1751 and Cisco 1760), in a high-speed WIC (HWIC) slot on the router (supported on the Cisco 2800 and Cisco 3800 series), or inside a network module (Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 series) such as the NM-HD-1V, NM-HD-2V, NM-HD-2VE, or NM-HDV2. For high-density analog PSTN interfaces, the NM-HDA (supported on the Cisco 2600, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 37xx, and Cisco 38xx) or the EVM-HD-8FXS/DID card (supported on the Cisco 2821, Cisco 2851, and Cisco 38xx) can be used.

Table 4-3 Analog Interfaces, Signaling, and Density

Interface Card	Signaling	Density
VIC-4FXS/DID	FXS and analog DID	4 ports
VIC2-2FXO	FXO and CAMA	2 ports
VIC-2DID	Analog DID	2 ports
VIC2-4FXO	FXO and CAMA	2 ports
VIC2-2FXS	FXS	2 ports
VIC2-2E/M	E&M	2 2
NM-HDA-4FXS, EM-HDA-8FXS, and EM-HDA-4FXO	FXS and FXO	4 ports on the baseboard, but can be expanded up to 12 FXS ports by adding an EM-HDA-8FXS card to the network module (NM), or up to 8 FXO ports by adding 2 EM-HDA-4FXO cards to the NM.
EVM-HD-8FXS/DID, EM-HDA-8FXS, EM-HDA-6FXO cards, and EM-HDA-3FXS/4FXO	FXS, FXO, CAMA, and analog DID	8 ports on the baseboard that can be FXS or DID. You can expand the EVM-HD to up to 24 FXS ports by adding 2 EM-HDA-8FXS cards, or up to 12 FXO ports by adding 2 EM-HDA-6FXO cards, or various combinations of FXS and FXO by adding 1 or 2 EM-HDA-3FXS/4FXO cards. The EVM-HD supports any combination of 2 EM cards.

The cards that support multiple signaling systems (such as FXS or DID, and FXO or CAMA) can be software configured on a per-port basis to support one or the other. For example, the VIC2-4FXO card can be configured to support one CAMA and three FXO ports, or two CAMA and two FXO ports.

Configuring Analog Trunks and Stations

All PSTN interfaces are configured as voice ports on the router. When you insert the card into the router, the configuration automatically creates and shows the corresponding voice ports. Directing calls to a voice port is based on the dial plan and is implemented with plain old telephone service (POTS) dial peers.

Note that the use of the 9T directive in the **destination-pattern** command of the dial peer in the following example configuration:

```
dial-peer voice 100 pots
 description PSTN
 destination-pattern 9T
 port 1/0/0

dial-peer voice 100 pots
 description PSTN
 destination-pattern 9T
 port 1/0/1
```

This command is a quick way of dealing with variable-length PSTN dial plans. The T denotes a timeout. The command **destination-pattern 9T** instructs the dial peer to match any dialed digits that start with a nine, regardless of how many digits follow. When the timeout expires, the digits are forwarded from the voice port to the PSTN. There are other, more explicit ways to make your **destination-pattern** commands match calls to the PSTN more exactly, including **9911**, **9411**, **91T**, and **9[2-9]**.

The dial peers shown in the following configuration example direct all calls (of a varying number of digits) that start with a nine to the two PSTN FXO trunks, ports 1/0/0 and 1/0/1. If no preference is given on the dial peers and both trunks are free, the Cisco IOS software chooses one of the two trunks based on an internal algorithm that considers idle times and usage of the trunks. You can control the order in which they are chosen by adding a **preference** command to the dial peer. The **dial-peer hunt** command offers additional control over the sequence in which dial peers, and therefore voice ports, are chosen.

You can also direct calls to different destinations over different trunks if required. This is shown in the following example, where calls to the 408 area code always use voice port 1/0/0, and calls to the 415 area code always use voice port 1/0/1:

```
voice-port 1/0/0

voice-port 1/0/1

dial-peer voice 100 pots
 description PSTN
 destination-pattern 9408.......
 port 1/0/0

dial-peer voice 101 pots
 description PSTN
 destination-pattern 9415.......
 port 1/0/1
```

The preceding example illustrates how you can connect to each independently and direct different types of calls to the correct trunks, if you have different local and long-distance PSTN provider connections.

If you require CAMA connectivity to comply with North American emergency calling regulations, you can configure one or more of your FXO ports for CAMA operation. This is shown in the following example, where port 2/0/3 on a VIC2-4FXO card is configured for CAMA signaling. The following example configuration illustrates this command usage:

```
voice-port 2/0/0

voice-port 2/0/1
   signal ground-start

voice-port 2/0/2

voice-port 2/0/3
   signal cama KP-NPD-NXX-XXXX-ST
```

Note For more information about the **signal** command, see your applicable Cisco IOS Command Reference. The following applies to Cisco IOS 12.3(T): http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a0080.

Analog Trunk Features

With analog FXO interfaces, caller ID information received for an incoming PSTN call is displayed on the IP phones. You can optionally enable the Flash softkey on your IP phones. Pressing the Flash softkey on the IP phone generates a hookflash signal on the FXO port and allows you to exercise PSTN subscriber line services, such as PSTN call waiting and three-way calling. However, Cisco IOS FXO ports do not support PSTN call waiting caller ID display.

You can also set up a direct link between a specific PSTN telephone line and an individual button on an IP phone. This is useful if you want to use PSTN-based voice mail services where a stutter dial tone on the PSTN line indicates that a message is waiting.

As mentioned earlier, in the "Analog Signaling" section on page 4-2. FXO interfaces are asymmetric. As such, calls can be disconnected in only one direction in pure FXO operation. The historic reasons for this are beyond the scope of this publication. Suffice it to say that today FXO ports are widely used as two-way trunks, and special care must be taken that calls disconnect properly in both directions and do not hang the port. You can use the following Cisco IOS commands on the voice port to facilitate proper call disconnect on FXO ports:

- **battery-reversal**
- **signal groundstart**
- **supervisory disconnect anytone**
- **supervisory disconnect dualtone**

The selection of a particular command depends on the complementary features provided by your PSTN CO switch. It also varies based on geographic location and the technology available in the CO.

In addition, FXO signaling does not receive dialed digits (DNIS). This means that an incoming call from the PSTN to an FXO port cannot be switched automatically by your Cisco Unified CME system to an extension, because there are no digits from the PSTN to tell Cisco Unified CME where to switch it. You can overcome this shortcoming of FXO signaling by using auto-terminate directives on the FXO voice port to switch the call to a predetermined destination. Commands you can explore include **connection plar** and **connection plar-opx**, which are described in the "PSTN Call Switching" section on page 4-12.

Digital Trunks

Digital trunks can be low-density (for example, BRI with two calls per port) or high-density (such as T1 or E1 ports with 24 or 30 calls per port, respectively). The specific hardware cards offering digital trunk interfaces are discussed in the following sections.

Digital Trunk Hardware

The digital interface cards listed in Table 4-4 are used to provide a range of low- to high-density digital PSTN interfaces.

Table 4-4 Digital Interfaces, Signaling, and Density

Interface Card	Signaling	Density
VIC2-2BRI-NT/TE	Q.931 or QSIG BRI	2 ports with 2 voice channels each.
NM-HDV	T1 and E1	Up to 2 T1/E1 ports. Up to 48 (T1) or 60 (E1) voice channels. Used in conjunction with a VWIC-1MFT-T1/E1 or VWIC-2MFT-T1/E1.
NM-HD-2VE	Analog, BRI, T1, and E1	Up to 4 T1/E1 ports, or 2 T1/E1 and 2 BRI ports, or 4 BRI ports. Up to 24 voice channels. Used in conjunction with a VWIC-1MFT-T1/E1, VWIC-2MFT-T1/E1, or VIC2-2BRI-NT/TE.
NM-HDV2	Analog, BRI, T1, and E1	Up to 4 T1/E1 ports, or 2 T1/E1 ports and 2 BRI ports. Up to 120 voice channels. Has up to 2 onboard T1/E1 ports. For the additional ports, a VWIC-1MFT-T1/E1 or VWIC-2MFT-T1/E1 is used. For BRI, the VIC2-2BRI-NT/TE card is used inside the NM.
EVM-HD-8FXS/DID, EM-4BRI-NT/TE	Analog and BRI	Up to 8 BRI ports (16 voice channels).
VWIC-1MFT-T1/E1 or VWIC-2MFT-T1/E1 in a WIC slot	T1 and E1	Up to 2 T1/E1 ports. Channel density depends on the router platform and where the DSPs are accessed from.

In the general case, a T1 port offers 24 voice channels, and an E1 port offers 30 voice channels. When using ISDN signaling, where one channel is dedicated to call control signaling (the D channel), a T1 carries 23 voice channels, and an E1 carries 30 voice channels. (An E1 always has a channel dedicated to signaling, no matter what type of protocol is used. With T1 this is not normally the case; using ISDN takes away one of the standard channels.)

You might not use the maximum number of channels on these ports, depending on what your PSTN service provider offers. You can configure your Cisco IOS router with any number of channels on the T1 or E1 interface, but it must be complemented by what is configured on the PSTN CO on the other side.

Fractional T1 service is quite common in North America and allows you to subscribe to PSTN T1 service with, for example, only 12 or 16 channels of service (and this service costs less than a full T1 of 24 channels). This service can be either T1 CAS or T1 PRI. Another service is to multiplex your WAN connection (Frame Relay or Point-to-Point Protocol [PPP]) on some channels of the same physical T1 used for your PSTN voice connection. For example, channels 1 to 6 could offer a 384-Kbps PPP WAN connection; channels 10 to 20 could offer ten channels of PSTN voice service using T1 E&M signaling.

Fractional E1 service is much less common. Your lower-density PSTN connectivity options in geographies that use E1 connectivity may be multiples of BRI until such time as a full E1 makes sense for your business.

Configuring Digital Trunks

Digital PSTN interfaces are configured in general just like analog interfaces—that is, as voice ports and POTS dial peers on the router to direct calls to the ports. The dial peer control and configuration are exactly the same, regardless of what type of voice port used.

T1/E1 ports, however, show up as controllers in a basic configuration (by just inserting the hardware into the router). Unlike an analog interface, the voice port is not created until you add more configuration details to the controller. T1/E1 ports are used for both data and voice access. Until you add specific configuration statements, the router does not know what your intention is with the T1/E1 port. Add a voice configuration to a T1/E1 port by using either the **ds0-group**, **tdm-group,** or **pri-group** command. A data T1/E1 port is configured with the **channel-group** command.

You often see the terms CAS and *common channel signaling* (*CCS*) when reading about T1/E1 trunks. CAS generally means that the signaling to control the call uses the same channel (or timeslot) as the call's media path. This is common on T1 interfaces. (It is also called *robbed-bit signaling* because a few bits out of the 64-kbps channel are "stolen" from the media path to convey call control information, such as on-hook and off-hook.) CCS means that a channel is dedicated to signaling. This channel carries the call control information for all the voice calls (media paths) on that same T1/E1 interface. For example, channel 16 on an E1 is used exclusively for call control and carries the control information for all the other channels (1 to 15 and 17 to 31) on that interface.

The following configuration example illustrates a T1 CAS (E&M immediate start) PSTN connection using a **ds0-group** configuration. In this example, you can see that the second port on the VWIC shows up as controller T1 2/1. This means that the hardware has been detected but no configuration has been done for this port

```
controller T1 2/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-immediate-start

controller T1 2/1

voice-port 2/0:0
 signal immediate

dial-peer voice 100 pots
 description PSTN
 destination-pattern 9T
 port 2/0:0
```

In this example, all 24 channels on the T1 are configured. But you could as easily have stated **ds0-group 0 timeslots 1-10** if you agreed with your provider to get only ten channels of PSTN service on this T1 (fractional T1 service). The result of the **ds0-group** command is that voice port 2/0:0 is created. The POTS dial peer, in this example, looks the same as the one in the FXO example earlier, except that it now points to voice port 2/0:0, which is a T1 port.

Note For more information about digital trunks, see the following document: http://www.cisco.com/en/US/tech/tk652/tk653/technologies_configuration_example09186a008010f05d.shtml

If you are using ISDN PRI service to the PSTN, you use the **pri-group** command to insert a voice configuration on a T1 or E1 controller. The following configuration example shows a sample configuration for a T1 PRI trunk.

```
isdn switch-type primary-5ess

controller T1 2/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
```

```
interface Serial2/0:23
 no ip address
 isdn switch-type primary-5ess
 isdn incoming-voice voice

voice-port 2/0:23
 echo-cancel coverage 64

dial-peer voice 100 pots
 description PSTN
 destination-pattern 9T
 port 2/0:23
```

Geographic variants of ISDN are controlled by the **switch-type** setting. A default router setting, seen in the preceding example as the first line in the configuration, is specified at the Cisco IOS global level (the **isdn switch-type** command). This default can be overridden on a per-interface basis by the **switch-type** statement under the controller. In the preceding example, both are set to **primary-5ess**, but they could be different. If they are different, the statement on the controller takes precedence.

The D- channel interface (**interface Serial 2/0:23**) and voice-port (**voice-port 2/0:23**) commands are automatically created by the insertion of the **pri-group** command on the controller. The POTS dial peer again looks exactly the same as in previous examples. You must adjust the voice port to which it refers.

Digital Trunk Features

For PRI/BRI interfaces using ISDN signaling, you can optionally allow the IP phone's full DID name and number to be used as the calling party's identity for outgoing calls. This puts extension-specific information into the PSTN billing records for the call. This can be useful if you want to rely on the PSTN provider's billing information to track the internal origin point of PSTN calls made from your Cisco Unified CME system. Alternatively, you can block IP phone extension-specific information from the outgoing ISDN call and instead substitute the general public phone number for your system.

Generally, PSTN providers do not use name information delivered to the PSTN by a subscriber system. Although the name can be included in the ISDN call setup, the PSTN typically overrides this with the information associated with the subscriber in the PSTN's own databases. You can, however, receive name display information from the PSTN on ISDN trunks, and display this on the IP phones in your business.

All digital trunks provide DID (or DNIS) information. ISDN trunks also provide caller ID delivery. Fractional CAS and PRI are supported on the Cisco IOS routers. If you configure fractional PRI, the D channel for the T1 must be on channel 24 and for E1 on channel 16. This cannot be customized. The voice channels (B channels) can be any subset of the remaining channels.

ISDN channels cannot be customized to be incoming only or outgoing only. However, through creative use of dial peers, you can limit the number of incoming or outgoing calls to and from your business. You cannot specify the exact channel each call should use. With T1 CAS, you have more granular control, because you can specify separate ds0-groups (up to a ds0-group per channel). Each ds0-group creates a separate voice port that you can control via dial peers as to what calls may reach those channels. The following configuration example illustrates this feature.

```
controller T1 2/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 0 timeslots 1-10 type e&m-immediate-start
 ds0-group 1 timeslots 15-20 type e&m-immediate-start

controller T1 2/1
```

```
voice-port 2/0:0
 signal immediate

voice-port 2/0:1
 signal immediate

dial-peer voice 100 pots
 description PSTN
 destination-pattern 9408.......
 port 2/0:0

dial-peer voice 101 pots
 description PSTN
 destination-pattern 9415.......
 port 2/0:1
```

The **ds0-group 0 timeslots 1-10** command results in voice port 2/0:0, and the **ds0-group 1 timeslots 15-20** command creates voice port 2/0:1.

DSP Hardware

Digital signal processor (DSP) technology provides voice compression, echo cancellation, tone generation, and voice packetization functions for servicing voice interfaces and converting the voice for transport over packet networks. To drive a PSTN voice connection, the analog or digital voice port must have access to a DSP for the call.

Some voice NMs include internal slots into which DSP modules can be plugged, and others have fixed DSP configurations. In some router models, such as the Cisco 1760, Cisco 2800, and Cisco 3800 series, you can plug DSP cards directly into the router's motherboard.

VWIC cards offer only physical T1/E1 port connections, and VIC cards offer only the physical analog or BRI ports. If a VIC or VWIC card is inserted into a router WIC slot (supported on the Cisco 1751, Cisco 1760, Cisco 28xx, and Cisco 38xx), the DSPs are typically provided by the onboard DSP cards. A VIC or VWIC inserted into an NM typically draws on DSPs resident on the NM itself.

One other variation is to use a VWIC in a WIC slot on the Cisco 2600 or Cisco 3700 series platforms, which do not support onboard DSPs. For this configuration, you can use a DSP AIM card such as the AIM-VOICE-30 or the AIM-ATM-VOICE-30 card. An Advanced Integration Module (AIM) is an internal plug-in module that fits on the router's motherboard. The AIM-based DSPs cannot drive analog or BRI VIC cards, only T1/E1 VWICs.

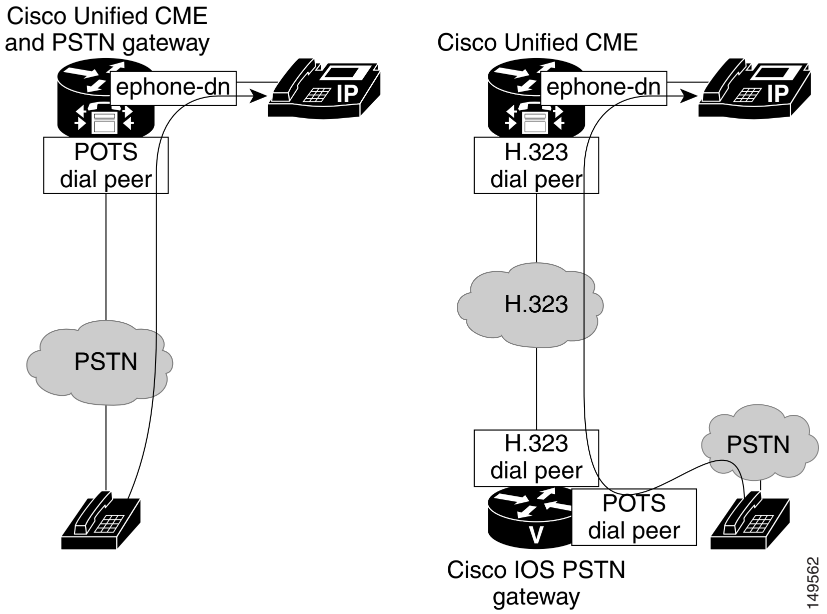
DSP cards for motherboard and NM-based slots come in many densities and use various DSP technologies. All are called packet voice/fax DSP module (PVDM) cards.

PSTN Trunks Integrated with or Separate from Cisco Unified CME

In a typical deployment, the PSTN connectivity for your business is integrated into your Cisco Unified CME router. However, you could also use a separate router platform as your PSTN gateway. You may choose to do this because you already have a router that acts as your PSTN gateway in your office or because the slot density on your Cisco Unified CME router is insufficient for the PSTN connectivity your office requires.

For PSTN trunks integrated onto your Cisco Unified CME router, the voice call is switched directly from the POTS interface to the IP phone and is straightforward to configure. Placing the PSTN gateway on a different platform gives you an H.323 (or SIP) call leg between the PSTN gateway and the Cisco Unified CME call controller where the IP phones are managed. This requires POTS dial peers on the PSTN gateway to direct calls to the PSTN interfaces, as shown in the previous configuration examples in this chapter. It requires H.323 dial peers to direct calls from the PSTN gateway to IP phones and from the IP phones to the PSTN gateway. From an H.323 standpoint, this configuration is similar to connecting two separate Cisco Unified CME systems via an H.323 VoIP interface between them. This is shown in Figure 4-1.

Figure 4-1 Integrated or Separate PSTN Gateways



We recommend that you deploy Cisco Unified CME with an integrated PSTN gateway, because this approach results in a much simpler network design and configuration. If Cisco Unity Express is used for the automated attendant (AA) or voice mail on your Cisco Unified CME system, the H.323 VoIP leg must be converted to a SIP call leg before the call can successfully terminate on the Cisco Unity Express application. For this type of implementation, we recommend Cisco Unified CME 3.2 because with Cisco Unified CME 3.2 and later, you can use the Cisco IOS translation shown in the following configuration example.

```
voice service voip
 allow-connections h323 to sip
```

PSTN Call Switching

The preceding sections explored the various PSTN trunk types, signaling methods, and router hardware you can use to connect to the PSTN. But there are more considerations than just physical connectivity. One thing to keep in mind is that the PSTN numbers and your internal extension numbers are almost certainly not the same, at least not the same length. Digit translation must occur to map one set of numbers to another. You will learn more about this in the "Digit Manipulation" section on page 4-15.

Another consideration is what PSTN numbers (and how many) your business has or needs. Do you have just one main office number, and the receptionist directs all calls to the correct employee? Do you need an AA menu to have callers switch to the person or service they want to speak to? Should you have DID numbers for all or some of your employees? Do you prefer a Key System type of operation, where a series of PSTN numbers appear as distinct line appearances on a number of phones, and any employee can pick up any call? There is interaction between your business needs, the PSTN service you get from your provider, the capabilities of the physical connection to the PSTN, and the Cisco Unified CME configuration (IP phone button appearances) to use.

The physical connection is likely dictated by cost, your office's geographic location, and the number of voice channels your office needs. You might want DID service for your business. However, if it is not offered in your area at a cost-effective level, you have little choice but to implement for non-DID service.

The following sections explore considerations about how calls may be routed depending on whether you have DID service and how you can handle calls to non-DID destinations within your business:

- PSTN Call Switching with DID Enabled, page 4-13
- PSTN Call Switching with DNIS (No DID), page 4-13
- PSTN Call Switching with No DNIS (FXO Trunks), page 4-14

PSTN Call Switching with DID Enabled

Many offices deploying Cisco Unified CME have DID capability from the PSTN provider for some subset of employees. PSTN calls to DID destinations can be switched automatically to the employee's phone without any manual intervention.

There are two situations to consider, depending on how DID numbers are allocated to destinations within your business:

- All employees, the AA, and voice mail pilot numbers have DID numbers assigned. In this configuration, PSTN calls can be switched as follows:
  - The main office number (non-DID calls) terminates on the AA pilot (for AA assistance) or on an IP phone extension (for receptionist assistance).
  - Employee DID numbers terminate on the extension for that person's IP phone.
  - The number employees call from PSTN locations to check their voice mail terminates on the voice mail pilot number.
- Some employees have DID numbers assigned, and others do not. In this configuration, PSTN calls are handled as follows:
  - Calls to the main office number and for PSTN voice mail checking are handled as per the preceding scenario.
  - Calls to employees with DID numbers terminate on the extension for that person's phone.
  - Calls to employees without DID numbers terminate on the AA (or receptionist's extension). These callers then can dial through or be transferred to the extension of the person they want to reach.

PSTN Call Switching with DNIS (No DID)

PSTN call switching with DNIS and no DID is not a likely configuration, but it is possible. In this configuration, your business does not have DID service and, therefore, has only a single main office number from the PSTN provider although you have multiple trunks. Or even if you have multiple PSTN numbers, they are not associated with particular employees, but instead are just alternate main office numbers.

Although the dialed number is delivered via DNIS from the PSTN to the PSTN gateway, it is of little use to switch calls to individual destinations. In this situation, you have two configuration choices:

- Regardless of the dialed number, all PSTN calls are terminated on the AA pilot (for AA assistance) or on a specific phone extension (for receptionist assistance).
- All PSTN lines appear on multiple phones (Key System operation). Any employee at these phones can answer any of the lines, regardless of what number the caller dialed.

If all calls are directed to the AA (or a receptionist), *caller-busy* conditions must be carefully considered. For example, you need to determine what should happen if all AA ports are busy or all the receptionists are busy. If you do not want busy tone returned, more ports or receptionists may be required, or alternate destinations to switch calls to (lower-preference dial peers) or DID service may be needed for high-volume destinations in your business.

PSTN Call Switching with No DNIS (FXO Trunks)

If the office has only FXO trunks, no DNIS (or DID) capability is technically possible. This scenario is very common for a small standalone office or a small branch of a bigger network that has only a few business lines from the local CO.

Because no dialed digits (DNIS) are available on FXO trunks, these calls must be autoterminated on a predetermined destination (most often the AA or the receptionist's extension) — or these calls must ring all phones that have the line appearance on them (in Key-system mode). This can be achieved with a private line automatic ringdown (PLAR) configuration on the voice port where a particular destination extension is associated with the trunk, and all calls arriving on that trunk are switched as if they had dialed the configured extension. This syntax is shown in the following configuration example, where all calls arriving on the FXO trunk on slot 1/0/0 are switched as if they had dialed extension 6800.

```
voice-port 1/0/0
  connection plar opx 6800
```

Most small offices have multiple FXO trunks to the PSTN because each trunk can carry only a single call. One or more PSTN numbers may be associated with these trunks or this trunk group, depending on the PSTN service the business subscribes to. Generally, there are two possibilities:

- *A single PSTN main office number*—In this configuration, all calls from the PSTN are terminated (via the PLAR feature) to the AA pilot (for AA assistance) or to a specific phone extension (for receptionist assistance).
- *Multiple PSTN numbers*—This might consist of one PSTN number for the main office and another for voice mail retrieval by employees. In this case, calls on main office trunks are switched as in the preceding case, and calls to voice mail are switched (via PLAR) to the voice mail pilot number. Clearly, these two types of calls must be delivered on different physical trunks or trunk groups so that each is autoterminated to the correct destination.

Sharing all FXO trunks across all PSTN calls (the first case in the preceding list) results in better trunk utilization than assigning distinct FXO trunk(s) to the main office number and other distinct FXO trunk(s) to the voice mail pilot number (the second case).

Digit Manipulation

There are various reasons to manipulate the digits dialed by the caller on a voice system. The most common reason is to allow both internal calls (from other extensions) and external calls from the PSTN (where a full E.164 phone number is delivered) to terminate directly on the user's phone without needing a receptionist to intercept and redirect the call.

Note E.164 is an International Telecommunication Union (ITU) recommendation that describes international telephone dial plans. It specifies phone number attributes such as international dialing codes, regional (area) codes, and the minimum and maximum length of each field in the phone number. Voice systems use the E.164 criteria to parse and interpret phone numbers. PSTN numbers are always fully qualified E.164 numbers, whereas extensions within your business typically are not, because they are private numbers of local significance only.

Here are some other reasons to translate (or manipulate) digits:

- To allow IP phone users to call each other directly by extension, and also to access the PSTN
- To allow for site access codes in a multisite on-net dial plan and to strip these digits to extract the extension as soon as the destination site is reached
- To allow for variable-length external (off-net) dialing while maintaining fixed-length internal dialing
- To block calls to certain numbers
- To redirect calls to certain numbers

For example, suppose your employee, UserU1, is at extension 3001, and her PSTN DID number is 4xx-5yy-3001. Without some form of digit manipulation or live intercept, a call incoming from the PSTN that dialed 4xx-5yy-3001 will not match the ephone-dn definition for UserU1's phone, which contains only her extension, 3001. Therefore, a method is needed to translate the string 4xx5yy3001 to 3001.

Several Cisco IOS digit manipulation tools can translate phone numbers. The following are the most common:

- Dial peer commands
- Cisco Unified CME **dialplan-pattern** command
- Cisco IOS translation rules

Dial Peer Commands

You can include several commands on a POTS dial peer to add, suppress, or substitute the digits forwarded to the PSTN trunk interface:

- **destination-pattern**
- **digit-strip**
- **forward-digits**
- **prefix**
- **translate-outgoing**
- **translation-profile**

Dial peer commands are useful if only small changes to the beginning or end of the dialed number are necessary, such as prefixing an area code, prefixing a CO designator (NXX) to an extension number, or forwarding only the last four digits of a longer number. The wildcard matching within the **destination-pattern** command automatically deletes the numbers explicitly matched. For example, when 5yy3001 is dialed and is matched by a dial peer that contains the command destination-pattern 5yy...., the default operation is to forward only the digits 3001.

Note For more information about **digit-manipulation** commands referenced in this section, see the Cisco IOS Command Reference for you Cisco IOS Release listed with the appropriate Cisco IOS Documentation Set at the following URL:
http://cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html

Cisco IOS Translation Rules

For more extensive digit manipulation, such as a wholesale change of a number or substituting digits in the middle of a number, translation rules are much more powerful. Translation rules are regular expressions attached to the dial peer with the **translation-profile** command.

Note For more information about voice translation rules, see the "Voice Translation Rules (Doc ID: 16083)" presented on Cisco.com.

Like the other dial peer commands discussed in the preceding section, translation rules are a generic Cisco IOS feature that allows manipulation of called numbers, calling numbers, and number types. It can also be attached in such a way that it translates calls in only one direction, either incoming or outgoing.

The following example illustrates configuration commands for a T1 PRI trunk, with translation profile **to_261x** attached for incoming calls (calls from the PSTN to the Cisco IOS PSTN gateway). Translation profile **to_261x**, in turn, references **translation rule 23**, which has ten rules specified. This CLI segment intercepts all calls incoming from the PSTN over this T1 PRI that contains a dialed number ending in the range 12610 to 12619. It does not matter what (or how many) numbers precede this range; for example, it could be 5xx-3y1-2610 or 5y1-2618. The numbers that match the rule (12610 to 12619) are translated to a completely unrelated number so that none of the original digits survive. To illustrate, if a call with a dialed number of 5xx-3y1-2610 arrives, it is translated to 32085, and an IP phone (or other dial peer) associated with that extension receives the call. A PSTN call with a dialed number of 5y1-2618 results in extension 79988 receiving the call.

```
voice translation-rule 23
 rule 1 /12611/ /37002/
 rule 2 /12612/ /37262/
 rule 3 /12613/ /37990/
 rule 4 /12614/ /57514/
 rule 5 /12615/ /30631/
 rule 6 /12616/ /50043/
 rule 7 /12617/ /28787/
 rule 8 /12618/ /79988/
 rule 9 /12619/ /68278/
 rule 10 /12610/ /32085/

voice translation-profile to_261x
 translate called 23

controller T1 2/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24

interface Serial2/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice

voice-port 2/0:23
 echo-cancel coverage 64

dial-peer voice 1261 pots
 translation-profile incoming to_261x
 incoming called-number 1261.
 direct-inward-dial
 port 2/0:23
```

The syntax for translation rules can be cryptic if you are unfamiliar with regular expressions, but these rules can provide a powerful facility to manipulate digits. Translation rules are not tied to Cisco Unified CME, so you can use it on any Cisco IOS voice-enabled router.

Here are some considerations when using the Cisco IOS voice translation rules feature:

- These rules make for a very powerful overall feature that can do almost any translation of digits required, but using these rules can be complicated and, therefore, prone to errors for inexperienced implementers.
- Being a generic Cisco IOS feature, the feature's rules apply to all calls that traverse the router. It can be applied at a global level, dial peers, and ephone-dns (Cisco Unified CME IP phones).
- The digits are manipulated before dial peer matching and call termination.
- Calling and/or called numbers can be manipulated on every call based on what is configured.
- The rules can be directionally applied to incoming or outgoing calls (or both).

When applying translation rules to ephone-dns, there is a side effect that if no rule is matched, an extra post-dial delay is incurred. As a workaround, create a dummy translation rule that acts as a pass-through. For example, if no rule is applied to extension-to-extension calls, and the extensions all start with 5, add a rule that "translates" 5 to 5, just to make sure that a rule is always matched, and the delay is not incurred.

Cisco Unified CME dialplan-pattern Command

The Cisco Unified CME **dialplan-pattern** command allows E.164 numbers to be mapped to extension numbers or, put another way, to extract the extension number from a longer DID number. The **dialplan-pattern** command does not actually translate the number (although the result from a call routing point of view is the same). It instead creates multiple dial peers that allow different dialed numbers to terminate on the same phone.

The **dialplan-pattern** command can be used in some cases (calls to IP phones) to achieve the same call routing as can be achieved by using translation rules. Because these two features operate differently, you should think carefully about which method to use. If you use both methods, you should be clear about how these might interplay with each other to affect your call routing. The **dialplan-pattern** command is explained in more detail in Chapter 6, "Connecting Multiple Cisco Unified CallManager Express Systems with VoIP."

The CLI shown in the following example illustrates the same mapping as the number translation discussed previously for employee UserU1.

```
telephony-service
```

```
load 7960-7940 P00303020214
max-ephones 48
max-dn 192
ip source-address 10.1.3.1 port 2000
system message CUE System 2691
create cnf-files version-stamp 7960 Jul 15 2003 13:48:12
dialplan-pattern 1 510395.... extension-length 4
voicemail 6800
max-conferences 8
web admin system name cue password cue
dn-webedit
time-webedit
```

Some considerations about using the Cisco Unified CME **dialplan-pattern** feature include the following:

- Feature provides a straightforward method to translate from full E.164 numbers to shorter extension numbers on Cisco Unified CME.
- It is a Cisco Unified CME feature, so it applies only to calls to and from IP phones controlled by Cisco Unified CME. It does not apply to calls from the PSTN gateway directly to the AA or voice mail pilot numbers. Therefore, if digit manipulation is needed on these calls, one of the other two methods must be used.
- The IP phone extension must have at least one digit in common with the original called number and be in the same sequence. (If the extension is completely different from the called number, or not in sequence, Cisco IOS translation rules must be used to manipulate the digits.)
- Like Cisco IOS translation rules, the digits are manipulated before dial peer matching and call termination.
- It manipulates the *called* number on a call to an IP phone and the *calling* number of a call from an IP phone. This operation is implicit and cannot be controlled or altered.
- The E.164 number patterns generated by the **dialplan-pattern** command can be registered to an H.323 gatekeeper or SIP proxy. Digit translations done with Cisco IOS translation rules are not registered to H.323 gatekeepers or SIP proxies.

PSTN Trunk Failover

Larger offices that use a digital trunk, such as a PRI, often need a backup method to connect to the PSTN. This requirement results in the PRI being the main PSTN connection point in addition to FXO trunks (typically used to back up a T1) or BRI interfaces (typically to back up an E1) used if the main interface is down.

In this configuration, the dial peers directing calls to the main interface must be duplicated to also point to the backup interface. You can prioritize calls to use the main interface when it is available by using the **preference** command on the dial peers pointing to these trunks.

Another need is to have a backup mechanism for a small office with FXO trunks if a power failure occurs. FXO hardware supports a feature called FXO Power Failover that allows a hardware (relay) connection between a *red* phone (a specially dedicated analog telephone in your office that normally is not in use) and the PSTN line, in case the router is not powered.

On Cisco voice hardware, the NM-HDA-4FXS FXO expansion card (the EM-HDA-4FXO) and the EVM-HD-8FXS/DID FXO expansion card (the EM-HDA-6FXO) each have one port per card that has this power failover capability. Other Cisco FXO hardware cards do not support this feature.

Note For more information about the **preference** command in relation to dial peer configuration, see the following URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7f30.html#wp1109642

CHAPTER 5

Cisco Unified CallManager Express Call Transfer and Forward

Configuring call transfer and forwarding for H.323 VoIP calls is a fairly complex task in most real-world H.323 VoIP networks. This is especially true if you have a mixture of H.323 VoIP systems from different vendors. Even if you have an all-Cisco H.323 VoIP network, there are still interactions to consider, unless all your VoIP systems are running relatively up-to-date Cisco IOS software. This means having at least Cisco IOS Release 12.3 software in all your voice-enabled routers. Ideally, you should have Cisco IOS Release 12.3(4)T or later software (this is the Cisco Unified CallManager Express (Cisco Unified CME) 3.0 base code version). There are also some special considerations if you are using a Cisco Unified CallManager in addition to your Cisco IOS-based Cisco Unified CME systems addressed in Chapter 6, "Connecting Multiple Cisco Unified CallManager Express Systems with VoIP." The good news is that with the right software and configuration, there are workable solutions for most of your VoIP call transfer and forwarding needs.

In a VoIP network, getting an optimized system working for call transfer and forwarding requires the active cooperation of all endpoints involved in a call transfer or call forward. This means your ability to perform a call transfer or forward depends on the capabilities of the calling party's VoIP system as well as your Cisco Unified CME system configuration. A call transfer also depends on the capabilities of the final VoIP system that you are transferring the call to.

In traditional TDM-based PBX telephony, call transfer and forwarding usually operate within the limited scope of a single PBX system and, therefore, are simpler operations. For example, you are often limited to call transfers between extensions on the same PBX only.

In a VoIP-based system, you can potentially transfer or forward calls between any VoIP endpoints, regardless of their physical location. Of course, being able to do this in practice requires making sure that you have support for transfer and forwarding built into all your VoIP endpoints.

With Cisco Unified CME, you have three basic choices for the protocol used to support call transfer and forwarding for H.323 VoIP calls:

- **Standards-based H.450**—Recommended because it provides for optimal call paths and unlimited sequential transfers and forwards.
- **Cisco H.323 extension**—Mostly obsolete, but useful if you are using software older than Cisco IOS Release 12.2(15)T.
- **Hairpin call routing**—Allows for maximum compatibility, but uses more WAN bandwidth and results in higher delay and jitter.

The default H.323 call transfer protocol used by Cisco Unified CME is the Cisco mechanism. This mechanism supports only blind call transfer (that is, no transfer consultation). It is selected as the default simply for purposes of backward compatibility with earlier Cisco IOS releases.

The default call forwarding mechanism provides for automatic local forwarding only (that is, within the same Cisco Unified CME system). It does not provide forwarding display update notification of the call forwarding to the calling party's IP phone. For incoming VoIP calls from another Cisco Unified CME system that are nonlocally forwarded to a third Cisco Unified CME system, the Cisco-proprietary H.323 protocol extensions are used.

Even if you do not require H.323 VoIP call transfers (because you do not need to make calls across an IP connection to another site), you should still select the H.450 configuration method for call transfers. This enables call transfer with consultation for local calls within your system and for PSTN calls that use PSTN voice ports that are physically on your Cisco Unified CME router. (PSTN voice ports on a router other than the Cisco Unified CME system appear as H.323 VoIP calls to the Cisco Unified CME system.) It also prepares your system to use the standards-based H.450 protocol in case you want to add support for H.323 or SIP VoIP transfer and forwarding to another site at some point in the future.

Sections that follow address the following topics:

- Call Transfer Methods for VoIP, page 5-2
- Cisco Unified CME VoIP Call Transfer Options, page 5-4
- Call Forward Methods for VoIP, page 5-4
- Cisco Unified CME VoIP Call Forwarding Options, page 5-5
- Transfer and Forward Proxy Function, page 5-6
- Call Transfer and Forward Interoperability with Cisco Unified CallManager, page 5-7
- Call Transfer and Forwarding with Routed Signaling H.323 Gatekeepers, page 5-8

Note For additional information, see the "Related Documents and References" section on page xii.

Call Transfer Methods for VoIP

This section describes several methods for implementing call transfer across VoIP networks:

- H.450 and SIP, page 5-2
- Hairpin Routing, page 5-3
- H.450.12, page 5-3
- Empty Capabilities Set, page 5-3

H.450 and SIP

The ITU-T standards-based H.450.2 transfer method and the Cisco method operate in a similar way. In both cases, when a call transfer occurs, a control message is sent back to the transferee party to request that the transferee initiates a follow-on call from the transferee to the final transfer-to destination. In the H.450.2 case, the follow-on call originated by the transferee can act to replace the transfer consultation call that is in progress between the transferor and the transfer-to destination party. The consultation call between transferor and transfer-to and the original transferee-transferor call are not torn down until the "replaces" operation is completed successfully. The term *replaces* is used here in the context of "Call 2 replaces call 1." If for any reason the replacement operation fails, it is usually possible for the transferor to reconnect the call to the transferee. The H.450.2 mechanism works in a manner similar to the REFER method used for SIP VoIP calls. The Cisco transfer mechanism does not support the call replacement mechanism and, therefore, allows you to perform only blind call transfers. This proprietary method is similar to the older BYE/ALSO method that was used to perform blind transfers for SIP VoIP calls. The BYE/ALSO method has been mostly superseded by the SIP REFER method.

Both of these H.323 call transfer methods result in an optimal direct call path between the transferee and the transfer-to party after the call transfer is committed.

Hairpin Routing

The third alternative is to hairpin route the VoIP call transfer. In this case, the original transferee-to-transferor VoIP call leg is kept, and a second transferor to transfer-to VoIP call leg is created for the consultation call phase of the transfer. When the transfer is committed, the original and consultation call legs are simply bridged together at the Cisco Unified CME router. This method has the advantage that it has no end-to-end dependency on the capabilities of the transferee or transfer-to VoIP endpoint.

It also has disadvantages. One significant disadvantage is that the final transferred call is relayed through the transferor’s Cisco Unified CME system. This means that the transferred call continues to consume resources on the transferor Cisco Unified CME system even after the transfer is committed. It also means that the media path for voice packets for the transferred call may hairpin route through the transferor’s Cisco Unified CME system, so both the original call and the transferred call continue to consume WAN bandwidth. If the amount of WAN bandwidth is limited, this may prevent new VoIP calls from being established until the transferred call is terminated. The other significant disadvantage of hairpin routing calls is the cumulative bandwidth, delay, and jitter problems that occur if a call is transferred multiple times (chained or sequential transfers).

H.450.12

You can compromise between the H.450.2 and hairpin routing call methods by turning on the H.450.12 protocol on your Cisco Unified CME system (this is recommended). You must be using at least Cisco Unified CME 3.1 to use H.450.12. With H.450.12 enabled, your Cisco Unified CME system can use the H.450.12 protocol to automatically discover the H.450.x capabilities of VoIP endpoints within your VoIP network. When H.450.12 is enabled, the Cisco Unified CME system can automatically detect when an H.450.2 transfer is possible. When it isn’t possible, the Cisco Unified CME system can fall back to using VoIP hairpin routing. Cisco Unified CME also can automatically detect a call from a (non-H.450-capable) Cisco Unified CallManager.

Empty Capabilities Set

For the sake of completeness, it is worth mentioning a fourth alternative for call transfers: Empty Capabilities Set (ECS). Cisco Unified CME does not support the instigation of transfer using ECS. But because a Cisco Unified CME router also has the full capabilities of the Cisco IOS Release H.323 voice infrastructure software, it can process receipt of an ECS request coming from a far-end VoIP device. In other words, a Cisco Unified CME system can be a transferee or transfer-to party in an ECS-based transfer. A Cisco Unified CME system does not originate a transfer request using ECS. The problem with ECS-based transfers is that in many ways they represent a combination of the worst aspects of the end-to-end dependencies of H.450.2 together with the cumulative problems of hairpin for multiple transfers. Many ECS-based transfer implementations do not allow you to transfer a call that has already been transferred in the general case of VoIP intersystem transfers.

Cisco Unified CME VoIP Call Transfer Options

Your Cisco Unified CME system by default is set up to allow local transfers between IP phones only. It uses the Cisco H.323 call transfer extensions to transfer calls that include an H.323 VoIP participant.

To configure your Cisco Unified CME system to use H.450.2 transfers (this is recommended), set **transfer-system full-consult** under the **telephony-service** command mode. You also have to use this configuration for SIP VoIP transfers.

To configure your Cisco Unified CME system to permit transfers to nonlocal destinations (VoIP or PSTN), set the **transfer-pattern** command under **telephony-service**. The **transfer-pattern** command also allows you to specify that specific transfer-to destinations should receive only blind transfers. You also have to use this configuration for SIP VoIP transfers. The **transfer-pattern** command allows you to restrict trunk-to-trunk transfers to prevent incoming PSTN calls from being transferred back out to the PSTN (employee toll fraud). Trunk-to-trunk transfers are disabled by default, because the default is to allow only local extension-to-extension transfers.

To allow the H.450.12 service to automatically detect the H.450.2 capabilities of endpoints in your H.323 VoIP network, use the **supplementary-services** command in voice service voip command mode.

To enable hairpin routing of VoIP calls that cannot be transferred (or forwarded) using H.450, use the **allow-connections** command. The following example shows a call transfer configuration using this command.

```
voice service voip
   supplementary-service h450.12
   allow-connections h323 to h323
telephony-service
   transfer-system full-consult
   transfer-pattern .T
```

The configuration shown in the preceding example turns on the H.450.2 (**transfer-system full-consult**) and H.450.12 services, allows VoIP-to-VoIP hairpin call routing (**allow-connections**) for calls that don't support H.450, and permits transfers to all possible destinations (**transfer-pattern**). The transfer permission is set to **.T** to provide full wildcard matching for any number of digits. (The T stands for terminating the transfer destination digit entry with a timeout.)

The following example shows a configuration for more restrictive transfer permissions.

```
telephony-service
   transfer-system full-consult
   transfer-pattern 1...
   transfer-pattern 2... blind
```

This example permits transfers using full consultation to nonlocal extensions in the range 1000 to 1999. It also permits blind transfers to nonlocal extensions in the range 2000 to 2999.

Call Forward Methods for VoIP

This section describes different mechanisms for handling call forwarding in a VoIP network:

- H.450.3 Call Forwarding, page 5-5
- H.323 Facility Message, page 5-5
- VoIP Hairpin Call Forwarding, page 5-5

You can configure your Cisco Unified CME to handle VoIP call forwarding in several different ways. Select the method to use depending on how you want forwarding to operate.

Cisco Unified CallManager Express Solution Reference Network Design Guide

H.450.3 Call Forwarding

You can use the ITU-T H.450.3 standard for call forwarding (this is recommended). It has some similarities to H.450.2 (call transfer). When a call is forwarded, an H.450.3 message is sent back to the calling party requesting that the caller reoriginate a follow-on call to the forwarded-to destination. If Cisco Unified CME is configured to use H.450.3, it is used even if the forward-to destination is another local IP phone within the same Cisco Unified CME system as the forwarding phone (or forwarder). Use this method if you want the calling VoIP party to always be able to see the phone number he or she is being forwarded to. Just like the H.450.2 transfer case, use of H.450.3 requires that all the VoIP endpoints in your VoIP network support H.450 services.

H.323 Facility Message

The second choice is to use the quasi-standard H.323 Facility Message mechanism for forwarding. This is the default call forwarding configuration for Cisco Unified CME. This method is used as the default, because it provides backward compatibility with earlier (and current) Cisco IOS releases. It's also quite widely supported by third-party and nonCisco IOS VoIP systems. When this mechanism is used, an H.323 Facility Message is sent back to the VoIP caller only for the case of forwarding to a nonlocal number. If the forward-to destination is local to the forwarding phone, the call forward operation is handled internally within the Cisco Unified CME system. In this case, the remote calling IP phone cannot update its display to show the forwarded destination.

VoIP Hairpin Call Forwarding

Your third choice is to use VoIP call hairpin routing. This is similar to the call transfer hairpin option. A second independent VoIP call leg is created for the forwarded call leg. This leg is bridged to the original incoming VoIP call leg. As for the transfer hairpin case, the disadvantage of this approach occurs if you have to support sequential or chained forwarding. Sequential hairpin forwarding of VoIP calls results in accumulated bandwidth and jitter/delay issues.

Just like the call transfer discussion, if you have to deal with only local LAN and PSTN connections and do not have to route VoIP H.323 calls across a WAN connection, you can just configure your system for H.450.3 operation to get your system ready to interoperate with other H.450-capable endpoints if you need this in the future.

You can also compromise between the H.450.3 and hairpin configuration by using the H.450.12 service to automatically detect H.450.3-capable VoIP endpoints, and fall back to hairpin routing for calls that do not support H.450.3.

Cisco Unified CME VoIP Call Forwarding Options

Your Cisco Unified CME system by default is configured to support internal local forwarding. It sends only H.323 Facility Messages back to the VoIP caller for nonlocal VoIP forwarding destinations. If you have direct PSTN access on your Cisco Unified CME system, PSTN destinations accessed via local ports are considered local for the purposes of this discussion.

To turn on H.450.3 services for VoIP calls, you use the **call-forward pattern** command under **telephony-service**. This command lets you conditionally select H.450.3 service based on matching the calling party's telephone number. This lets you invoke H.450.3 for calls only from VoIP phone numbers that you know support H.450.3. You can configure the matching pattern to use **.T** to match all possible calling party numbers. This is similar to the match-all configuration used with the **transfer-pattern** command.

To permit VoIP-to-VoIP hairpin call routing for forwarded calls, set the **allow-connections** command under **voice services voip**. If you've already done this to allow hairpin transfers, you don't need to do it again for call forwarding.

As with the H.450.2 transfer case, you can turn on the H.450.12 service to compromise and allow H.450.3 where possible, and fall back to hairpin forwarding otherwise. Note that H.450.12 support was introduced in Cisco Unified CME 3.1.

The following example shows a basic configuration.

```
voice service voip
   supplementary-service h450.12
   allow-connections h323 to h323
telephony-service
   call-forward pattern .T
```

Transfer and Forward Proxy Function

The transfer and forward discussion so far in this chapter has related to the configuration of a single Cisco Unified CME system to cope with various possible VoIP network scenarios, including networks that have endpoints with mixed capabilities. If you have a network of Cisco Unified CME systems, you should consider partitioning it to provide a section that contains only H.450-capable endpoints. This allows you to gain the full set of H.450 service benefits within the group of VoIP network devices that support them. You can then link this segment of your VoIP network to the non-H.450 network using a Cisco IOS router configured to act as an H.450 IP-to-IP gateway.

An H.450 IP-to-IP gateway can act as a proxy for H.450.2 and H.450.3 services on behalf of VoIP devices that don't support H.450. Calls between the H.450 and non-H.450 devices can be routed to pass through the H.450 IP-to-IP gateway. H.450 messages originated by Cisco Unified CME systems can be terminated on the H.450 IP-to-IP gateway, which can invoke hairpin call routing for transfers and call forwarding as needed.

An H.450 IP-to-IP gateway makes the most sense if your network topology is arranged in a hub-and-spoke fashion. Consider a network design that has a number of Cisco Unified CME systems located at the end of WAN link spokes connected to a central hub network. In this type of network, it often makes sense to locate an H.450 IP-to-IP gateway at the central hub and to use it as a linkage point to act as a bridge into the non-H.450 segment of the VoIP network. With an H.450 IP-to-IP gateway, calls that enter the H.450 network segment through the IP-to-IP gateway can be transferred and forwarded using H.450 services within the H.450 segment of the network. Calls transferred or forwarded to destinations outside the H.450 segment are hairpin routed as needed by the H.450 IP-to-IP gateway. If the H.450 IP-to-IP gateway is located at a central hub location, hairpin routing the call at the hub is a better option than hairpin routing the call from a Cisco Unified CME system located at the far end of one of the network spokes over a WAN link. Figure 5-1 in the next section shows a IP-to-IP gateway.)

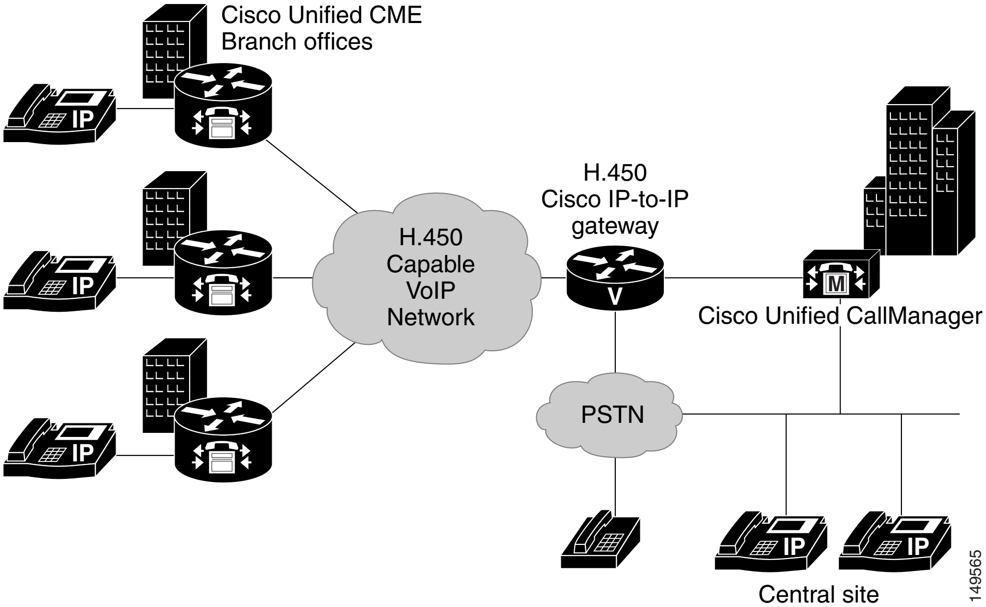
Call Transfer and Forward Interoperability with Cisco Unified CallManager

Cisco Unified CallManager 4.0 and earlier does not support H.450 services. Cisco Unified CME 3.1 can automatically detect H.323 calls that go to or come from Cisco Unified CallManager. It does this using H.323 information elements included in H.323 call setup, progress, alerting, and connect messages. You can optionally turn on H.450.12 services for calls to Cisco Unified CallManager, and use the lack of H.450.12 indications to invoke hairpin VoIP call routing by your Cisco Unified CME systems, but this is not required.

You may have a VoIP network in which turning on H.450.12 produces ambiguous results as far as the detection of H.450.2 and H.450.3 capabilities. One example of this occurs when you have older Cisco Unified CME 3.0 (or even Cisco ITS [the earlier Cisco Unified CME name] 2.1) systems in your network. Although Cisco Unified CME 3.0 systems do support H.450.2 and H.450.3, they don't support H.450.12 capabilities indications. If you turn on H.450.12 on your Cisco Unified CME 3.1 systems and you also have some older Cisco Unified CME 3.0 routers, the Cisco Unified CME 3.1 systems assume that the Cisco Unified CME 3.0 routers cannot perform H.450.2/3 services, because no H.450.12 indication is forthcoming from the Cisco Unified CME 3.0 systems. So in a network with a mixture of Cisco Unified CME 3.0, Cisco Unified CME 3.1, and Cisco Unified CallManagers, it makes sense to turn off the H.450.12 service and assume that all endpoints can perform H.450.2/3 except for the endpoints that are detected as explicitly being Cisco Unified CallManager systems.

Also, if you have a Cisco Unified CallManager system, it is probably located at a central corporate site with Cisco Unified CME systems at branch offices. This arrangement lends itself naturally to a hub-and-spoke network design with the Cisco Unified CallManager at the hub and the Cisco Unified CME systems at the ends of the network spokes. This type of network design is a good candidate for an H.450 IP-to-IP gateway using the H.450 IP-to-IP gateway to front-end the Cisco Unified CallManager and act as a proxy for H.450 services between the Cisco Unified CallManager and the network of Cisco Unified CME systems. The H.450 IP-to-IP gateway can also be configured to act as the PSTN Voice gateway for the Cisco Unified CallManager system (using either H.323 or MGCP), so you don't need to dedicate a separate router for the H.450 IP-to-IP gateway. It can also provide centralized PSTN access for the Cisco Unified CME systems. Performance wise, calls that pass through the H.450 IP-to-IP gateway consume a similar amount of CPU and memory resources as a call terminated by the router as a PSTN gateway call. See Figure 5-1.

Figure 5-1 H.450 IP-to-IP Gateway



Cisco Unified CallManager 4.0 or earlier should be configured to interface with Cisco Unified CME systems or an H.450 IP-to-IP gateway using H.323 Inter-Cluster Trunk (ICT) mode and a Media Termination Point (MTP). In addition, Cisco Unified CallManager 3.3(3) should be configured to disable H.323 fast-start.

Call Transfer and Forwarding with Routed Signaling H.323 Gatekeepers

An H.323 gatekeeper that uses routed signaling acts as a call proxy for basic A-to-B calls. All calls that reference the gatekeeper have H.323 signaling that passes through the gatekeeper. The presence of this type of gatekeeper in your network has a significant impact on your network from the H.450 service point of view. Your routed signaling gatekeeper may or may not support H.450 services. It may be able to pass through H.450 messages transparently, or it may block some or all of them. It may even be able to act as an H.450 IP-to-IP gateway.

A worst-case design approach for dealing with a routed signaling gatekeeper would be to assume that H.450.2/3 services do not work through the gatekeeper. In this case you can configure your Cisco Unified CME systems to force hairpin routing of all VoIP calls that have to transfer or forward back into the VoIP network. You can do this by turning off H.450 services under the **voice service voip** command, as shown in the following example.

```
voice service voip
   no supplementary-service h450.2
   no supplementary-service h450.3
   allow-connections h323 to h323
telephony-service
   call-forward pattern .T
   transfer-system full-consult
   transfer-pattern .T
```

Note Note that by default, the H.450.12 service is disabled, so there is no need to specifically include commands to turn it off.

Connecting Multiple Cisco Unified CallManager Express Systems with VoIP

This chapter describes the ways in which you can use Cisco Unified CallManager Express (Cisco Unified CME) as a component of a larger network using the two major Voice over IP (VoIP) protocols—H.323 and SIP—to link multiple Cisco Unified CME systems. It examines some of the considerations that apply within a networked environment that do not arise in simpler standalone configurations. This chapter focuses on the call handling implications of using Cisco Unified CME in a network.

The following sections address specific multiple Cisco Unified CME deployment issues:

- Considerations When Integrating Cisco Unified CME in H.323 and SIP VoIP Networks, page 6-1
- Integrating Cisco Unified CME in an H.323 Network, page 6-4
- DTMF Relay for H.323, page 6-17
- Call Transfer and Call Forwarding in an H.323 Network Using H.450 Services, page 6-20
- Integrating Cisco Unified CME in a SIP Network, page 6-30

Note For additional information, see the "Related Documents and References" section on page xii.

Considerations When Integrating Cisco Unified CME in H.323 and SIP VoIP Networks

H.323 is the dominant protocol deployed for VoIP networks from an installed-base perspective. Because H.323 is more mature than SIP, you can expect to see increased real-world interoperability between different vendors' H.323 products, particularly with basic call handling. However, many of the high-level VoIP networking considerations that apply to H.323 apply equally in the SIP context. Some technical and protocol-specific differences exist between H.323 and SIP VoIP networking, but for the most part, you'll find more commonality than difference, at least at the level of technical detail that this chapter addresses.

The shared aspects of the two protocols means that the overall high-level architecture and distribution of hardware and primary component roles within your VoIP network don't significantly depend on which protocol you choose to use for intersite VoIP. For networks built on either H.323 or SIP, you are dealing with peer-to-peer communication between sites. Therefore, you also need some kind of telephone number directory system to be able to resolve the IP address of the appropriate destination VoIP peer device for intersite calls.

In contrast, this similarity between H.323 and SIP does not extend to Media Gateway Control Protocol (MGCP) (and also Skinny Client Control Protocol [SCCP]), which takes a significantly different approach to telephony. Of course, it is still possible to connect Cisco Unified CME to MGCP networks, primarily using either H.323 or SIP. Many MGCP Call Agent implementations (using MGCP internally for phone control) use H.323 or SIP to connect separate Call Agents (as intersystem peer-to-peer). Cisco Unified CME itself does not support control of MGCP endpoints. Cisco Unified CME uses SCCP for phone control, and SCCP shares many common traits with MGCP.

The term *VoIP* here specifically describes “long-distance” VoIP telephone calls that traverse a WAN. This interpretation excludes SCCP used to control local IP phones. Although SCCP technically does use VoIP technology, it is primarily used in the context of operating voice calls within the confines of a LAN with more or less unlimited bandwidth and many fewer concerns about security.

You can view the H.323/SIP versus SCCP contrast as the difference between interbranch office voice traffic and intrabranch office voice traffic, or alternatively as long distance (WAN) versus local VoIP (LAN). This division is useful in many ways, because it inherently supports the often-necessary difference in treatment of calls between internal and external phone users.

In some cases, you might want to treat H.323 calls as internal calls and not want a high degree of differentiation in the treatment of LAN versus WAN calls, such as calls between separate systems on two floors of the same building. Cisco Unified CME has features that address this, although currently you cannot treat a network of many Cisco Unified CME systems as if they are a single logical entity with full intersite feature transparency. Both H.323 and SIP still have obstacles to overcome before this is really possible. Not least of these are issues surrounding meaningful interoperability with another company’s devices for services beyond basic calls.

When you extend VoIP calling into the WAN space, you might also have to consider the difference between VoIP calls that come from other Cisco Unified CME nodes within your WAN network versus VoIP calls that are from VoIP Public Switched Telephone Network (PSTN) gateways or even from other independent external/wholesale VoIP carrier networks. You can link independent VoIP networks together and into your corporate VoIP network using IP-to-IP gateways. This arrangement may be desirable if you want to obtain international and long-distance phone service directly from a carrier-class VoIP service provider and have this linked at the VoIP level to your private enterprise VoIP network.

Note For more information about Cisco IP-to-IP Gateway functionality, see the document at: http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_qanda_item09186a00801da69b.shtml

SIP potentially has some advantages over H.323 in terms of separating intersite VoIP calls from true external VoIP calls, because SIP uses the Internet concept of domains. It is a fair assumption that all of the intersite calls will use the same root domain name and that this fact can be used to make the required distinction. However, from a purely practical security point of view, you will probably want any truly external VoIP traffic entering your corporate VoIP network to pass through an IP-to-IP gateway and also a firewall, regardless of whether you choose to use SIP or H.323. This means that you should have the opportunity to appropriately classify and mark the external calls at the point of entry in either type of network.

Alternatively, you can keep your VoIP network entirely separate at the IP level and simply connect into VoIP service provider carrier networks through time-division multiplexing (TDM)-based PSTN-like gateways (at some cost in terms of increased end-to-end voice path delay). For the sake of simplicity and clarity, the rest of this chapter ignores the IP-to-IP possibility and includes only the PSTN gateway scenario. For many reasons, what is on the far side of the gateway—whether PSTN or IP-to-IP—is not hugely significant. It’s the gateway’s job to take care of whatever adaptation is needed to provide the interconnection path.

Note When you configure SIP or H.323 on a router, the ports on all its interfaces are open by default. This makes the router vulnerable to malicious attackers who can execute toll fraud across the gateway if the router has a public IP address and a public switched telephone network (PSTN) connection. To eliminate the threat, you should bind an interface to private IP address that is not accessible by untrusted hosts. In addition, you should protect any public or untrusted interface by configuring a firewall or an access control list (ACL) to prevent unwanted traffic from traversing the router.

Cisco Unified CME uses the standard ports summarized in Table 6-1 for call signaling, and media transport. The same ports are used by Cisco Unified CallManager and Cisco IOS voice gateway products.

Table 6-1 Cisco Unified CME VoIP Port Numbering

Protocol	Port Numbers	Port Type
H.225 (call signaling)	1720	TCP
SIP	5060	UDP/TCP
RTP	16384 to 32768	UDP (dynamic)
RTP (LAN)	2000	UDP
SCCP	2000	TCP
H.245	11000 to 11999	TCP (dynamic)
H.225 RAS	1719	UDP
Unicast GK Discovery	1718	UDP
Multicast GK Discovery	223.0.1.4	UDP

Integrating Cisco Unified CME in an H.323 Network

There are two basic approaches to connecting a Cisco Unified CME system to an H.323 network: the first uses no gatekeeper (GK), and the second does. A direct interconnection of sites with H.323 implies that each site must be knowledgeable about how to reach every other site. This works well in small networks of only a handful of nodes, but as the network grows larger, the configuration becomes increasingly cumbersome to maintain. In its simplest form, a gatekeeper is a device that provides a directory service that translates a telephone number into an IP address. Using a gatekeeper provides significant scalability by centralizing the interconnection of the individual sites so that each site needs to be aware of only the gatekeeper and not every other site in the network.

The following sections discuss different approaches to building H.323-based Cisco Unified CME networks:

- A Simple Two-Node Topology with H.323, page 6-5
- A Large Multinode Topology with H.323, page 6-7
- The Role of an H.323 Gatekeeper, page 6-9
- Public and Internal Phone Numbers in an H.323 Network, page 6-13
- Registering Individual Telephone Numbers with a Gatekeeper, page 6-15
- Internal and External Callers for VoIP, page 6-16

Rather than being alternative approaches, they represent a simpler approach for smaller networks with only a few nodes and a more scalable approach for larger multinode networks.

A Simple Two-Node Topology with H.323

In the simplest case, you can just connect two Cisco Unified CME systems via an IP-enabled serial data link (or Ethernet), and configure VoIP dial peers on each system to symmetrically direct calls that are destined for nonlocal extension numbers to the other Cisco Unified CME system. In other words, if the Cisco Unified CME recognizes that the extension number being dialed is not present in its internal list of phone numbers, it can assume that it should send the call to the other Cisco Unified CME, as shown in Figure 6-1.

Figure 6-1 Simple Two-Node Cisco Unified CME H.323 Network

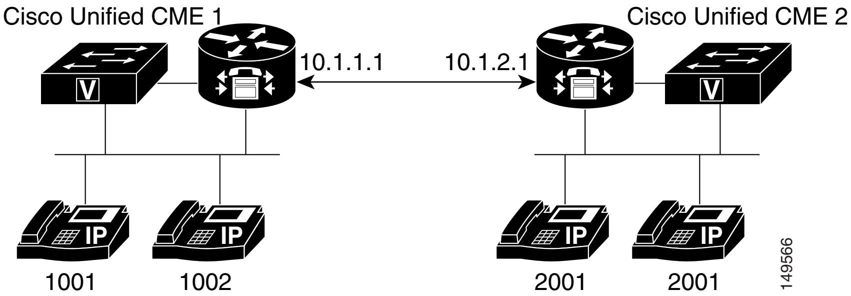
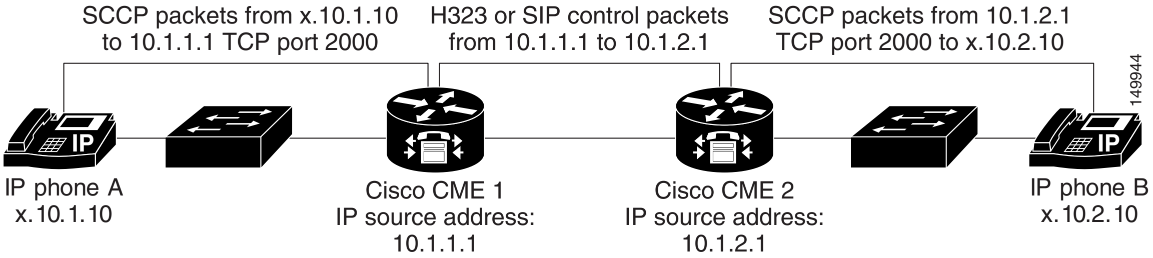

Cisco Unified CME 1
Cisco Unified CME 2
10.1.1.1
10.1.2.1
V
V
IP
IP
IP
IP
1001
1002
2001
2001
149566

Figure 6-2 and Figure 6-3 present flow diagrams illustrating proxy behavior between Cisco Unified CME nodes in the two-node H.323 network illustrated in Figure 6-1.

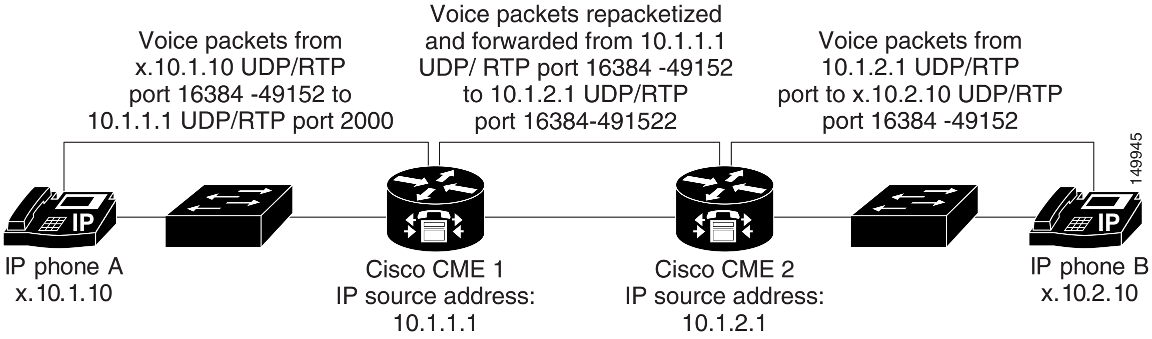
For VoIP across the WAN, all skinny and H.323 call control packets are proxied by the IP source address of the local Unified CME router. See Figure 6-2.

Figure 6-2 Cisco Unified CME VoIP Call Flow—Call Control Packet Proxy Behavior


SCCP packets from x.10.1.10
to 10.1.1.1 TCP port 2000
H323 or SIP control packets
from 10.1.1.1 to 10.1.2.1
SCCP packets from 10.1.2.1
TCP port 2000 to x.10.2.10
IP
IP
IP phone A
x.10.1.10
Cisco CME 1
IP source address:
10.1.1.1
Cisco CME 2
IP source address:
10.1.2.1
IP phone B
x.10.2.10
149944

After call signaling is established, RTP/UDP media traffic will be proxied by IP source address UDP/RTP port 2000 of the local Unified CME router. See Figure 6-3.

Figure 6-3 Cisco Unified CME VoIP Call Flow—RTP/UDP Traffic Proxy Behavior


Voice packets from x.10.1.10 UDP/RTP port 16384 -49152 to 10.1.1.1 UDP/RTP port 2000
Voice packets repacketized and forwarded from 10.1.1.1 UDP/ RTP port 16384 -49152 to 10.1.2.1 UDP/RTP port 16384-491522
Voice packets from 10.1.2.1 UDP/RTP port to x.10.2.10 UDP/RTP port 16384 -49152
149945
IP
IP phone A x.10.1.10
Cisco CME 1 IP source address: 10.1.1.1
Cisco CME 2 IP source address: 10.1.2.1
IP phone B x.10.2.10

The following examples show the relevant configuration extracts of the two systems. It shows a pair of Cisco Unified CME systems that have extensions 1000 to1099 on *Cisco Unified CME 1* (IP address 10.1.1.1) and 2000 to 2099 on *Cisco Unified CME 2* (IP address 10.1.2.1).

- Cisco Unified CME 1

```
dial-peer voice 2000 voip
     destination-pattern 20..
     session target 10.1.2.1
     dtmf-relay h245-alphanumeric
     codec g729r8
     no vad
telephony-service
ip source-address 10.1.1.1 port 2000
```

- Cisco Unified CME 2

```
dial-peer voice 1000 voip
     destination-pattern 10..
     session target 10.1.1.1
     dtmf-relay h245-alphanumeric
     codec g729r8
     no vad
telephony-service
ip source-address 10.1.2.1 port 2000
```

Note The **dtmf-relay** configuration portion of the output is explained in the "DTMF Relay for H.323" section on page 6-17.

You can use this simple symmetrical VoIP dial peer technique to join two Cisco Unified CME systems even within a single site to increase the total phone count supported beyond the capacity of a single Cisco Unified CME system. The downside of doing this is that it does not give you a truly monolithic system from a configuration, inter-Cisco Unified CME feature transparency, and management point of view. This arrangement requires you to administer the two systems separately, which may be acceptable if the two systems are split between naturally different and separate sections of your company (for example, administration and manufacturing).

This arrangement also limits the phone features you can use across the two systems. You can operate simple features such as call transfer and forwarding, and you can share a single voice mail device between systems, including inter-Cisco Unified CME distribution of message waiting indication (MWI). However, Cisco Unified CME does not support more advanced features, such as shared line and call pickup, across the H.323 or SIP interconnection.

One final point about this arrangement is that you can optionally choose to provide a physical PSTN connection on just one Cisco Unified CME system and have that Cisco Unified CME system also act as a VoIP PSTN gateway for the second Cisco Unified CME system.

Although this discussion considers H.323 and SIP "long-distance" protocols, the use of these protocols is not related to physical distance. You can use H.323 and SIP to link systems 1000 feet apart the same as you would link systems 1000 miles apart. This ability is one of the key advantages of VoIP technology over traditional TDM systems. With the appropriate IP infrastructure, you can link systems and users more or less independent of the physical distance that separates them. This means that you can give a remotely located Cisco Unified CME system a phone extension number and voice mailbox that appears to your phone users to belong to their local Cisco Unified CME system (with the aforementioned restriction on advanced phone feature operation between systems across VoIP). The historical out-of-area-code restrictions that apply to traditional TDM-based centrex phone systems largely do not apply in the VoIP context.

The one caveat in this area is the impact on access to public emergency services. Users dialing for emergency assistance (such as police, fire, or ambulance) should be routed into the PSTN via a PSTN connection that is local to their physical location. The calling party information provided to the PSTN connection and emergency services operator for this type of call must display an appropriate phone number (and therefore an associated physical location) that is within the emergency services area of the PSTN link being used.

A Large Multinode Topology with H.323

If you want to connect more than two Cisco Unified CME systems, you can extend the basic approach used to connect two systems and add a third, fourth, or more Cisco Unified CME systems—up to a point. For a low number of systems, such as five or six, it's usually possible to add VoIP dial peers to your Cisco Unified CME system that indicate the static IP address of the other system to reach. This is especially true if your dial plan is reasonably well segmented such that you can infer to which Cisco Unified CME system the call should be sent based on the first one or two digits of the dialed extension number. For example, Cisco Unified CME system 1 is given extension numbers 5000 to 5099, Cisco Unified CME system 2 is given extension numbers 5100 to 5199, and so on.

Even if your dial plan is not entirely evenly divided, you can still use this approach if you are prepared to build the necessary dial peer-based configuration. At the limit of this method, you can construct systems in which you create an individual H.323 VoIP dial peer on each Cisco Unified CME system for each remotely located extension number. You can follow this approach as far as available memory and your patience in creating and maintaining the configuration allow. As the number of dial peers increases, the post-dial delay increases somewhat, because the Cisco Unified CME system might need to search through a couple hundred dial peers to find the right information. In the very worst case, a network of five Cisco Unified CME systems with 20 extensions each would need 80 VoIP dial peers created (and maintained) on each system. That is assuming that your extension number distribution is fully random across the full set of Cisco Unified CME systems. Troubleshooting such a system in the event of misconfiguration is challenging, however.

Another drawback of the multiple dial peer configuration is that there is no good way to do call admission control (CAC) in order to prevent an excessive number of voice calls from trying to use the same WAN link at the same time. This can be an issue if your expected maximum call volume might be greater than the capacity of your WAN links. See the next section for more on this issue.

Cisco IOS software has a built-in CAC mechanism with the **call threshold** interface command. This feature limits both inbound calls and outbound calls for a specific interface on the Unified CME router once a maximum threshold has been exceeded. For example, the following command causes calls from GigabitEthernet0/0 to be rejected after the number of simultaneous inbound/outbound calls exceeds five. Calls are then allowed once the maximum number of simultaneous calls falls below 3.

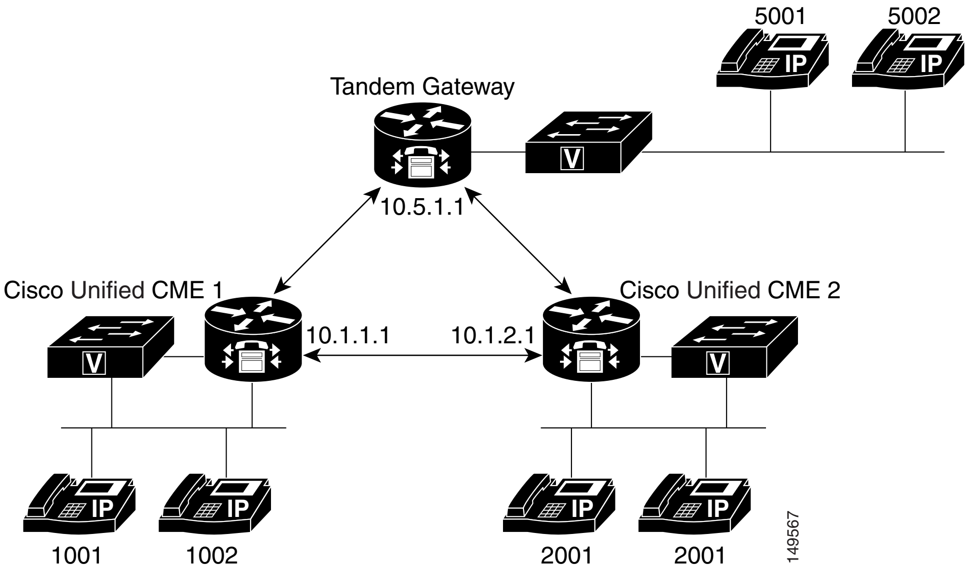
```
call threshold interface GigabitEthernet0/0 int-calls low 3 high 5
```

The benefit of this feature is that it does not require gatekeeping and can operate across multiple dial-peers. It is not subject to dial-peer maximum connection limitations. The limitation of this mechanism is that the maximum number of simultaneous calls is an aggregate of the total inbound and outbound calls. You cannot set up different thresholds for outbound or inbound calls using this mechanism.

Alternatively, you can use the VoIP Tandem Gateway feature of Cisco Unified CME 3.1 and above. This allows you to construct hub-and-spoke or hop-by-hop call routing arrangements. Hub-and-spoke call routing arrangements are historically common in small-scale voice over Frame Relay (VoFR) and voice over ATM (VoATM) networks. In these small-scale networks, you might have a single larger “hub” Cisco Unified CME system with approximately 100 users at a primary site, with perhaps five satellite Cisco Unified CME systems, each with 20 users linked on VoIP “spokes” to the primary. In this arrangement, only the central hub site needs VoIP dial peers to be configured to define the location of all network-wide extensions. The spoke satellite sites only need to know to send nonlocal calls to the hub site. The central hub site can then relay the call to the final spoke site destination.

This type of arrangement makes the most sense if the physical (Layer 1 and Layer 2) connectivity topology of your IP transport network mirrors the same hub-and-spoke arrangement as the dial plan. With this situation, IP packets that flow between different spoke sites inevitably get IP Layer 3 routed via the central hub site Cisco Unified CME router. The hub-and-spoke dial plan arrangement causes the VoIP calls and voice packets to get routed by the application layer instead, with relatively minor added delay, as shown in Figure 6-4.

Figure 6-4 Multinode Cisco Unified CME Tandem Gateway H.323 Network



The following example shows the relevant configurations of the nodes shown in the network.

- Cisco Unified CME 1

```
dial-peer voice 2345 voip
   destination-pattern [2345]0..
   session target ipv4:10.1.5.1
   no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1345 voip
```

```
   destination-pattern [1345]0..
   no vad
session target ipv4:10.1.5.1
```

- Tandem Gateway Node

```
voice service voip
   allow-connections h323 to h323
   dial-peer voice 1000 voip
      destination-pattern 10..
      session target ipv4:10.1.1.1
      no vad
   dial-peer voice 2000 voip
      destination-pattern 20..
      session target ipv4:10.1.2.1
      no vad
```

Using a single dial peer at the spoke sites to direct calls to the hub site and all far-end spoke sites beyond it also allows you to more easily use CAC per dial peer call-counting mechanism (which you'll learn more about in the following section). This is shown in Figure 6-4. You can use regular expressions in dial peer destination patterns. For example, if you need a single dial peer that references extensions in multiple ranges, such as 10xx, 30xx, 40xx, and 50xx (not including 20xx), you can use the following command:

destination-pattern [1345]0..

The values in square brackets ([ ]) provide a list of alternative values—in this case, 1, 3, 4, and 5. You can also use this to encompass a continuous range. For example, you can also write the preceding example as 1,3-5:

destination-pattern [13-5]0..

However, an even better and fundamentally more scalable approach to inter-Cisco Unified CME H.323 VoIP call routing is to use an H.323 GK (as you will see in the next section). This is the most practical approach to link tens or hundreds of Cisco Unified CME systems.

The Role of an H.323 Gatekeeper

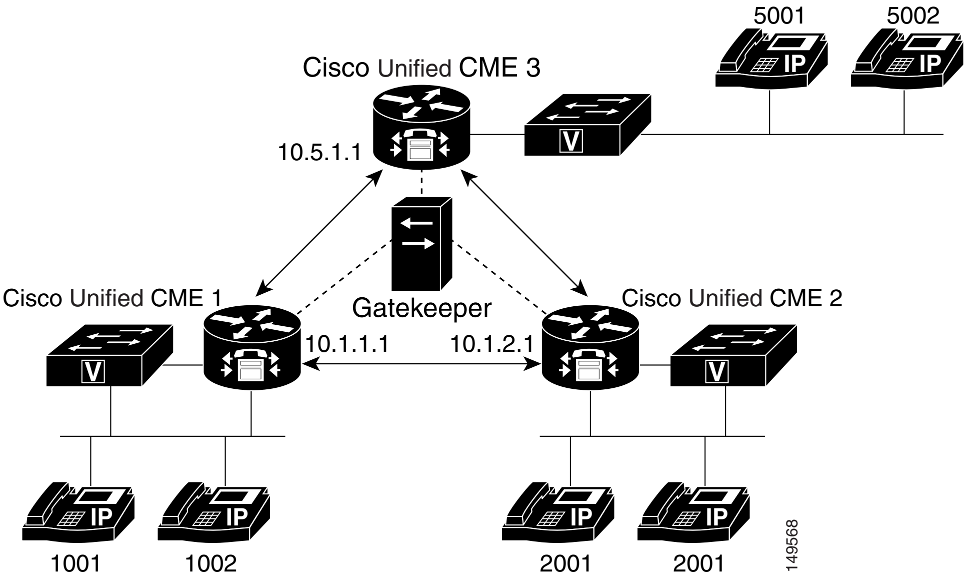
The primary role of an H.323 gatekeeper is to provide a conversion lookup between a telephone number and an IP address. This service essentially centralizes the dial plan (all the telephone numbers in the network and how to reach them) in a single place in the network, as opposed to each node needing the configuration information to do this. This significantly eases the management of a large network.

Gatekeepers also provide other services, depending on the type of gatekeeper used. These services are discussed in this section:

- Telephone Address Lookup, page 6-11
- Call Admission Control, page 6-11
- Billing, page 6-12
- Using a Gatekeeper as a Proxy for Additional Services, page 6-12

Figure 6-5 shows a sample gatekeeper network.

Figure 6-5 Multinode Cisco Unified CME Gatekeeper Network



The following example shows the relevant dial peer configurations of the nodes shown in the network:

Note Note the use of **session target ras**; it is explained in the next section.

- Cisco Unified CME 1

```
dial-peer voice 2345 voip
   destination-pattern [2345]0..
   session target ras
   no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1345 voip
   destination-pattern [1345]0..
   session target ras
   no vad
```

- Cisco Unified CME 3:

```
dial-peer voice 1234 voip
   destination-pattern [1234]0..
   session target ras
   no vad
```

The following example shows a more detailed example from an individual Cisco Unified CME router setup to interwork with an H.323 gatekeeper connected via the Cisco Unified CME router's Ethernet interface. Note that the **gk ipaddr** comand defines the gatekeeper's IP address.

```
interface FastEthernet0/0
ip address 10.1.1.1 255.255.0.0
load-interval 30
duplex auto
speed auto
no cdp enable
h323-gateway voip interface
h323-gateway voip id gk ipaddr 10.1.10.1 1719
h323-gateway voip h323-id cme1
```

```
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 10.1.1.1

dial-peer voice 1234 voip
       destination-pattern [1-4]0..
       session target ras
       no vad
```

Telephone Address Lookup

The simplest type of gatekeeper provides only telephone number-to-IP address resolution. When a Cisco Unified CME system uses a gatekeeper to help route a call, it sends a message to the gatekeeper to request the IP address that corresponds to a certain specific phone number. As soon as Cisco Unified CME gets the correct IP address, it can send an H.323 call setup message for the desired phone number to the IP address of the remote Cisco Unified CME system (provided by the gatekeeper) that hosts that phone number. Instead of having a VoIP dial peer that points to every Cisco Unified CME system in your network, the Cisco Unified CME has only one dial peer that points to the IP address of the H.323 gatekeeper.

To reference a gatekeeper from a VoIP dial peer, use **ras** as the target instead of a specific IP address:

session target ras

In most cases, the H.323 gatekeeper gets the appropriate phone number-to-IP address configuration dynamically from the component Cisco Unified CME systems. For each individual phone number that is configured on a Cisco Unified CME system, the Cisco Unified CME system can send a Registration message to the gatekeeper. The Registration message basically says, “I’m an H.323 gateway-like device at IP address x.x.x.x, and I have phone number Y.” The gatekeeper aggregates the information from the H.323 Registration messages from all the Cisco Unified CME gateways (and other H.323 gateways) into a composite database that contains all the current locations of all the telephone numbers in the network.

Call Admission Control

In addition to providing simple telephone number-to-IP address resolution, a gatekeeper can provide call admission control (CAC) for your VoIP network. CAC keeps track of the number of simultaneous VoIP calls present at each H.323 gateway and prevents overloading of the gateway’s WAN links (and sometimes also provides load balancing for PSTN access ports). Without CAC, if too many calls attempt to use the same WAN link at the same time, either calls will fail in uncontrolled ways, or too many voice packets will try to get sent at the same time, leading to voice quality problems.

The Cisco Unified CME can do a limited amount of CAC itself without a gatekeeper, either by limiting the number of simultaneous calls associated with each dial peer or by using an end-to-end bandwidth reservation protocol called Resource Reservation Protocol (RSVP). However, per-dial peer call counting does not work well if you are using more than one dial peer per WAN link, and the RSVP mechanism requires end-to-end support of the RSVP protocol within your network infrastructure, so the gatekeeper-based CAC approach generally is far superior.

You can accomplish CAC with the following two Cisco IOS commands:

- **call threshold command**

  Using the **call threshold** command allows you to limit the number of calls allowed through a particular interface. This can be done with a single Cisco Unified CME. The following is an example:

  ```
  call threshold interface GigabitEthernet0/1 int-calls low 5 high 5
  ```

- **dial-peer command**

  Using the **dial-peer** command limits number of calls based on the **max-conn** parameter under the **dial-peer** command. This constraint to the specified maximum number of calls from given dial peer. A caveat associated with this command is that there are usually multiple dial peers on specific Cisco Unified CME and the Cisco Unified CME does not track the number calls across all dial peers. If a Cisco Unified CME does have multiple dial peers, with outbound and inbound calls, the dial-peer command solution will not work. If all inbound and outbound calls are routed through a single dial peer, this command is an effective option. The following is an example of the applicable **dial-peer** command:

```
dial-peer voice 10 voip
 max-conn 10
 destination-pattern 9T
 session target ras
 dtmf-relay h245-alphanumeric
 no vad
```

Billing

The gatekeeper keeps track of the number of active calls based on messages from the gateway indicating when individual calls start and stop. Because the gatekeeper knows the start and stop times and the called and calling phone numbers, a gatekeeper can provide a centralized point to connect to a billing service (for the VoIP calls).

This type of billing typically does not know about calls being made by a Cisco Unified CME system using its local PSTN connection. These calls do not involve H.323 VoIP call legs, so the H.323 gatekeeper typically does not see them. You can use the Cisco IOS Voice Gateway Remote Authentication Dial-In User Service (RADIUS) feature in conjunction with a central RADIUS server to track all Cisco Unified CME calls for both H.323 and PSTN for billing purposes.

Note Note that *syslog* is a viable option for accumulating call detail records (CDR) as an alternative to RADIUS as billing server. One limitation for syslog is that you cannot record billing account codes. All syslog messages (including system alerts/events that are not related to CDR) are sent to the syslog server. As a result, you will require a third-party application to parse relevant CDR info. However, to make CDRs viewable for operational purposes you will need a third-party application, even with RADIUS.

Using a Gatekeeper as a Proxy for Additional Services

The other major type of gatekeeper to consider is a *routed signaling gatekeeper*. Instead of simply providing phone number-to-IP address resolution, the routed signaling gatekeeper acts as an H.323 proxy device and participates in all the H.323 call signaling. With this type of gatekeeper, the Cisco Unified CME system sends the H.323 call setup directly to the gatekeeper. The gatekeeper then relays the H.323 setup to the final (or next-hop) destination. This is very similar to the Tandem Gateway hub-and-spoke VoIP call routing described earlier with Cisco Unified CME systems.

The routed signaling gatekeeper approach has two disadvantages:

- You tend to need more Routed Signal Gatekeepers because each individual gatekeeper has more work to do per call. Instead of just being primarily involved in the phone number-to-IP address resolution at the start of the call, a routed signaling gatekeeper stays involved throughout the call. It has to process all the H.323-related messages that pass through it.

- Routed signaling gatekeepers tend not to be transparent to the supplementary service ITU-T H.450 messages used for call transfer and forwarding between Cisco Unified CME systems. The presence of a routed signaling gatekeeper may actually prevent you from using H.450 services between Cisco Unified CME systems.

Note Certain extensions, such as MWI, call park, and intercom extensions should *never* register to the gatekeeper because these extensions have no meaning outside the local Cisco Unified CME system.

However, a routed signaling gatekeeper may be able to provide your network with additional services. This is generally truer in an H.323 VoIP network that is used for residential services. In this case, a routed signaling gatekeeper can provide services, such as call forwarding and call waiting, on behalf of H.323 endpoints that (unlike Cisco Unified CME) do not natively support these services. The situation can get more complicated in some service provider networks where the same VoIP infrastructure is used to provide both direct residential and hosted or managed enterprise and small or medium business VoIP services.

Finally, one other point that sometimes favors using routed signaling gatekeeper is in service provider networks, where there is a legal regulatory requirement to support lawful interception of telephone calls for government law enforcement agencies. In the United States this requirement is called Communications Assistance to Law Enforcement Agencies (CALEA). In this case, having the routed signaling gatekeeper present in both the signaling and media path for all calls to the H.323 endpoint allows wiretapping to take place such that it is undetectable to the H.323 endpoint that is having its voice calls monitored. If you are interested in building a private corporate VoIP network, however, you do not need to be concerned with this consideration.

Public and Internal Phone Numbers in an H.323 Network

You have already seen how a Cisco Unified CME system can register its phone numbers to a central H.323 gatekeeper to provide the VoIP network with a phone number-to-IP address directory. Now you must determine which phone numbers to register. In some cases, you may simply want to register all of them. The effect of this is to give all your Cisco Unified CME extensions a direct inward dial (DID) phone number that means that any extension within your Cisco Unified CME system can be called from anywhere in your VoIP network. However, when phone numbers are registered to a gatekeeper, they typically have to be in an appropriate form. In many cases, gatekeepers cannot handle raw (abbreviated) three- or four-digit extension numbers. Extension numbers typically must be converted into a format that looks more like regular PSTN phone numbers. For example, if you have extensions 1000 to 1099 on your Cisco Unified CME system, you may need to register them in long form as something like 408-555-0100 to 408-555-0199.

Registering secondary numbers for ephone-dn might be required if the DIDs you have been assigned are non-contiguous and do not fit into a particular pattern. For example, if you are assigned DID 408-555-0100 to 408-555-0125, and you want to map to internal extensions 1000 to 1025, you would use secondary dns:

```
ephone-dn 1
number 1000 secondary 4085550100 no-reg primary
!
ephone-dn 2
number 1001 secondary 4085550101 no-reg primary
!...and so on...
```

This makes the most sense when your Cisco Unified CME extension numbers also have matching real PSTN phone numbers. In this case, you probably have a PSTN link that uses an ISDN interface so that the PSTN network signals the calls from the PSTN number by providing you with the full national phone number of the number called. This type of numbering is often called E.164 format after the ITU-T recommendation that describes the transnational telephone number formatting rules. The term E.164 is often used a little loosely in that strictly using E.164 requires an indication of whether the phone number includes an international access code or otherwise.

One advantage of using E.164 numbers with a gatekeeper is that it simply gives you a larger number space to work with. This means that you are less likely to run out of phone numbers. It also makes it easier to add links to independent external VoIP networks if you need to. A larger number space also means that you can have overlapping extension numbers across different Cisco Unified CME systems. For example, you might have two Cisco Unified CME systems that (for historical reasons) need to use the same extension number range. You could have two Cisco Unified CME systems that both use the extension range 0100 to 0199, but have different E.164 numbers, such as 408-555-0100 and 510-555-0100. Using the full E.164 number helps resolve any potential conflict.

Cisco Unified CME can automatically convert your local extension numbers from two to five digits into E.164 format using the dialplan-pattern command. The following is a basic example:

```
telephony-service
       dialplan-pattern 1 40855501.. extension-length 4
```

The **dialplan-pattern** command causes the Cisco Unified CME system to attempt to match the extension numbers created by the **ephone-dn** command entries against the defined pattern. Using this example, the extension number 0123 would be matched against the final four digits of the dialplan pattern **01**.., where the **.** characters provide a wildcard match. The extension number 0123 would be expanded to 4085550123, and this number would be registered with the gatekeeper. You can define up to five different dialplan patterns. The 1 immediately following the **dialplan-pattern** command is simply a tag number, 1 to 5, that indicates which of the five **dialplan pattern** entries you are using.

The dialplan-pattern command can also perform leading-digit replacement for cases in which the extension number to E.164 number expansion is not a simple concatenation of a PSTN area code and prefix. The following example shows a more complex configuration.

```
telephony-service
    dialplan-pattern 1 5105yy99.. extension-length 3 extension-pattern 1..
```

Note The variable letter *y* in the preceding example represents arbitrary digits in the prefix of a telephone number. This convention is used when phone numbers outside the range of 555-0100 to 555-0199 are required for a given example.

Using the preceding example, extension 123 is expanded to E.164 number 5105yy9923. The three-digit extension number is matched first against the extension pattern and then is substituted into the E.164 pattern defined. Without this capability, simple truncation of the ten-digit E.164 number to a three-digit extension would result in three-digit extensions in the range 900 to 999, which causes a number plan conflict with the traditional “Dial 9 for an outside line.”

The **dialplan-pattern** command allows the Cisco Unified CME IP phone extension lines to be dialed using both the abbreviated two-to-five-digit extension number and the full E.164 or national phone number. In addition to helping with matching the called number on incoming calls, the **dialplan-pattern** command also promotes the *calling party* number included on outgoing calls from the extension to E.164 format. This is often a requirement on PSTN links using ISDN that usually will not accept abbreviated extension numbers as legitimate calling party identification. You have to choose your extension number range such that it does not conflict with the E.164 area code. For example, if your E.164 phone number is 408555xxxx, you cannot use extension numbers of the form 408x.

Note Using the **dialplan-pattern** command does not require you to use an H.323 gatekeeper.

You can turn off the gatekeeper registration triggered by the **dialplan-pattern** command using the **no-reg** command option at the end of the command.

Registering Individual Telephone Numbers with a Gatekeeper

If you do not want to register all your Cisco Unified CME system's extension numbers with a gatekeeper, you can omit usage of the global **dialplan-pattern** command, and control registration of each individual extension number from within the **ephone-dn** command that is used to create the extensions (or virtual voice ports).

Each ephone-dn allows you to assign a primary and secondary number to associate with the extension. You then have a choice to register both, either, or neither of these with the gatekeeper using the **no-reg**, **no-reg primary**, or **no-reg both** command options for the **ephone-dn number** command.

If you decide not to use the **dialplan-pattern** command, you can still provide the three-to-five-digit abbreviated number and full E.164 numbering for each ephone-dn by using the **secondary** number option, as shown in the following example.

```
ephone-dn 1
       number 0123 secondary 4085550123 no-reg primary
```

Using the secondary number allows incoming calls to the ephone-dn to use either 0123 or 4085550123 as the called number. It also only registers the secondary number 4085550123 to the Cisco Unified CME system's gatekeeper. This approach gives you control over what is registered on a per-ephone-dn basis.

Note that this approach does not modify the default calling party number selected on outgoing calls from the extension. In the preceding configuration example, the calling party number for outgoing calls is set to 0123. This is normally just fine for internal extension-to-extension calling. If you need to promote the calling party number to E.164 format for the benefit of VoIP or ISDN calls, you can do this using an IOS voice gateway translation rule applied to the call's outgoing dial peer.

You can mix and match the two approaches for controlling gatekeeper registration by using narrower extension pattern matches within the **dialplan-pattern** command. For example, instead of using **extension-pattern 10.**. to match all the extensions in the 0100 to 0199 range, you can add multiple (up to five) **dialplan-pattern** commands that have narrow match ranges such as **extension-pattern 012.**, which matches only extension numbers in the 0120 to 0129 range.

If you do not have enough E.164 DID numbers available, but you still need a few extra extension lines, you can assign them to a different range of numbers. You can then use the **dialplan-pattern** command to register E.164 phone numbers in the match range with a gatekeeper. For example, you might give all your employees extension numbers in the 0100 to 0199 range, have these match a **dialplan-pattern** and, thus, register to a gatekeeper, and then simply assign nonemployee phone numbers, such as break room and lobby phones, into a separate range that does not have corresponding DID E.164 numbers, as shown in the following example.

```
telephony-service
       dialplan-pattern 1 40855501.. extension-length 4
ephone-dn 1
       number 0123
       name employee1
ephone-dn 2
       number 0124
       name empolyee2
ephone-dn 3
```

```
        number 2001
        name BreakRoom
```

In the preceding configuration example, the extension numbers 0123 and 0124 are registered with the gatekeeper as 4085550123 and 4085550124. The break room extension 2001 is not registered.

With this approach, one final detail to take care of is deciding what calling party number identification you want to provide for ISDN or VoIP calls placed from the break room phone. The simplest solution is to add a translation rule on the outgoing dial peer for calls from the break room phone to map the calling party number to your main or receptionist E.164 number, such as 4085550100. You may choose to do this for all outgoing calls from all extensions if you do not want the called party to be able to see individual extension numbers.

Internal and External Callers for VoIP

With the **dialplan-pattern** command, you can cause certain incoming VoIP calls to be treated as "internal" calls. By default, calls between IP phones on the same Cisco Unified CME system are treated as internal calls and ring with an internal ringer cadence. All other calls (VoIP and PSTN) are treated as external calls and ring with a different external call ringer cadence. Analog phones attached to router Foreign Exchange Station (FXS) voice ports also are treated as external calls by default. However, incoming calls that have calling party numbers that match one of the available five **dialplan-pattern** commands are treated as internal calls.

For example, suppose you have two Cisco Unified CME systems linked via VoIP and you use extension numbers 100 to 299 with E.164 numbers 4085yy0100 to 4085yy0199 on one system and extension numbers 200 to 299 with E.164 numbers 5105yy0200 to 5105yy00299 on the second system. You can create **dialplan-pattern** commands on both systems that provide extension number matches for both systems, as shown in the following example.

```
telephony-service
      dialplan-pattern 1 4085yy01.. extension-length 3
      dialplan-pattern 2 5105yy02.. extension-length 3
```

Note The variable letter *y* in the preceding example represents arbitrary digits in the prefix of a telephone number. This convention is used when phone numbers outside the range of 555-0100 to 555-0199 are required for a given example.

Any incoming calls that match either of the dialplan patterns are treated as internal calls, regardless of where the call physically originates. When the incoming calling party number matches the dialplan pattern, the Caller ID displayed for the call is demoted from E.164 format back to abbreviated three-to-five-digit extension number format. Also, the call is presented using the internal ring cadence. This allows you to treat incoming VoIP calls from other Cisco Unified CME systems within your network as internal calls.

To make a call coming from a router FXS voice port appear as an internal call, you need to set the voice port **station-id number** to match the dialplan pattern number range, as shown in the following example.

```
voice-port 1/0/0
       station-id number 4085550188
       station-id name AnalogPhone
dial-peer voice 408188 pots
       destination-pattern 4085550188
       port 1/0/0
       no vad
dial-peer voice number 188 pots
       destination-pattern 188
       port 1/0/0
       no vad
```

This configuration causes calls from the analog phone to have caller ID 4085550188. It also allows the analog phone to be called by dialing either the long form 4085550188 or the abbreviated three-digit extension number 188.

Note Calls from analog phones that are attached to Cisco Analog Telephony Adapters (Cisco ATAs) are treated as IP phones and do not need any special treatment.

DTMF Relay for H.323

Dual-tone multifrequency (DTMF) relay is a mechanism for reliably carrying DTMF digits across VoIP connections. If you need to signal the 0 to 9, *, and # keypad digits (DTMF digits) from your IP phone across your VoIP network, you must configure DTMF relay. DTMF digits are also sometimes called TouchTone digits.

You should configure DTMF relay if you want to operate a remotely connected voice mail system, use calling card access for PSTN calls placed through a remote VoIP PSTN gateway, or access any type of DTMF-driven interactive voice response (IVR) system (for example, telephone banking or airline flight information services).

The following sections discuss DTMF deployment considerations in the context of Cisco Unified CME networks:

- DTMF Digits, page 6-17
- Transporting DTMF Digits Reliably Using DTMF Relay, page 6-18
- Different Forms of DTMF Relay, page 6-18

DTMF Digits

DTMF describes a method of encoding telephone digits using two audio tones. For a conventional telephone keypad in which the keys are arranged in three columns by four rows, the first audio tone selects the row of the key, and the second audio tone selects the column. Each row-and-column tone uses a different audio frequency (pitch). This method of telephone digit signaling replaced the old-fashioned loop disconnect (dial pulse) digit dialing used by old rotary-style analog phones.

There are 16 DTMF digits (arranged as four columns by four rows). In addition to the standard 12 keypad digits—0 to 9, *, and #—an additional four digits form an extra fourth column of digits called simply A, B, C, and D. Because the ABCD digits are unavailable on a normal phone keypad, you are unlikely to ever come across these for normal phone calls. They are used occasionally by voice mail systems to operate an intersystem exchange of voice messages between separate voice mail systems using a standard called Analog Message Interchange Standard (AMIS).

Some security-type phones also use the ABCD digits for initial negotiation. You may also see these used in some Cisco Unified CME configuration examples where there is a need to create telephone numbers that cannot be directly dialed from a phone keypad. One example of this is if you want to create nondialable phone numbers for intercoms. You normally place an intercom call by pressing a button specifically configured for intercom (this works somewhat like a speed-dial button), so you do not need to be able to enter individual dialed digits.

Transporting DTMF Digits Reliably Using DTMF Relay

In the simple case of analog phones, the phone keypad digits result in the generation of DTMF audio tones. DTMF signaling works fine for analog phones connected directly to PSTN analog subscriber lines that travel only a relatively short distance to reach a central office (CO) telephone exchange. However, when the analog phone is connected to a VoIP system, and telephone calls are made using compressed voice (for example, G.729 at 8 Kbps), there is a substantial risk that the audio tones of the DTMF digits sent through the compressed voice path may become too distorted to be predictably recognized correctly by a remote voice mail system.

Even when you use uncompressed G.711 A-law/µ-law 64 Kbps for VoIP calls, there is still a risk that DTMF digits can get distorted in transit. This is because of the risk of packet loss in the VoIP network. If the network drops an occasional IP packet containing voice, this is usually imperceptible to the human ear. However, if an IP packet is dropped that contains an audio encoding of part of a DTMF tone, this is probably to keep the DTMF digit detection in the far-end system from detecting the digit (or to make it erroneously detect multiple digits). This is also the reason that other nonvoice audio signals such as fax and data modems need special treatment in VoIP networks.

To work around this issue, you generally have to use some form of DTMF relay. DTMF relay causes the digit press to be detected by the PSTN trunk or analog phone interface on the VoIP gateway. The originating VoIP gateway then signals the digit as an explicit event to the far-end VoIP gateway and removes the audio signal for the DTMF from the voice packet stream. When the far-end VoIP gateway receives the signal for the DTMF event, it regenerates the DTMF audio signal and inserts it into the outgoing audio stream to the PSTN or analog phone.

In the case of the Cisco SCCP IP phones, the digit never exists as an audio signal from the VoIP perspective, because it is directly signaled via SCCP. The digit audio that the phone user hears from the phone handset is for the benefit of the phone user only and is not passed to the VoIP connection.

Different Forms of DTMF Relay

In general, there are two main ways to signal DTMF events between VoIP gateways: H.245 digit relay and Real-Time Transport Protocol (RTP)-based DTMF digit relay. This is true for both H.323 and SIP, although the specific details are different.

The H.245 digit relay option sends a message via the H.323 control channel that is associated with the VoIP call. (This is called H.245 digit relay because it uses the H.245 control channel part of the H.323 protocol to signal the digit event.)

The RTP-based DTMF digit relay method carries the digit event through the voice media channel as a special marked RTP media packet. The problem of possible IP packet drop is overcome by sending multiple redundant copies of the event so that even if one of the copies is lost, there is little chance that all copies will be lost.

H.245 Digit Relay

There are two types of H.245 digit relay: signal and alphanumeric. The dial peer commands for these are **dtmf-relay h245-signal** and **dtmf-relay h245-alphanumeric**.

In signal mode, two events are sent: one to indicate the start of the digit and one to indicate the end of the digit. This lets the duration of the keypress on the phone be reflected in the duration of the digit regenerated by the far-end VoIP gateway. This is useful for calling card PSTN access where a long-duration press of the # key is sometimes used to indicate the end of a calling card call plus the intention to place a follow-on call (without needing to reenter a calling card number and its associated PIN).

Alphanumeric mode has only a single event signal. This results in the regeneration of a fixed-duration DTMF signal (usually 200 milliseconds) by the far-end VoIP gateway. In this mode, the length of the regenerated digit is unrelated to how long you press the keypad button on the phone. Some implementations generate the alphanumeric DTMF signal when you press the phone's keypad button, and others generate the signal when you release the keypad button. You can use this duration-of-press-independent property to tell which type of VoIP DTMF digit relay is being used.

H.245 alphanumeric mode is the one that should be used with Cisco Unified CME IP phones.

RTP Digit Relay

RTP-based digit relay mode also has two types:

- **RFC 2833**—A standards-based mechanism, sometimes called *Named Telephony Events* (*NTE*) or *Named Signaling Events* (*NSE*). The Cisco IOS **dial peer** command for this mode is **dtmf-relay rtp-nte**. This method is prevalent in SIP VoIP networks.
- **cisco-rtp**—A Cisco proprietary mechanism that represents an implementation of RTP-based DTMF relay that predates the RFC 2833 standard. The dial peer command for this is **dtmf-relay cisco-rtp**. If you enable the **dtmf-relay** command without specifying an explicit DTMF relay type, you get the cisco-rtp type.

When you press a keypad digit on an IP phone, you hear a tone in the phone handset that corresponds to the digit you press. Although you hear this audio tone, the far-end party that your call is connected to does not. The IP phone sends the keypad audio signal only to the phone's handset (or speaker). It does not insert the audio digit indication into the outgoing voice packet stream. When you press the keypad digit on an SCCP-based IP phone, the phone sends a control message to the Cisco Unified CME router via SCCP. Because the digit press originates from the phone as a control channel message, the SCCP digit message is simply converted into an H.245 alphanumeric message to send this across H.323 VoIP.

The SCCP digit press event does not indicate the duration of the keypad button press. This means that the H.245 signal method cannot be used, because the SCCP phone does not provide digit-start and digit-stop information. Also, the SCCP phones do not natively support either the RFC 2833 or cisco-rtp RTP-based digit relay mechanisms.

For you to signal DTMF keypad digits across H.323, you need to configure your VoIP dial peers as shown in the following example:

```
dial-peer voice 510200 voip
       destination-pattern 51055502..
       session target ipv4:10.1.1.1
       dtmf-relay h245-alphanumeric
      no vad
```

If you are using your Cisco Unified CME system in a SIP network, you have to use the RFC 2833 DTMF relay method where possible. Cisco Unified CME 3.2 (and later) software provides automatic conversion from the SCCP control channel DTMF messages received from the SCCP IP phone into standard SIP RFC 2833 RTP digits.

Call Transfer and Call Forwarding in an H.323 Network Using H.450 Services

The ITU-T H.450 services are a set of standard supplementary services defined for H.323 VoIP networks. H.450 provides services above and beyond basic A to B telephone calls.
Cisco Unified CME 3.0 offers only the services related to call transfer (H.450.2) and call forwarding (H.450.3). Cisco Unified CME 3.1 also introduced support for the H.450.12 capabilities discovery protocol to ease interworking issues with another company's H.323 systems.

The following is a full list of the H.450.x services, including the date when they became formal ratified ITU-T standards:

- **H.450.1 (2/1998)**—A generic functional protocol that supports supplementary services in H.323 (supported by Cisco Unified CME)
- **H.450.2 (2/1998)**—A call transfer supplementary service for H.323
- **H.450.3 (2/1998)**—A call diversion supplementary service for H.323 (supported by Cisco Unified CME)
- **H.450.4 (5/1999)**—A call hold supplementary service for H.323
- **H.450.5 (5/1999)**—A call park and call pickup supplementary service for H.323
- **H.450.6 (5/1999)**—A call waiting supplementary service for H.323
- **H.450.7 (5/1999)**—An MWI supplementary service for H.323
- **H.450.8 (2/2000)**—A name identification service
- **H.450.9 (11/2000)**—A call completion supplementary service for H.323 (includes callback for a busy subscriber)
- **H.450.10 (3/2001)**—A call offering supplementary service for H.323 (includes camp-on busy subscriber)
- **H.450.11 (3/2001)**—A call intrusion supplementary service for H.323
- **H.450.12 (7/2001)**—A common information additional network feature for H.323 (for H.450.x capabilities discovery, supported by Cisco Unified CME 3.1 and later releases)

An important thing to note about the dates these standards became available is that many H.323 networks were brought into service before these standards were issued. This means that support of these standards within H.323 networks varies widely, which causes some challenges in deploying these services within multivendor H.323 networks.

H.450.2 and H.450.3 services are present and enabled by default in Cisco IOS Release 12.3(4)T and later releases (for voice-enabled images). This allows a Cisco IOS voice gateway (without Cisco Unified CME configuration) to be used as a VoIP-to-PSTN gateway and to automatically support the forwarded party, transferee, and transfer-to roles when using the standard default voice session application.

The earlier Cisco IOS Release 12.2(15)T and later releases can also support H.450.2 and H.450.3 provided that they are configured to use a special Tool Command Language (TcL) script (called app_h450_transfer.tcl and available on Cisco.com) in place of the default voice session application.

H.450.12 services are available in Cisco IOS Release 12.3(7)T. They need to be explicitly enabled using the **supplementary-service** command.

The following sections address issues related to call transfer and call forwarding in an H.323 network using H.450 services:

- H.450.2 Call Transfer, page 6-21
- H.450.3 Call Forwarding, page 6-24
- H.450.12 Supplementary Services Capabilities, page 6-25
- DSP Resources for Transcoding, page 6-26
- Configuring H.450.x Services, page 6-27
- Cisco Unified CME Local Supplementary Services, page 6-28
- H.450.x and Cisco Unified CallManager, page 6-28
- H.450.x Proxy Services, page 6-29

H.450.2 Call Transfer

For call transfer with consultation, the basic operation of the telephone user interface is expected to look like this:

1. The inbound call to the phone is answered. The parties talk.
2. The phone user (transferor) presses the transfer key, gets dial tone, and enters the transfer-to destination. The calling party (transferee) is placed on hold and may hear the music on hold audio feed.
3. The transferor hears the transfer-to phone start to ring.
4. The phone at the transfer-to destination is answered, and a consultation call takes place between the transfer-to and the transferor.
5. The transferor presses the transfer key a second time (or simply hangs up) to execute the transfer.
6. The original caller (the transferee) is connected to the transfer-to party.

The H.450.2 protocol is designed to allow this operation to take place where the transferee, transferor, and transfer-to parties are all associated with different H.323 endpoints, regardless of physical location. This means (for example) that a transferee party originating a call in Paris can place a call to a transferor in Los Angeles and get transferred to a transfer-to destination in London. In a VoIP network that fully supports H.450.2, the resulting post-transfer call between Paris and London is a direct call and does not have to be relayed via the transferor (in Los Angeles). This is an especially important consideration when you consider the network design implications from a voice quality, delay, and scalability point of view. It is an important consideration for cases in which a call might need to be transferred multiple times before it reaches its final destination.

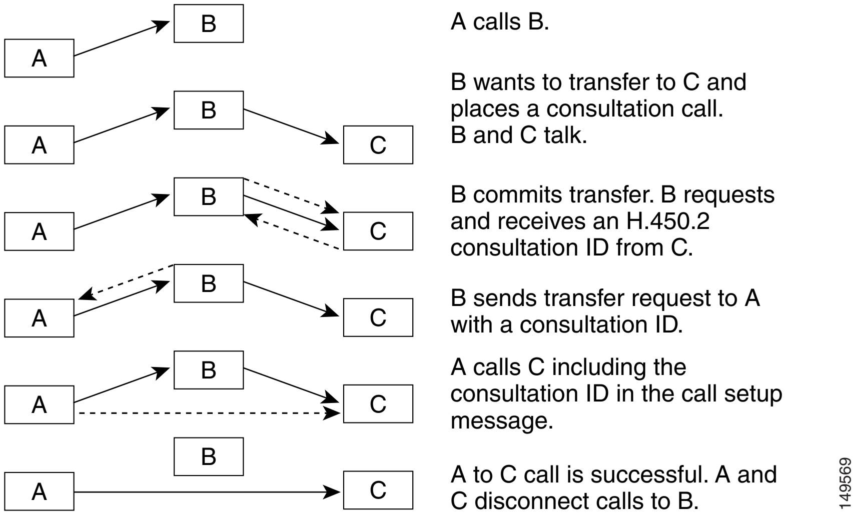
Multiple transfer is one area in which VoIP-based networks have considerable superiority over traditional legacy-based TDM networks—if they are implemented to take full advantage of the H.450.2 service.

There are other ways of invoking a call transfer that do not follow the usual user interface steps. One particular example is a three-party conference call where A calls B, B calls C, and then B joins the A–B and B–C calls together as a conference. If the B party conference initiator wants to drop out of the conference and leave the A and C parties connected to each other, this can be implemented as a call transfer where B invokes a transfer of A to C.

The following detailed protocol transactions allow the transfer to take place (see Figure 6-6):

1. The original incoming call is just an ordinary “A calls B” H.323 call between two parties. Of course, the original call does not have to be an incoming call. For example, it could be an outgoing call placed by an assistant on behalf of an executive who is transferred to the executive as soon as the call is successfully connected.
2. The transferring party presses the transfer key. This puts the original call on hold. A second line or call instance is acquired on the transferor’s phone, and dial tone is obtained. The transferor dials the phone number of the transfer-to destination using the second line or call instance. This consultation call is also a simple “B calls C” H.323 call between two parties. To the external H.323 network, the A–B and B–C calls are seen as unrelated at this point. At this stage in the process, there is no guarantee that a transfer will actually take place. The B–C call can return a busy indication, and the B (transferor) party can elect to try a different transfer-to destination, D. The B–C call may connect, and a consultation call may take place in which C declines to talk to A. The B–C call can terminate at that point, and the transferor B party may then resume the A–B call. Alternatively, B can place another consultation call B–D.
3. The transferor B decides to commit the transfer either by pressing the transfer button a second time or by hanging up. At this point, a complex sequence of actions takes place in an attempt to transfer the call. First, the transferor B puts the B–C call into a hold state and then sends an H.450.2 message to the transfer-to destination C. This informs C that a transfer will take place and requests that C issue a unique consultation ID to B. This consultation ID is used to identify the call that is being transferred.
4. When B receives the consultation ID from C, it sends an H.450.2 transfer request to A containing the consultation ID. This message includes the phone number for C.
5. When the A party (the transferee) receives the transfer request, it places a direct H.323 call to C using the phone number provided by B. This call includes the consultation ID that was generated by C and passed via B (the transferor). The transfer-to destination receives the A–C call from A. At this point the B–C consultation call is still active. The transfer-to C destination uses the consultation ID from the A–C call to match the B–C call. Because the B–C and A–C calls have the same consultation ID, the transfer-to C party can tell that the A–C call is intended to replace the B–C call.
6. As soon as the transfer-to C has matched up the A–C and B–C calls using the consultation ID, C disconnects the B–C call. When the transferee A gets a successful call response from C so that the A–C call enters the connected state, the transferee A disconnects the A–B call. The transferor B party gets a disconnect indication for both the A–B and B–C calls and drops out of the transferred call.

Figure 6-6 H.450.2 Call Transfer Protocol


A
B
C
A calls B.
B wants to transfer to C and places a consultation call. B and C talk.
B commits transfer. B requests and receives an H.450.2 consultation ID from C.
B sends transfer request to A with a consultation ID.
A calls C including the consultation ID in the call setup message.
A to C call is successful. A and C disconnect calls to B.
149569

A couple of minor variations on this flow are worth mentioning. The transferor phone user at B can choose to commit the transfer before the B–C consultation call is answered, while the B–C call is still in the alerting (ringing) state. The B to C consultation ID request can take place regardless of whether the B–C consultation call is in the connected or alerting (ringing) state.

The transferor phone B can be configured to invoke a transfer to C without first placing a consultation call. In this case, the B to A call transfer request carries a zero consultation ID. This type of transfer has the disadvantage that B has no guarantee that the A–C transferred call will succeed. It has the advantage that it does not require the transfer-to C destination to support the H.450.2 protocol and the associated B–C-to-A–C call replacement operation. This type of blind transfer is useful when the transfer-to destination is some type of automatic voice system, such as a voice mail device or a call queuing service.

So, as you can see, you can invoke three types of transfers using the H.450.2 call transfer protocol:

- Transfer with consultation with the transfer committed when the B–C call is in the connected state. Cisco Unified CME calls this type *full consult with transfer at connected.*
- Transfer with consultation with the transfer committed when the B–C call is in the alerting (ringing) state. Cisco Unified CME calls this type *full consult with transfer at alerting*.
- A blind transfer that does not involve a consultation call. Cisco Unified CME calls this type a full-blind transfer.

Cisco Unified CME lets you mix and match the full-consult and full-blind transfer types at several levels:

- Configure a global default using the **transfer-system** command (under **telephony-service**) and select either **transfer-system full-consult** or **transfer-system** full-blind.
- Override the global transfer system selection for each IP phone line (ephone-dn) using the **transfer-mode** command. You can select either **transfer-mode consult** or **transfer-mode blind**. For example, you might choose to have a receptionist phone that deals with a high volume of calls always perform blind transfers.
- Use the **transfer-pattern** command to force selection of the blind transfer mode for specific transfer-to destination numbers. The t**ransfer-pattern** command is also used to set up transfer permissions for nonlocal transfer-to destinations. This is useful if you need to prohibit trunk-to-trunk transfers and prevent toll fraud.

Now that you understand the process for H.450.2 call transfer, the next section discusses H.450.3 call forwarding.

H.450.3 Call Forwarding

For call forwarding, as with call transfer, the following apply:

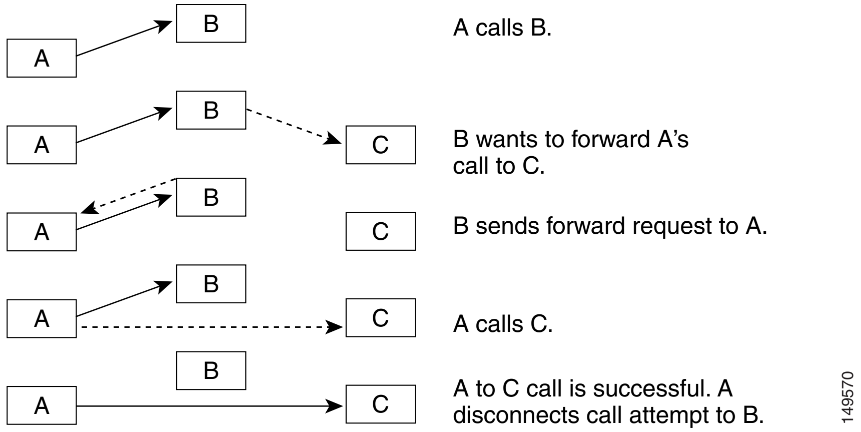
1. An inbound call is placed to an IP phone.
2. The IP phone is busy, does not answer, or is configured for unconditional call forwarding (call forward all).
3. The IP phone forwards the call to an alternate destination.
4. The original calling phone may optionally receive a display update to show that the call has been forwarded. This can be an important issue if billing or cost differences depend on the location of the final destination.
5. The IP phone at the alternate destination answers the call or may forward it to another destination. The IP phone that receives the forwarded call receives information that lets it know that the call was forwarded. This may include information about the original called number.

The H.450.3 protocol is designed to allow this operation to take place where the original calling party, forwarding phone, and forward-to party are all associated with different H.323 endpoints, regardless of physical location.

This means, for example, that a calling party originating a call in Paris can place a call to an IP phone in Los Angeles and get forwarded to a destination in London. In a VoIP network that fully supports H.450.3, the resulting forwarded call between Paris and London is a direct call and does not have to be relayed via the forwarder (in Los Angeles).

The H.450.3 forwarding protocol details are quite a bit simpler than the H.450.2 transfer case. When call forwarding takes place on an A to B call, the forwarding party B simply sends an H.450.3 message back to the calling A party to request that A call C (the forward-to destination). Generally, there is no requirement that the C party be aware of the H.450.3 protocol message exchange between A and B. If the A party accepts the call forwarding request, the A party disconnects the original A–B call, as shown in Figure 6-7.

Figure 6-7 H.450.3 Call Forwarding Protocol


B
A
A calls B.
B
A
C
B wants to forward A's
call to C.
B
A
C
B sends forward request to A.
B
A
C
A calls C.
B
A
C
A to C call is successful. A
disconnects call attempt to B.
149570

You activate the H.450.3 service using the **call-forward pattern command**. This is designed to let you selectively invoke the end-to-end H.450.3 style of call forwarding based on matching the calling party phone number. To invoke H.450.3 for all possible calling party numbers, you configure **call-forward pattern .T**, where the **.T** pattern parameter provides a wildcard match of any length.

Note because all calling party numbers are not known, in an H.450 network you should always enable the **call-forward pattern .T** command.

If you do not configure the H.450.3 service, by default you are restricted to forwarding incoming VoIP calls only within the scope of the local Cisco Unified CME system. The local scope includes forwarding to other local IP phones or to voice ports physically connected to the router (including PSTN access).

Caution If you permit call forwarding of incoming PSTN calls into outgoing PSTN calls where your PSTN interface uses simple analog Foreign Exchange Office (FXO) ports, you may have a problem with disconnect supervision. In many cases, your PSTN provider will not have enabled call disconnect signaling on the PSTN subscriber lines connected to your FXO ports. For the case of a PSTN FXO-to-FXO hairpin call path, this can result in hung voice ports, because there is no signaling of disconnect when the remote PSTN parties hang up. If you encounter this problem, you need to contact your PSTN service provider to enable disconnect supervision on your PSTN phone lines. Note that for most PSTN hairpin call paths, the caller ID of the original caller is replaced by the caller ID of the outgoing PSTN interface.

H.450.12 Supplementary Services Capabilities

The H.450.2 and H.450.3 protocols can give you a significant degree of flexibility in distributing and moving H.323 calls in your VoIP network regardless of geographic location considerations. At the same time, this can present a challenge when you attempt to deploy these services into an existing H.323-based network where support of H.450.x is not widespread.

To help you operate H.450.2 and H.450.3 services in a mixed-capability network, Cisco Unified CME 3.1 introduced support of H.450.12. The formal name for this service is *Common Information Additional Network Feature for H.323*. Basically, this means that H.450.12 provides an H.450.x service capabilities exchange between H.323 endpoints.

The H.450.12 protocol allows Cisco Unified CME to detect the H.450.x service capabilities that are available on a call-by-call basis. This allows the Cisco Unified CME system to safely invoke H.450.2 transfer and H.450.3 forwarding without risk of dropping calls, because one or more of the remote endpoints involved in the call does not support H.450.

If Cisco Unified CME detects that H.450.2 or H.450.3 is not supported for the call, you can configure Cisco Unified CME to support the transfer or forwarding by locally bridging together the call legs to form VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call paths. The term *hairpin* is used because the call path doubles back on itself in a U shape that resembles a hairpin. You may sometimes see this type of call path called *tromboning*, because a trombone has a similar U shape.

In the case of a call transfer, this means that the A–B original call and the B C consultation calls are retained and then simply bridged together to create a hairpin or Cisco IP-to-IP Gateway call A-to-B-to-C. In the case of a call forward, the call path for A calls B and B forwards to C also becomes A-to-B-to-C.

The Cisco Unified CME 3.1 code has the restriction that to successfully hairpin or Cisco IP-to-IP Gateway VoIP calls, the call legs for the A–B and B–C segments must have compatible properties. This primarily means that the A–B and A–C call legs must both use the same voice compression codec (either G.729 or G.711). This restriction does not apply in the special case that either A and B or B and C are phones or voice ports connected to the same Cisco Unified CME system.

Cisco Unified CME 3.2 allows you to overcome this single-codec restriction, because it supports SCCP-based digital signal processor (DSP) farms that can be used to provide transcoding of voice packets between the bridged call legs. The DSP farm transcoding service supports conversion of G.711 voice packets to G.729 as needed.

With the VoIP-to-VoIP Cisco IP-to-IP Gateway call routing approach, you lose the final call path optimization that you would get if H.450.x were fully supported. Costs associated with this nonoptimal call routing include extra bandwidth used and additional end-to-end delay in the voice path.

DSP Resources for Transcoding

DSP resources is a group of one or more DSPs that are not directly associated with any physical interfaces (such as PSTN voice ports). Instead, the DSPs are available as a pool of signal processing resources that can be used to provide additional processing services for telephony calls. The primary applications that require DSP resource services are transcoding for VoIP hairpin calls and transcoding for G.729 three-party conferencing. Support for DSP resources for transcoding is available in Cisco Unified CME 3.2 and later versions.

The term *transcoding* describes the operation of converting a telephone call that is encoded (compressed) using one type of voice coder-decoder (codec) into another. Specifically, transcoding is used to convert voice packets between the G.711 (64 Kbps) and G.729 (8 Kbps) compression formats.

Cisco Unified CME supports the use of DSP resources for only transcoding services. It does not support DSP resources for conferencing services, although it does use DSP resources to support three-party conferencing for G.729 VoIP calls. The Cisco Unified CME three-party conferencing service uses software-based audio mixing of G.711 audio streams. When Cisco Unified CME needs to conference three-party G.729 calls, it uses the DSP transcoding service to convert the G.729 audio into G.711 and then applies the G.711 software-based audio mixing to the transcoded G.711 audio. DSP resources require separate physical DSPs for the transcoding-versus-conferencing service. It is generally more cost-effective to support G.729 three-party conferencing via a transcode-plus-software-mixer approach rather than dedicating whole DSPs to support just the conferencing service.

Although the DSPs in a resource pool are not directly associated with physical voice ports, they are hardware devices. If you need DSP resource services, you have to consider how and where you can attach these to your Cisco Unified CME system.

The DSP resource systems that Cisco Unified CME supports are the same as those used by Cisco_Unified CallManager. So this is one more place where we provides investment protection in case you ever need to redeploy hardware originally purchased for Cisco Unified CME into Cisco Unified CallManager environments (or vice versa).

You can attach DSPs to Cisco Unified CME systems in a number of ways. The simplest way is to insert DSP modules into the DSP sockets on the motherboards of some of the newer routers, such as the Cisco 2800 and Cisco 3800 series Integrated Services Routers (ISRs).

For Cisco routers that do not have motherboard DSP sockets, you can usually overprovision extra DSPs into voice network modules (NM) such as the NM-HDV and NM-HDV2 that are used to provide PSTN interfaces. The extra DSPs in these modules that are not needed to support the PSTN interface connections can be configured as DSP resource pools.

The DSP resources do not even have to be in the same physical router as Cisco Unified CME. The DSP resources are operated and controlled using SCCP over TCP/IP. This means that you can use a spare NM slot in a second router (that supports DSP resources) and have it controlled by a Cisco Unified CME in a separate router. In practice, the Cisco Unified CME and DSP resource routers do need to be connected locally over Ethernet or some other high-bandwidth interface.

Because the DSP resources are operated using SCCP, this means that, just as with the SCCP IP phones, the SCCP DSP resources can be used in support of either H.323 or SIP networks.

The configuration steps for DSP resources are too detailed to include in this publication. However, they are covered in detail in the *Cisco Unified CME 3.2 System Administrator Guide*. Look for the **dspfarm** command for configuring the actual DSP resources and the **sdspfarm** command for configuring the Cisco Unified CME to manage the DSP resources.

Configuring H.450.x Services

This section provides a quick look at the Cisco IOS commands that you use to configure H.450 services. To enable basic H.450.2 and H.450.3 call transfer and call forwarding, you use the **transfer-system** and **call-forward pattern** commands, as shown in the following example.

```
telephony-service
       ip source-address 10.1.1.1 port 2000
       max-ephones 24
       max-dns 48
       transfer-system full-consult
       call-forward pattern .T
       create cnf-files
```

To turn on the H.450.12 service (in Cisco Unified CME 3.1 and later), use the following:

```
voice service voip
    supplementary-service h450.12
```

To permit VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call routing to work with remote H.323 endpoints that do not support H.450.x service, use this:

```
voice-service-voip
    allow-connections h323 to h323
```

Older Cisco Unified CME 3.0 and earlier code does not support the H.450.12 service. This means that if you enable H.450.12 on a Cisco Unified CME 3.1 system and place a call from a Cisco Unified CME 3.0 system, the Cisco Unified CME 3.1 system will incorrectly infer that H.450.x services are not supported by the Cisco Unified CME 3.0 system.

The workaround for this upgrade issue it to operate the H.450.12 service in advertise-only mode. In this mode, your Cisco Unified CME system transmits H.450.12 capability indications for the benefit of remote H.323 systems that are H.450.12-aware, but it does not require receipt of H.450.12 indications from a remote H.323 endpoint. You can then manually disable the H.450.2 and H.450.3 service for each non-H.450-capable VoIP link using per-dial peer configuration, as shown in the following example.

```
voice service voip
       supplementary-service h450.12 advertise-only
       allow-connections h323 to h323
dial-peer voice voip 5000
       destination-pattern 50..
       session target ipv4 10.1.20.1
       no supplementary-service h450.2
       no supplementary-service h450.3
       no vad
```

With this configuration, no attempt is made to invoke H.450.2 transfer and H.450.3 forwarding for calls using the VoIP dial peer. Instead, VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call routing is used.

Cisco Unified CME Local Supplementary Services

Cisco Unified CME is designed to make use of H.450.2 call transfer and H.450.3 call forwarding for all calls that involve one or more VoIP call legs. For example, for an incoming H.323 VoIP call that is internally forwarded from one local IP phone to a second IP phone, Cisco Unified CME sends an H.450.3 response back to the original calling party. This causes the caller to cancel the original H.323 call to the Cisco Unified CME system's first phone and creates a new H.323 call back to the Cisco Unified CME using the second phone's number.

At first, this might seem like doing things the hard way. However, the point of doing this is to make sure that the original caller can see that the call has been forwarded. Returning the call to the originator and to issue a new call allows the calling party system to have full visibility of what is going on and allows the display on the calling phone to be updated accordingly. This is an important feature if you are trying to create a seamless multisite Cisco Unified CME network as part of an internal enterprise-wide phone system.

You can use the **supplementary-service** commands to disable this VoIP end-to-end behavior and invoke hairpin and Cisco IP-to-IP Gateway call handling. For the special case in which the forwarding phone and forward-to phone are part of the same Cisco Unified CME system, the hairpin and Cisco IP-to-IP Gateway call routing mechanism can be used without incurring any real-world penalty. For incoming VoIP calls that are locally forwarded within a single Cisco Unified CME system, the final call and media path are the same, regardless of which mechanism you use to handle call forwarding. Although this example describes only local call forwarding, the same principle applies to call transfer.

Also, it is important to stress that the complexities associated with the H.450.x end-to-end services apply only to calls that involve at least one VoIP call leg. For simple standalone Cisco Unified CME usage, in which all external calls directly use the router's PSTN interfaces, Cisco Unified CME operation is more simplified. However, to use call transfer with consultation, you still need to configure **transfer-system full-consult**.

H.450.x and Cisco Unified CallManager

Cisco Unified CallManager (as of 4.0) does not support H.450.x services, including H.450.12. However, Cisco Unified CME 3.1 (and above) automatically detects a call that involves a Cisco Unified CallManager using special H.323 nonstandard information elements (IEs). Even without an H.450.12 indication, Cisco Unified CME system's automatic Cisco Unified CallManager detection can be used to invoke VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call routing when needed for call transfer and forwarding. You need to enable the **allow-connections h323 to h323** command to make this work.

Some special configuration of the H.323 interface on Cisco Unified CallManager may also be required, depending on the specific Cisco Unified CallManager software version used. For example, you may be required to configure a Media Termination Point (MTP), disable H.323 Fast, Start, and use Cisco Unified CallManager system's H.323 Inter-Cluster Trunk (ICT) mode.

H.450.x Proxy Services

You have seen how you can use Cisco Unified CME to create VoIP-to-VoIP call paths for call forwarding and transfer initiated by IP phones attached to Cisco Unified CME. What may not be obvious is that this same mechanism can be applied to calls that simply need to pass physically through a router. This is true regardless of whether the router is configured as a Cisco Unified CME with IP phones attached. Calls that pass through a router as a result of deliberate H.323 call processing (within the router) are not the same as calls that pass through the router at the basic IP packet routing and IP connectivity level. The distinction being made here is the difference between routing H.323 calls and routing IP packets.

When a call passes through a router and the router is used in onward routing of the called number, this is called Cisco IP-to-IP Gateway. In the special case that the Cisco IP-to-IP Gateway call routing results in the call entering and exiting the router on the same VoIP interface, the result is a VoIP-to-VoIP hairpin call.

A Cisco Unified CME system that is deployed at a remote branch office typically has only a single WAN and VoIP interface. This means that all VoIP-to-VoIP call paths created by the Cisco Unified CME inevitably are of the hairpin form. Hairpin VoIP-to-VoIP paths are inherently undesirable, because the doubled-back voice path is an inefficient use of scarce WAN bandwidth.

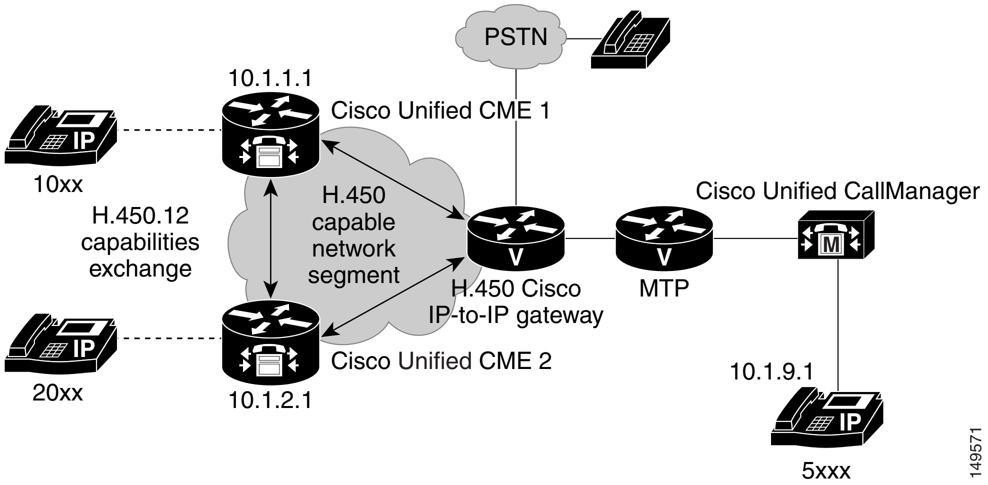
The more general VoIP-to-VoIP Cisco IP-to-IP Gateway case may offer some real advantages. One example is when you choose to use VoIP Cisco IP-to-IP Gateway call routing to provide a proxy for H.450 services.

Consider a VoIP network that connects to a central Cisco Unified CallManager system at a company's central site. Assume that the central site has a single voice mail system. Attached to the central system are a number of remote branches with Cisco Unified CME systems connected over WAN links in a hub-and-spoke arrangement, with the Cisco Unified CallManager site acting as the hub. Because the Cisco Unified CallManager does not support H.450 services, a call from the Cisco Unified CallManager site to a remote Cisco Unified CME system that is forwarded-on-busy to a voice mail system at the central site is VoIP-to-VoIP hairpin routed. This means that the call and media path for the voice mail call extends all the way from the central Cisco Unified CallManager to the remote Cisco Unified CME site and then hairpins back to the central voice mail. This consumes two calls worth of bandwidth on the WAN link and could potentially block other calls from reaching the remote-site Cisco Unified CME.

You can configure a router to act as an H.450 Cisco IP-to-IP Gateway, and use it to proxy H.450 service for the Cisco Unified CallManager, and avoid extending the hairpin call path all the way to the remote-branch Cisco Unified CME system.

Calls from the Cisco Unified CallManager to the remote Cisco Unified CME systems are configured to pass through an H.450 Cisco IP-to-IP Gateway that is co-located with the Cisco Unified CallManager at the central site. The H.450 Cisco IP-to-IP Gateway adds an H.450.12 capabilities indication to the call before it is sent to the remote Cisco Unified CME system. This allows the remote Cisco Unified CME system to invoke H.450.2 transfer or H.450.3 call forwarding on the call. The H.450 Cisco IP-to-IP Gateway intercepts any H.450.x service messages sent by the Cisco Unified CME system. If the call path required by the H.450 service invocation requires a VoIP-to-VoIP hairpin, the hairpin is created at the central site, where bandwidth is more plentiful. You still get a VoIP-to-VoIP hairpin path, but the hairpin is located in the central site network instead of the call path going all the way to the remote Cisco Unified CME system at the far end of the WAN link, as shown in Figure 6-8. In this figure, the H.450 Cisco IP-to-IP Gateway provides proxy services for H.450 messages coming from the Cisco Unified CME systems. Call transfers/forwards are rolled back to the Cisco IP-to-IP Gateway instead of hairpinning the call at the remote-branch site.

Figure 6-8 H.450 Cisco IP-to-IP Gateway



Consider the case of a call from the Cisco Unified CallManager that goes through the H.450 Cisco IP-to-IP Gateway to Cisco Unified CME 1 and is then H.450.3 forwarded to Cisco Unified CME 2. For this case, the H.450.3 forwarding request causes the original call to be rolled back to the H.450 Cisco IP-to-IP Gateway and then reoriginated to the second Cisco Unified CME 2. The final call path for the forwarded call is actually optimum for this case. It's the same call path as a direct dialed call from the Cisco Unified CallManager to Cisco Unified CME 2. The physical IP packet path for the call is the same as you would get for a pure H.450.3 case.

Furthermore, the router you deploy to act as the H.450 Cisco IP-to-IP Gateway can also be equipped with physical voice ports. It then can do double duty and act as a PSTN gateway to provide central PSTN access for the Cisco Unified CallManager and also, optionally, for the remote Cisco Unified CME systems.

To configure a router to act as an H.450 Cisco IP-to-IP Gateway, you simply create VoIP dial peers to direct incoming VoIP calls to outgoing VoIP links, as shown in the following example.

```
voice service voip
       supplementary-service h450.12
       allow-connections h323 to h323
```

The same caveats that apply to Cisco Unified CME hairpin routing also apply in the H.450 Cisco IP-to-IP Gateway case. The inbound and outbound VoIP call legs need to use the same codec unless you use a DSP farm to provide transcoding.

In the case that you use an H.450 Cisco IP-to-IP Gateway to also provide PSTN access, you may need to configure separate dial peers to allow the central site Cisco Unified CallManager-to-PSTN calls to operate using G.711 at the same time Cisco Unified CallManager-to-Cisco Unified CME via Cisco IP-to-IP Gateway calls
use G.729.

Integrating Cisco Unified CME in a SIP Network

Much of what you have read about linking Cisco Unified CME systems over WAN VoIP links for H.323 also applies to SIP, so a lot of the heavyweight detail that's been covered for H.323 is not repeated here. Instead, the following sections focus on some of the differences between SIP and H.323 implementations. This approach also helps you understand some of the issues associated with investment protection for your VoIP network and hopefully provides some reassurance about picking the "right" protocol for intersite calls. Cisco Unified CME provides you with flexibility and safeguards against protocol dependencies.

A major point that should be made here is that Cisco IOS software and Cisco Unified CME system support of SIP is primarily for *SIP trunking*, or using SIP as a protocol to connect calls between peer Cisco Unified CME systems over a WAN link. This is primarily a property inherited from the Cisco IOS Voice Infrastructure functionality that underlies Cisco Unified CME. This is quite a different usage case than that of connecting SIP phones directly to Cisco Unified CME.

However, you can host SIP phones directly on Cisco Unified CME 3.0, because the same Cisco IOS Release 12.3(4)T also independently includes the Survivable Remote Site Telephony for SIP (SIP-SRST) feature that provides a basic Registrar and Redirect Server. The services and features that you can access from the SIP phones are very limited in comparison to the phone features offered for SCCP-based phones. More significantly, Cisco Unified CME 3.x does not provide any mechanisms to support administration and configuration management for SIP phones.

You can also host H.323-based phones on a Cisco Unified CME system if you use a router image that includes gatekeeper functionality. These services that enable support of H.323 and SIP phones are part of the general Cisco IOS Voice Infrastructure functionality and are unrelated to Cisco Unified CME.

You should understand here that although you can concurrently and independently operate the IOS Voice SIP and H.323 phone-hosting capabilities with Cisco Unified CME, this functionality is not integrated and productized in the same way as support for SCCP phones. Cisco Unified CME 3.0, 3.1, and 3.2 are not marketed as providing SIP or H.323 phone support for this reason.

The following sections describe using SIP to interconnect Cisco Unified CME systems:

- Two-Node Topology with SIP, page 6-31
- SIP Proxy/Registrar/Redirect Server, page 6-33
- Public and Internal Phone Numbers in a SIP Network, page 6-34
- DTMF Relay and RFC 2833 for SIP, page 6-34
- SIP Supplementary Services, page 6-35
- SIP REFER, page 6-36
- SIP 3XX Response, page 6-36
- SIP Interoperability, page 6-37

Two-Node Topology with SIP

You can connect two Cisco Unified CME systems using a pair of VoIP dial peers configured symmetrically on each Cisco Unified CME to point to the other Cisco Unified CME. This is exactly the same as the H.323 case described in "A Simple Two-Node Topology with H.323" section on page 6-5. The only difference is that you must explicitly select SIP in your dial peer, whereas H.323 is the default protocol.

For a pair of Cisco Unified CME systems that have extensions 1000 to 1099 on Cisco Unified CME 1 (IP address 10.1.1.1) and 2000 to 2099 on Cisco Unified CME 2 (IP address 10.1.2.1), you need the dial peers shown in the following example:

- Cisco Unified CME 1

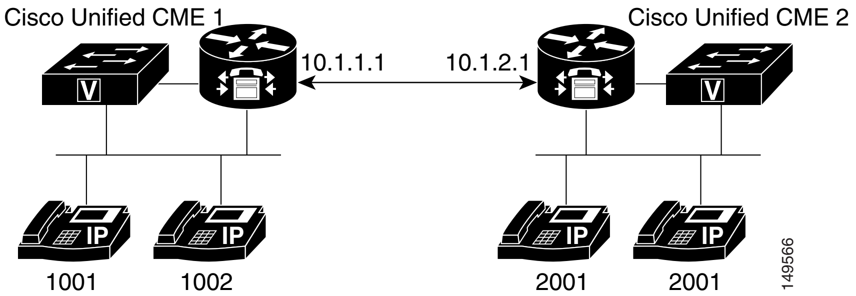
```
dial-peer voice 2000 voip
     destination-pattern 20..
     session target 10.1.2.1
     session protocol sipv2
     dtmf-relay sip-notify
     dtmf-relay rtp-nte
     codec g729r8
     no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1000 voip
     destination-pattern 10..
     session target 10.1.1.1
     session protocol sipv2
     dtmf-relay sip-notify
     dtmf-relay rtp-nte
     codec g729r8
     no vad
```

As you can see, switching your simple two Cisco Unified CME system network from H.323 to SIP is easy. All you need to add is **session protocol sipv2** to the dial peers on both systems and it is done. You will also notice that the dtmf-relay method has been changed. Additional information about this command is provided in"DTMF Relay and RFC 2833 for SIP" section on page 6-34. Note that the sip-notify form of DTMF relay is required for Cisco Unified CME systems that use Cisco Unified CME 3.1 or earlier versions. Cisco Unified CME systems based on Cisco Unified CME 3.2 or later versions should use the **dtmf-relay rtp-nte** form where possible. See Figure 6-9.

Figure 6-9 Simple Two-Node Cisco Unified CME SIP Network



The following example shows the relevant Cisco Unified CME node configurations.

- Cisco Unified CME 1

```
dial-peer voice 2000 voip
   destination-pattern 20..
   session target ipv4:10.1.2.1
   session protocol sipv2
   dtmf-relay rtp-nte
   no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1000 voip
   destination-pattern 10..
   session target ipv4:10.1.1.1
   session protocol sipv2
   dtmf-relay rtp-nte
   no vad
```

You face exactly the same issues and options as in the H.323 case in expanding beyond a two-node H.323 Cisco Unified CME network to a multinode SIP network. The exception is that Cisco Unified CME does not natively support Cisco IP-to-IP Gateway SIP call routing. However, you can easily buy another company's SIP proxy or redirect server to do this instead.

SIP Proxy/Registrar/Redirect Server

In H.323 you saw how you can use an H.323 gatekeeper to provide telephone number-to-IP address resolution. In SIP this same function is often carried out using a SIP registrar and a SIP Redirect Server that are internally linked. The SIP Registrar accepts SIP REGISTER messages from client voice endpoint systems (called user agents [UAs] in the SIP world) and uses them to build a phone number-to-IP address conversion database. Just as Cisco Unified CME can generate H.323 gatekeeper registrations, Cisco Unified CME can generate SIP REGISTER messages based on the Cisco Unified CME ephone-dn extension numbers and **dialplan-pattern** command. Cisco Unified CME can maintain concurrent registrations with both an H.323 gatekeeper and SIP Registrar at the same time.

There is a small difference in the protocol flow between the H.323 and SIP cases. In the H.323 case, an explicit address query (ARQ) goes from the Cisco Unified CME to the gatekeeper to obtain the destination IP address from the destination phone number. As soon as that operation is successful, the Cisco Unified CME initiates a call setup. In the SIP case the Cisco Unified CME sends an INVITE call setup message to the combined SIP Registrar/Redirect Server. The Redirect Server responds with a REDIRECT message that guides the Cisco Unified CME to send a second INVITE message to the correct IP address.

The combination of a Registrar and Redirect Server in a single system is often called a *SIP proxy*, albeit a very basic one. In an alternative implementation, the proxy accepts the initial INVITE sent by the Cisco Unified CME. Instead of responding with a redirect response, the proxy may simply relay the INVITE to its final destination. This is similar to Cisco IP-to-IP Gateway call routing and to the action of a routed signaling gatekeeper in the H.323 context.

To use the services of a SIP proxy with your VoIP dial peers, you can use the configuration shown in the following example.

```
sip-ua
       sip-server ipv4:10.1.10.2
dial-peer voice 408525 voip
       destination-pattern 408525....
       session target sip-server
       dtmf-relay rtp-nte
       no vad
```

You can use a DNS name instead of a raw IP address for the sip-server address.

To register your Cisco Unified CME phone numbers with an external SIP registrar, you can use the configuration shown in the following example.

```
sip-ua
 authentication username user1 password 12345 realm domain
 no remote-party-id
 registrar dns:10.1.10.2 expires 3600
```

Note that the authentication command authenticates against the SIP registrar. In order for extensions to register to the SIP registrar, each must successfully authenticate.

Public and Internal Phone Numbers in a SIP Network

Just as for H.323, you may need to choose which phone numbers you register with a SIP registrar. You can control this in the same way that you learned for H.323 using the **dialplan-pattern** command and the **no-reg** option for the **ephone-dn number** command.

Although SIP does allow the use of Internet domain names for telephone number scoping purposes, this is not supported by the IOS SIP Voice Gateway software. The IOS SIP Voice Gateway software mostly ignores domain names in SIP messages.

DTMF Relay and RFC 2833 for SIP

The same technical issues and motivations exist for DTMF relay in SIP as in H.323. The first-choice DTMF relay method for most SIP networks is the RTP-based RFC 2833 protocol. Unfortunately, the Cisco SCCP IP phones do not natively support this.

As you saw in"DTMF Relay for H.323" section on page 6-17, the Cisco SCCP phones only provide out-of-band control channel signaling for DTMF digits. In the H.323 world, this can be easily translated into H.245 alphanumeric signaling events to pass across VoIP over WAN.

The equivalent method in the SIP domain is to use a SIP NOTIFY event. However, this is not well standardized. The original SIP DTMF NOTIFY implemented in the Cisco IOS Voice Gateway software is based on an early draft proposal for this mechanism and, therefore, is not supported on most third-party SIP products. However, this mechanism is adequate provided that you are using only Cisco IOS voice endpoints with Cisco IOS Release 12.3(4)T or later. You also need to transport DTMF keypad events across VoIP to an IOS PSTN voice gateway for regeneration as an audio signal into a PSTN trunk or FXS port.

To enable the SIP NOTIFY for dtmf-relay, add the following command to your SIP VoIP dial peers:

```
dtmf-relay sip-notify
```

Cisco Unified CME 3.2 introduces support for conversion and interworking between the SCCP control channel DTMF digit indications and RTP-based RFC 2833 (for SIP only). This significantly improves the Cisco Unified CME system's ability to work with SIP networks that include another company's SIP-based voice mail systems. To use this RFC 2833 RTP in-band to SCCP out-of-band interworking function for dtmf-relay, you use the following:

```
dtmf-relay rtp-nte
```

Note Cisco Unity Express 2.2 and earlier versions support only the **sip-notify** format of DTMF relay. When using Cisco Unity Express 2.2 or earlier versions, youmust use **sip-notify** on the SIP VoIP dial peers used to interconnect Cisco Unified CME with Cisco Unity Express. Even when using the notify method in the SIP VoIP dial peers for interworking with Cisco Unity Express, you can simultaneously use the RFC 2833 mechanism on other SIP VoIP dial peers that require it. Cisco Unity Express 2.3.1 and later support RFC 2833. For these versions, you can use RFC2833 **dtmf-relay rtp-nte** on the SIP VoIP dial peers used to interconnect Cisco Unified CME with Cisco Unity Express.

We recommend using of RFC 2833 **dtmf-relay rtp-nte** for SIP when possible.

Note Cisco Unified CME does not support raw, in-band DTMF which is the implementation used by some SIP service providers. If these situations, Cisco Unified CME IP phones will not be able to send DTMF to the SIP cloud and inbound calls terminated on the Cisco Unified CME will not be able to receive DTMF. The SIP service provider to which the Cisco Unified CME connects must either support RFC 2833 or SIP-notify in order for DTMF to operate properly.

SIP Supplementary Services

The SIP supplementary services for call transfer and call forwarding enjoy significantly more widespread support across the majority of another company's SIP implementations compared with supplementary services for H.323. These services have been part of the SIP landscape from fairly early on in the development of SIP, in contrast with the history of H.323, where these services were defined relatively late.

The main difference between H.323 supplementary services is that SIP supplementary services (such as MWI notification, REFER, and 3XX) cannot be disabled (unlike H.450). If you connect a Cisco Unified CME to a SIP service provider that does not support these service, then call forwards and transfers invoked by the Cisco Unified CME will fail.

MWI Notification

Message waiting indicator (MWI) notification is a SIP supplementary service that enables outcall-based Cisco Unified CME support of Subscribe/Notify and unsolicited notify functions for receiving MWI over SIP. Key capabilities include the ability to:

- Generate unsolicited notify messages to SIP endpoint for outcall
- Subscribe to MWI server for SIP endpoint
- Relay unsolicited notify messages to SIP endpoints for unsolicited notify and subscribe/notify
- Support unsolicited notify internetworks with MWI Relay

Several MWI notification examples follow:

- MWI notification outcall configuration example

```
ephone-dn1
  number 9000...
  mwi on-off
```

  In the preceding example, the number 9000... command defines the MWI callback pilot number.

- Unsolicited notify configuration example

```
sip-ua
  mwi-server ipv4:10.5.49.200 unsolicited
voice register dn 1
  number 1234
  mwi
```

  In the preceding configuration example, the **mwi-server** command defines the unsolicited MWI server and the standalone **mwi** command specifies extension support.

- Subscribe/notify configuration example

```
sip-ua
  mwi-server ipv4:10.5.49.200
```

```
voice register dn 1
  number 1234
  mwi
```

In the preceding configuration example, the **mwi-server** command defines the subscribe/notify MWI server.

SIP REFER

Call transfer with SIP is supported using the SIP REFER method. As its name suggests, it allows one SIP UA, or endpoint, to refer a caller to a different SIP UA. It operates in a similar way to H.450.2. It triggers a replacement of the transferor-to-transfer-to consultation call by a transferee-to-transfer-to call. Just as in the H.450.2 case, the original and consultation call legs are treated as unrelated and independent entities until the call transfer is actually committed. Just like H.450.2, three possible transfer scenarios exist:

- Transfer-consult with commit-at-connect
- Transfer-consult with commit-at-alerting
- Blind transfers (without any consultation call)

One difference is that there is no specific consultation ID exchange transaction between the transferor and transfer-to parties, because SIP inherently contains a mechanism to uniquely identify the call being replaced at the transfer-to endpoint.

For the sake of completeness in describing SIP transfers, an older (and less preferred) SIP method called BYE/ALSO exists for executing blind transfers with SIP. As its name suggests, this is a method whereby the transferor terminates the original call from the transferee (BYE) but includes a request in the termination for the transferee to generate a follow-on call (to the transfer-to destination) using the ALSO part. Cisco Unified CME does not use the BYE/ALSO method to initiate transfers, but it does support receipt of this method from other SIP devices. This is the method used by the automated attendant (AA) in Cisco Unity Express.

To enable Cisco Unified CME to send REFER messages for call transfers, you need to configure **transfer-system full-consult** under **telephony-services**. This is the same basic configuration that is needed for H.450.2 transfers.

Unlike the H.450.2-related IOS CLI, there are no configuration commands to directly control usage of the REFER mechanism. This is a reflection of the almost-universal support that exists for REFER. There is little need to be able to enable and disable it in the same way as H.450.2.

SIP 3XX Response

Call forwarding in SIP is supported mostly using the 302 moved temporarily in response to an incoming SIP call setup INVITE message. Just like the H.450.3 protocol, this response includes the alternate forward-to destination information (phone number). It requests that the caller cancel the original call and create a new call to the indicated destination. A range of SIP responses in the 3xx value code range includes a 300 multiple-choice response that allows the forwarding party to provide the caller with a range of alternative contacts. The 300-response code is not directly supported in the Cisco Unified CME context. However, the Cisco IOS voice router SIP-SRST feature can generate this under some circumstances that are a little outside the scope of this book. You can find more information on this on Cisco.com by searching for “SIP Survivable Remote Site Telephony” under the *Cisco Unified SRST 3.2 Feature Guides*.

To enable call forwarding using the 302 response, you need to configure **call-forward pattern .T** under the **telephony-services** command. This is the same basic configuration that is used for H.450.3 call forwarding.

Like the REFER case, no commands in Cisco IOS software specifically control the generation of the 302 response because of the universal support of this message by another company's SIP devices.

SIP Interoperability

Interoperability for basic calls and transfer and forwarding for SIP is generally widespread among multiple SIP offerings from Cisco and another company's products. The one major caveat for this with Cisco Unified CME 3.0 and 3.1 is the lack of RFC 2833 support for DTMF relay. This is solved with Cisco Unified CME 3.2.

SIP is undergoing very rapid evolution, and many Internet Engineering Task Force (IETF) RFC drafts are in circulation at any given time. This is a good news/bad news situation. On the plus side, it shows that SIP is a flexible and extensible protocol. On the minus side, this situation has a lot of the larger and more conservative VoIP customers in a mode where they are waiting to see some stability before going to large, widespread deployments. By their very nature, large-scale deployments have difficulty absorbing significant and rapid protocol churn. If 100,000 endpoints are deployed in a VoIP network, it is very hard to do frequent upgrades to absorb the latest and greatest new protocol features.

Because Cisco Unified CME is based on top of the H.323 and SIP software that is part of the Cisco IOS Voice Gateway code, Cisco Unified CME automatically keeps up with, and benefits from, the best of both protocols. It represents a low-risk approach to VoIP telephony.

CHAPTER 7

Integrating Cisco Unified CallManager Express with Cisco Unified CallManager

This chapter covers the deployment of Cisco Unified CallManager Express (Cisco Unified CME) for branch offices in conjunction with a Cisco Unified CallManager deployed at a central office site. In this situation, the central Cisco Unified CallManager site can act as a hub linking the remote Cisco Unified CME sites. Cisco Unified CME and Cisco Unified CallManager can communicate across IP WAN links using H.323 (or using Session Initiation Protocol [SIP] with Cisco Unified CallManager 5.0 or later versions).

In H.323 networks, Cisco Unified CME provides supplementary service interworking (H.450) using Voice over IP (VoIP) hairpin call routing when needed for intersite call transfer and forwarding. This chapter discusses these services in a network that has both Cisco Unified CME systems and one or more Cisco Unified CallManager systems.

The following sections address considerations in designing effective integration and interoperability solutions for Cisco Unified CME and Cisco Unified CallManager.

- Goals of Interoperability, page 7-1
- Basic Calls Between Cisco Unified CallManager and Cisco Unified CME, page 7-2
- Call Transfer, page 7-4
- Call Forwarding, page 7-10
- Connected Party Name and Number Services, page 7-12
- Using H.450.x Cisco IP-to-IP Gateway, page 7-13

Note For additional information, see the "Related Documents and References" section on page xii.

Goals of Interoperability

Real enterprise VoIP networks that have been designed consistently from the ground up and that adhere to a single uniform architectural approach are rare. The technologies available to network designers have evolved rapidly over the past decade or two. This rapid evolution will probably continue for some time. It requires organizations to continually rethink their network architectures to take advantage of the latest available enhancements. Not only do the technologies change, but so do the companies trying to make best use of them. Companies split and merge and reinvent themselves in a continuous effort to stay profitable and competitive. This leads to real-world networks made up of a mixture of architectures formed by the ad hoc fusion of components contributed by multiple network designs.

Looking at VoIP networks that incorporate Cisco components, you commonly see both central-site Cisco Unified CallManager networks using Cisco Survivable Remote Site Telephony (Cisco SRST) at some remote branch offices coupled with Cisco Unified CME systems used at other remote offices. Being able to interconnect these systems is a fairly important consideration. In fact, some businesses deliberately design their networks using both central and distributed models to take into account issues with geographic variation in the availability of WAN services. For example, in the banking industry, central Cisco Unified CallManager designs have been widely used in city branches located in metropolitan areas where adequate bandwidth and quality of service (QoS)-enabled WAN links are fairly readily available. However, Cisco Unified CME systems have been used in small-town bank branches located in more rural areas where WAN services might be less sophisticated and unable to support voice.

Both Cisco Unified CallManager and Cisco Unified CME support H.323, which you can use to create Cisco Unified CallManager-to-Cisco Unified CME links. Cisco Unified CME also supports SIP for VoIP interconnect. SIP is also being introduced as a WAN trunking interface on Cisco Unified CallManager. This chapter focuses only on the H.323 interconnect option, because the SIP interconnect option is still a work in progress as SIP support on successive Cisco Unified CallManager versions evolves. However, you can expect that most of the architectural issues raised in this chapter are also applicable in the SIP context.

The descriptions contained in this chapter apply to the Cisco Unified CME 3.1 and 3.2 releases and the Cisco Unified CallManager 3.3(3) and 4.0. Newer versions may have different behaviors and options than those described here.

Basic Calls Between Cisco Unified CallManager and Cisco Unified CME

Even before the introduction of Cisco Unified CME, Cisco Unified CallManager used Cisco IOS voice routers to provide a Public Switched Telephone Network (PSTN) access gateway for Cisco Unified CallManager IP phones. Both the H.323 and Media Gateway Control Protocol (MGCP) VoIP protocols can support this function. The choice between these two is partly a historic issue and partly related to the type of PSTN interface used, but this topic is outside the scope of this guide.

Direct MGCP integration between Cisco Unified CME IP phones and Cisco Unified CallManager is not supported. Although this does not preclude the concurrent operation of MGCP (used for the PSTN gateway ports) and H.323-with-Cisco Unified CME on the same Cisco IOS voice router, we do not recommend this configuration. Using MGCP with Cisco Unified CallManager to control the PSTN voice ports on a Cisco Unified CME system would force PSTN traffic originated by the Cisco Unified CME IP phones to route through the Cisco Unified CallManager to reach the PSTN. In most cases, this would be inefficient because it would result in the Cisco Unified CME-to-PSTN voice traffic traversing the Cisco Unified CME-to-Cisco Unified CallManager WAN link twice.

Because Cisco Unified CME is built on top of the Cisco IOS voice infrastructure software foundation also used by the Cisco IOS router-based PSTN gateways, Cisco Unified CME inherits most of the H.323 gateway-to-Cisco Unified CallManager interoperability. You should be aware of some minor differences, however.

In the simple PSTN gateway case, most of the call progress signaling for calls is performed as in-band audio tones. For example, when an IP phone (hosted by Cisco Unified CallManager) places an outbound call to the PSTN, the ringing tone (also called the *alerting* or *ringback tone*) heard by the caller is usually generated as an audio signal that is passed through end-to-end from the PSTN trunk. This means that the audio path from the gateway to the IP phone is opened and active before the call is connected.

In the case where a call is placed from a Cisco Unified CallManager IP phone to a Cisco Unified CME IP phone, the ringing tone is provided as an out-of-band H.323 indication from Cisco Unified CME (through H.323 control channel signaling). This means that the Cisco Unified CME system signals to the Cisco Unified CallManager, which in turn instructs the Cisco Unified CallManager IP phone to generate the ringing tone locally.

The reasons for this difference include the following:

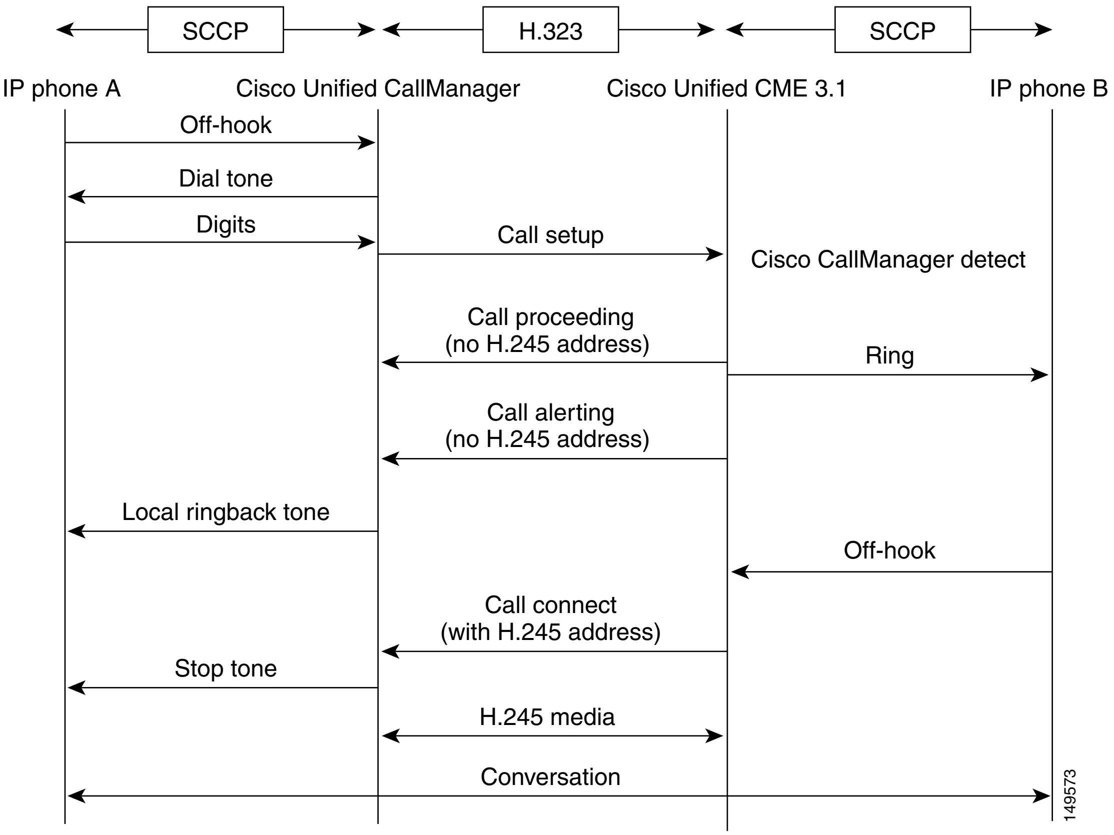
- It saves some bandwidth because the audio path is not opened until the call actually connects.
- The Skinny Client Control Protocol (SCCP)-based IP phones attached to Cisco Unified CME cannot generate in-band ringing tone.
- It avoids issues with shared extension lines, where an inbound H.323 call to Cisco Unified CME may ring multiple phones at the same time. This could create complexity in choosing which phone should physically be required to do the tone generation. Add to this the fact that any of the Cisco Unified CME phones involved might also have calls already in progress, and it should become clear why out-of-band signaling of call progress tones is the preferred approach for Cisco Unified CME.

This issue of ringing-tone signaling causes some specific changes in the H.323 protocol exchange that Cisco Unified CME uses when talking to a Cisco Unified CallManager, compared with H.323 signaling to another Cisco IOS PSTN gateway, for example.

To get Cisco Unified CallManager to provide local ringing-tone generation for outbound calls from Cisco Unified CallManager, the Cisco Unified CME delays negotiation of the media path until the call connects. The Cisco Unified CallManager 3.3 and 4.0 H.323 implementations assume that in-band ringing tone is provided (by the Cisco Unified CME or another H.323 device) on all calls that negotiate the media path (using H.245) before the call is connected. This delayed negotiation can lead to a minor delay (typically about a quarter of a second) in establishing the audio path when the call actually connects. This delay is called the *voice cut-through delay.*

Cisco Unified CME only uses this delayed H.245 media negotiation on calls that go to or from a Cisco Unified CallManager. Cisco Unified CME (3.1 and later versions) can explicitly identify Cisco Unified CallManager calls based on special nonstandard H.323 information element (IE) messages that Cisco Unified CallManager attaches to its H.323 call setup, proceeding, alerting, and connected messages. See Figure 7-1.

Figure 7-1 Cisco Unified CallManager-to-Cisco Unified CME 3.1 Basic Call


SCCP
H.323
SCCP
IP phone A
Cisco Unified CallManager
Cisco Unified CME 3.1
IP phone B
Off-hook
Dial tone
Digits
Call setup
Cisco CallManager detect
Call proceeding
(no H.245 address)
Ring
Call alerting
(no H.245 address)
Local ringback tone
Off-hook
Call connect
(with H.245 address)
Stop tone
H.245 media
Conversation
149573

Call Transfer

Cisco Unified CallManager and Cisco Unified CME implement significantly different approaches to handling call transfer. These differences are related to the basic architectural differences that exist between a highly centralized (Cisco Unified CallManager) and fully distributed (Cisco Unified CME) VoIP network architecture.

In Cisco Unified CME (and all other Cisco IOS software-based voice gateways), the preferred mechanism for handling call transfer is H.450.2. This allows calls to be transferred in a highly optimized way not only between phones on the same Cisco Unified CME system, but also between different Cisco Unified CME systems. This is a significant attribute when you consider that Cisco Unified CME system-based VoIP networks can include hundreds or thousands of individual Unified CME nodes. Each Cisco Unified CME node is a distinct and separate H.323 device with autonomous call processing.

In Cisco Unified CallManager, the call transfer mechanism is designed to allow calls to be transferred between hundreds or thousands of IP phones controlled by the *same* Cisco Unified CallManager (or Cisco Unified CallManager cluster). Furthermore, in a Cisco Unified CallManager environment, there is a significant need to separate the H.323 control path from the H.323 media path. Because a single Cisco Unified CallManager server can be required to control approximately 2500 IP phones, it’s impossible for the server to play an active intermediary role in the media path for all phone calls. Consider that there is a media packet in each direction every 20 milliseconds (ms) for each call, and then multiply this by 2500 phones. To allow a Cisco Unified CallManager to support this number of phones, the media path for phone-to-phone calls must be directly between the phones whenever possible.

Note Each Cisco Unified CallManager (or Cisco Unified CallManager cluster) represents a single H.323 device from the external VoIP network perspective regardless of how many IP phones it supports.

One other issue to examine when comparing Cisco Unified CallManager to Cisco Unified CME operation is that for enterprise telephone systems, the ratio between internal and external call counts is related to the overall size of the phone system. As the number of extensions attached to a phone system increases, so does the relative proportion of internal calls compared to external calls. For example, in a system with only ten phones, almost 100 percent of phone calls are external calls between a phone and the outside world. In a system with 1000 phones, the external calls may make up only about 10% of the total call volume.

You can view this call transfer difference between Cisco Unified CallManager and Cisco Unified CME as being equivalent to the difference between an internal intraprivate branch exchange (PBX) call transfer and an inter-PBX transfer. Viewed from the legacy PBX perspective, you can see that these are fundamentally different problems.

The following sections describe integration-related call transferring considerations:

- H.323 Call Transfer Using an Empty Capabilities Set, page 7-5
- H.323-to-H.323 Call Transfer, page 7-6
- Call Transfer and the Media Termination Point, page 7-7
- Connecting Cisco Unified CallManager with Cisco Unified CME, page 7-8
- Intersite Call Transfer with Multiple Cisco Unified CME Systems, page 7-9

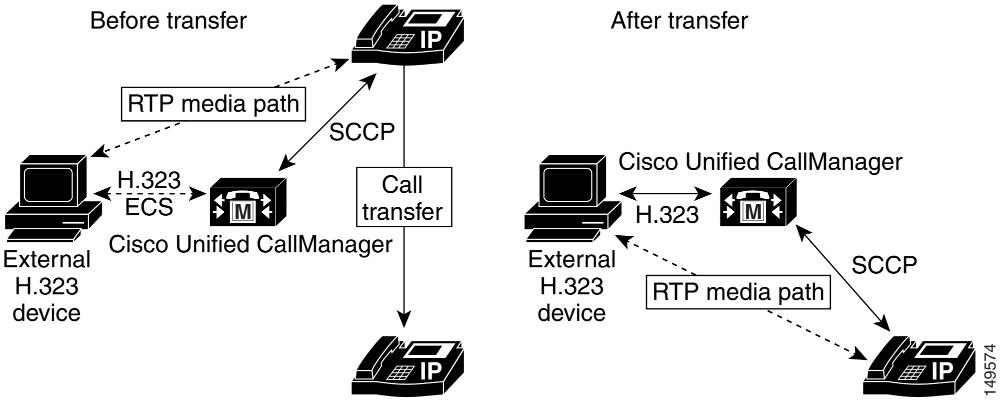
H.323 Call Transfer Using an Empty Capabilities Set

The problem with call transfer becomes more complex when you consider the interaction of Cisco Unified CallManager IP phones with an external H.323 network. When an H.323 call exists between an external H.323 device and a Cisco Unified CallManager IP phone, the preferred arrangement is to have a direct media path between the endpoints that does not pass through the Cisco Unified CallManager server. In some cases, a direct media path is not possible (as described in the "Call Transfer and the Media Termination Point" section on page 7-7. In this case, it is necessary to introduce a Media Termination Point (MTP) into the media path. The MTP acts as a media relay or middleman and relays the Real-Time Transport Protocol (RTP) voice packets between the two terminating endpoints. The call signaling path does pass through the Cisco Unified CallManager server. The H.323 signaling is terminated on the Cisco Unified CallManager server and then is converted into SCCP to talk to the IP phone. The Cisco Unified CallManager is required to participate in this signaling path to provide the needed conversion between H.323 and SCCP.

When there is a call transfer for an H.323 call from one Cisco Unified CallManager IP phone (phone A) to another (phone B), the H.323 signaling path does not change. It remains terminated on the Cisco Unified CallManager server. The Cisco Unified CallManager server establishes a new SCCP signaling path to phone B. Of course, the media path also has to change. Changing the media path on the IP phones is easy. The Cisco Unified CallManager simply sends the appropriate SCCP messages to phone B, telling it to participate in the media connection to the external H.323 endpoint.

To change the media connection on the H.323 side, the Cisco Unified CallManager uses a mechanism known as Empty Capabilities Set (ECS). This mechanism informs the external H.323 device that it should stop sending its media packets to phone A's IP address and should instead send the media packets to phone B's IP address. This mechanism allows the media stream to be redirected to the transfer-to destination phone while preserving the original H.323 control path connection. Figure 7-2 shows the media path before and after the transfer.

Figure 7-2 Cisco Unified CallManager ECS Transfer



With this arrangement, there is no limit on the number of times the call can be transferred, as long as the call termination point remains within the set of phones controlled by Cisco Unified CallManager. This is the behavior you would expect, considering how a legacy time-division multiplexing (TDM)-based PBX works. There is usually no limit on the number of internal chained transfers. Cisco Unified CME (and Cisco IOS software-based H.323 PSTN gateways in general) supports receipt of ECS signaling from Cisco Unified CallManager but does not initiate ECS signaling for call transfer.

H.323-to-H.323 Call Transfer

Now consider what happens when the transfer-to destination is not an internal IP phone. In the case of an H.323 endpoint that calls an internal IP phone and then is transferred to a second external H.323 endpoint, the same ECS mechanism can be used. The transferred call has its H.323 signaling path relayed through the Cisco Unified CallManager, but the media path is direct between the two external H.323 endpoints.

This process works fine except in the case where one of the H.323 endpoints wants to further transfer the call (or perform some other media-related operation, such as call hold with music on hold [MOH]). In general, chained H.323 ECS operations do not work well. This is because the attempt to chain-transfer the call results in a very indirect H.323 control path. None of the entities in the H.323 control path is directly connected to *both* of the call media final termination points. This means that the media path negotiations have to pass through two transit points instead of one.

For example, for the first transfer, A calls B and is transferred to C. The transferor node B is in direct contact with both the A and C points and can help them negotiate a mutually acceptable media path. The H.323 control path is A-to-B-to-C, but the media path is A-to-C.

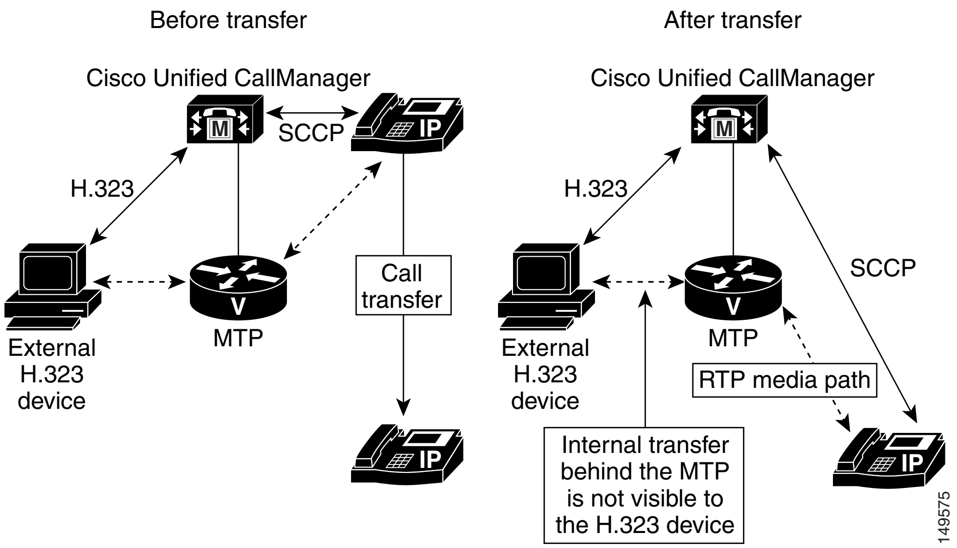
A problem arises when C wants to transfer the call to D. This would create an A-to-B-to-C-to-D H.323 control path. In this case, neither of the B or C middlemen is in direct contact with both of the A and D final endpoints. This can make successful media negotiation between A and D quite difficult to achieve in practice.

Call Transfer and the Media Termination Point

One way to solve the problem of end-to-end negotiation of the media path is to use an MTP that can provide *transcoding* services. One example of this type of MTP is the digital signal processor (DSP) farms that are supported on Cisco IOS voice-enabled routers. DSP farms are controlled by a Cisco Unified CallManager (or Cisco Unified CME) using SCCP. The term *transcode* means the ability to convert the media stream from one codec type to another. You may sometimes see this term abbreviated as *xcode*.

If you introduce a transcoding MTP into the media path, there is no need to perform end-to-end media path renegotiation for the chained call transfer case. The use of an MTP simplifies the problem of connecting or transferring a call through multiple H.323 endpoints, because it removes the need to perform a multiparty negotiation and capabilities adaptation between all the H.323 entities involved. Figure 7-3 shows the media path before and after the transfer.

Figure 7-3 Cisco Unified CallManager Transfer with MTP



In general, the MTP approach simplifies the set of H.323 signaling operations required and increases the overall the ability to interoperate. This is true even in cases where everyone uses the same codec type and actual transcoding of codecs is unnecessary.

The drawback to this approach is the impact on overall scalability, because an MTP channel is needed for every H.323 (external) call. A mitigating factor in this situation (see the "Call Transfer" section on page 7-4) is that as the number of IP phones in the Cisco Unified CallManager cluster increases, the fraction of H.323 calls to internal calls decreases. In general, the expense of adding MTPs is worthwhile because of the reduction in H.323 interoperability issues.

Another issue with the chained transfer cases is that each leg in the transfer chain contributes additional delay to both the signaling and media path. If a call is chain-transferred too many times, the resulting delay and voice quality will probably become unacceptable. In general, end-to-end one-way delays of more than 150 to 200 ms are unacceptable to phone users.

The chained-transfer issues apply only to intersite transfers that are chained across multiple separate H.323 nodes. Transfers within the internal scope of a single H.323 node do not suffer from this problem, because (with an MTP) the transfer is invisible to the other H.323 endpoints involved.

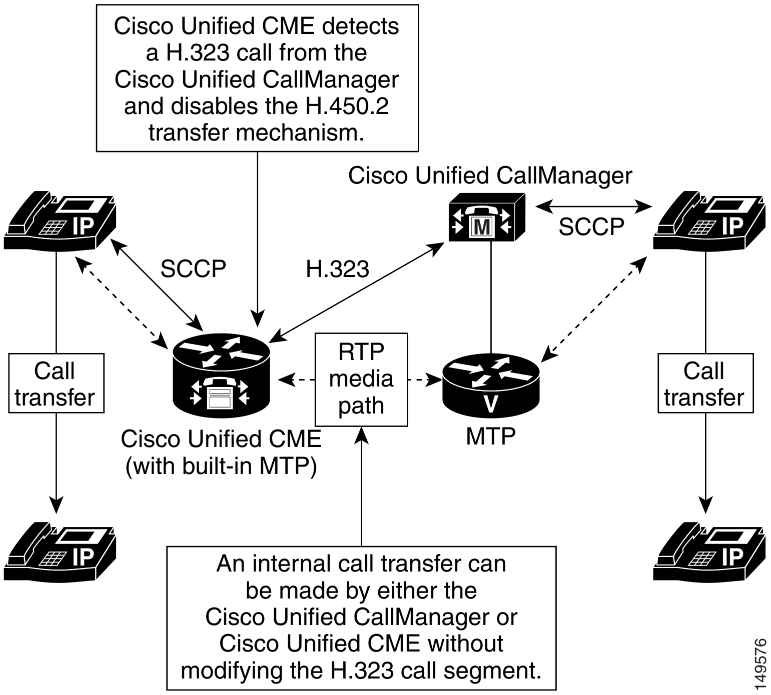
Connecting Cisco Unified CallManager with Cisco Unified CME

This section examines how what you've learned so far in this chapter relates to connecting a Cisco Unified CallManager to a network of Cisco Unified CME systems.

You learned inChapter 6, "Connecting Multiple Cisco Unified CallManager Express Systems with VoIP," that Cisco Unified CME prefers to perform call transfers using H.450.2 but can perform VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway routing when needed. You also learned that a Cisco Unified CME can automatically detect calls to or from a Cisco Unified CallManager and can use this information to disable its normal H.450.2 behavior. The final piece of this puzzle is to understand that an H.323 call to a Cisco Unified CME IP phone always passes through an MTP-like mechanism within Cisco Unified CME. This arrangement allows the Cisco Unified CME to optionally perform its internal transfers without using H.450.2 and without affecting the H.323 connection to Cisco Unified CallManager.

In Cisco Unified CME, the MTP is the Cisco Unified CME router itself. However, you still need a separate MTP device on the Cisco Unified CallManager side in case the Cisco Unified CallManager phone itself invokes additional call transfer operations on the same call. Figure 7-4 shows Cisco Unified CME connecting to a Cisco Unified CallManager using MTP.

Figure 7-4 Cisco Unified CallManager and Cisco Unified CME Connected Using MTPs


Cisco Unified CME detects a H.323 call from the Cisco Unified CallManager and disables the H.450.2 transfer mechanism.
Cisco Unified CallManager
M
SCCP
IP
SCCP
H.323
Call transfer
RTP media path
V
MTP
Cisco Unified CME (with built-in MTP)
An internal call transfer can be made by either the Cisco Unified CallManager or Cisco Unified CME without modifying the H.323 call segment.
149576

The issue of MTP scalability largely does not apply to Cisco Unified CME for two reasons. First, the RTP media stream voice packets have to pass through the Cisco Unified CME router anyway. Even if Cisco Unified CME did not deliberately invoke MTP treatment for the media stream packets, the packets would still need to be routed by the Cisco Unified CME IP routing function. In many cases, the router might also have to perform other operations on the media stream packets, such as firewall and Network Address Translation (NAT). As a result, no additional real-world penalty is incurred by the MTP treatment; it is more or less free.

Second, the number of IP phones that Cisco Unified CME supports is relatively low compared to a Cisco Unified CallManager. The number of phones supported by a Cisco Unified CME router is scaled according to the overall performance of the specific Cisco IOS router model used. Many different router models are available with IP phone support, which ranges from 24 phones to about 240 phones.

The only condition under which the Cisco Unified CME MTP treatment incurs an additional cost is when you actually need codec transcoding. Even in this case, the additional cost usually is not large, because you almost certainly already have DSP resources included in your Cisco Unified CME router to support its PSTN ports. In many cases, you can meet the MTP transcoding requirement simply by adding DSP chips to your existing voice-port hardware. This is in contrast to the need to explicitly add an entire voice module solely for DSP farm transcoding purposes.

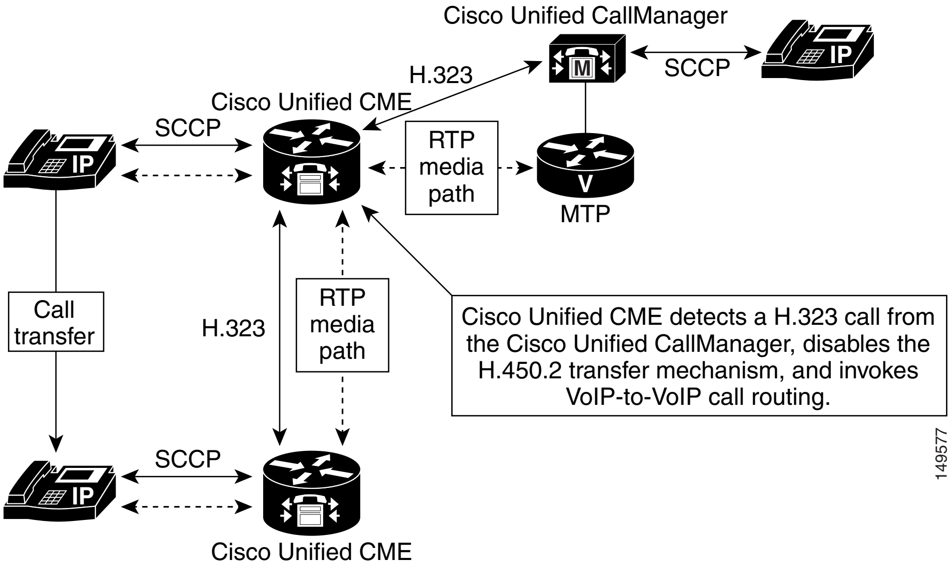
However, in many cases transcoding for call transfer is unneeded, because a Cisco Unified CME has only a single WAN link carrying H.323 calls, and all the H.323 calls tend to use the same codec (either G.711 or G.729). Your Cisco Unified CME may still need DSP farm transcoding services to support three-party conferencing for G.729 calls (see Chapter 6, "Connecting Multiple Cisco Unified CallManager Express Systems with VoIP").

Note The H.323 traffic source from a Cisco Unified CME should be bound to the loopback address. This loopback address should be registered to Cisco Unified CallManager as an H.323 gateway. See "The Role of an H.323 Gatekeeper" section on page 6-9.

Intersite Call Transfer with Multiple Cisco Unified CME Systems

The final call transfer scenario you should understand is what happens with a call placed from a Cisco Unified CallManager to a Cisco Unified CME system that is then transferred to a second Cisco Unified CME system (see Figure 7-5). In this case, the first Cisco Unified CME detects that the call is from a Cisco Unified CallManager. As a result, it invokes VoIP-to-VoIP Cisco IP-to-IP Gateway or hairpin routing to provide the call path (see Chapter 6, "Connecting Multiple Cisco Unified CallManager Express Systems with VoIP," for details).

Figure 7-5 Intersite Call Transfer for a Cisco Unified CallManager with Multiple Cisco Unified CME Systems


Cisco Unified CallManager
H.323
SCCP
Cisco Unified CME
SCCP
RTP media path
MTP
Call transfer
H.323
RTP media path
Cisco Unified CME detects a H.323 call from the Cisco Unified CallManager, disables the H.450.2 transfer mechanism, and invokes VoIP-to-VoIP call routing.
SCCP
Cisco Unified CME
149577

Call Forwarding

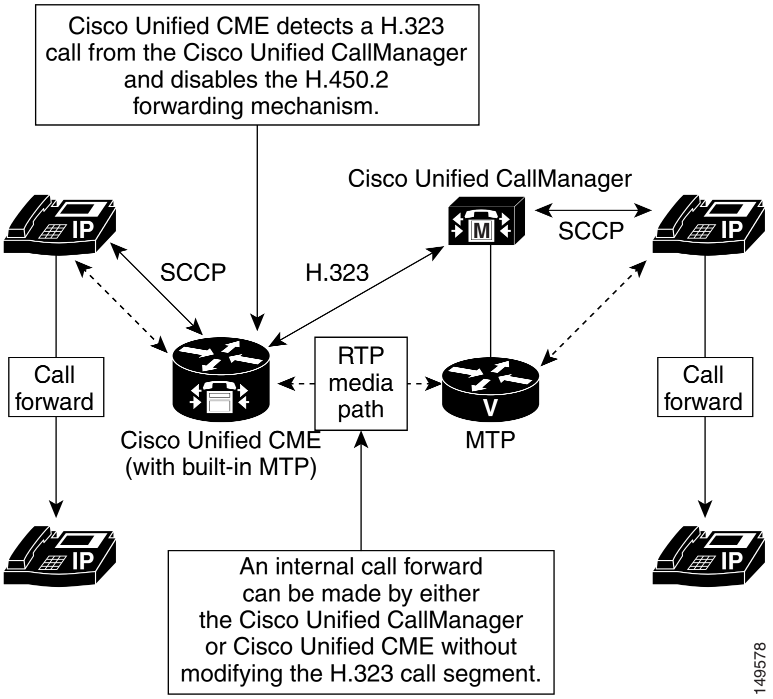
Call forwarding (for busy, no-answer, and unconditional forwarding) raises many of the same issues as call transfer. Likewise, these issues can be addressed using an MTP to simplify the H.323 signaling operations.

The preferred method of handling call forwarding for Cisco Unified CME is H.450.3. Again, Cisco Unified CME can disable its H.450.3 feature when it detects calls from a Cisco Unified CallManager. Under these circumstances, the Cisco Unified CME system falls back to using internal call forwarding or VoIP-to-VoIP call routing for intersite call forwarding.

Note Automatic H.323 to H.323 hairpin is supported starting with Cisco Unified CME 3.1 only. H.450.12 should be enabled for auto-detection of H.450 capabilities. Automatic H.323-to-H.323 hairpin and H.450.12 are supported starting with Cisco Unified CME 3.1.

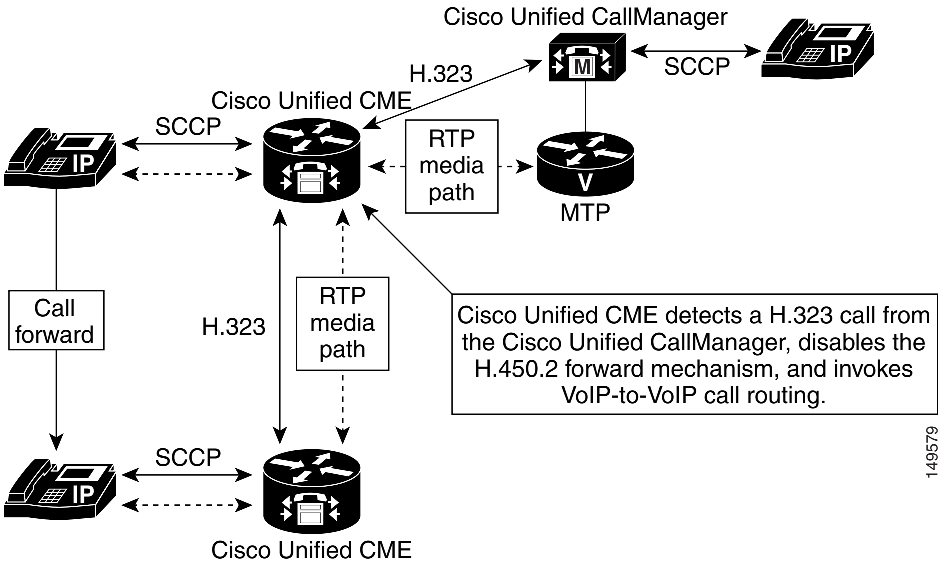
Just like the call-transfer case, an MTP allows internal call forwarding to occur without impact to the H.323 call leg. Of the three types of forwarding—busy, no-answer, and unconditional—the no-answer form generally involves more signaling complexity. When a call forward no-answer occurs, the preliminary call negotiation for the original called phone must be revoked (after the no-answer timeout). It is replaced with a new call to the forward-to destination phone. The forwarded call can potentially require the use of different parameters than those negotiated for the original called phone. The busy and unconditional forms of call forwarding usually do not involve a preliminary call actually reaching the forwarding phone; this tends to simplify the signaling. Figure 7-6 shows call forwarding between a Cisco Unified CME system and a Cisco Unified CallManager using MTP.

Figure 7-6 *Cisco Unified CallManager and Cisco Unified CME Call Forwarding with MTP*


Cisco Unified CME detects a H.323 call from the Cisco Unified CallManager and disables the H.450.2 forwarding mechanism.
Cisco Unified CallManager
SCCP
SCCP
H.323
IP
IP
IP
IP
M
Call forward
RTP media path
V
Call forward
Cisco Unified CME (with built-in MTP)
MTP
An internal call forward can be made by either the Cisco Unified CallManager or Cisco Unified CME without modifying the H.323 call segment.
149578

You can see that Figure 7-5, which shows call transfer, and Figure 7-6, which shows call forwarding, are nearly identical. Figure 7-7 shows intersite Cisco Unified CME call forwarding for a call from a Cisco Unified CallManager. Compare it to Figure 7-5 for the equivalent call transfer case.

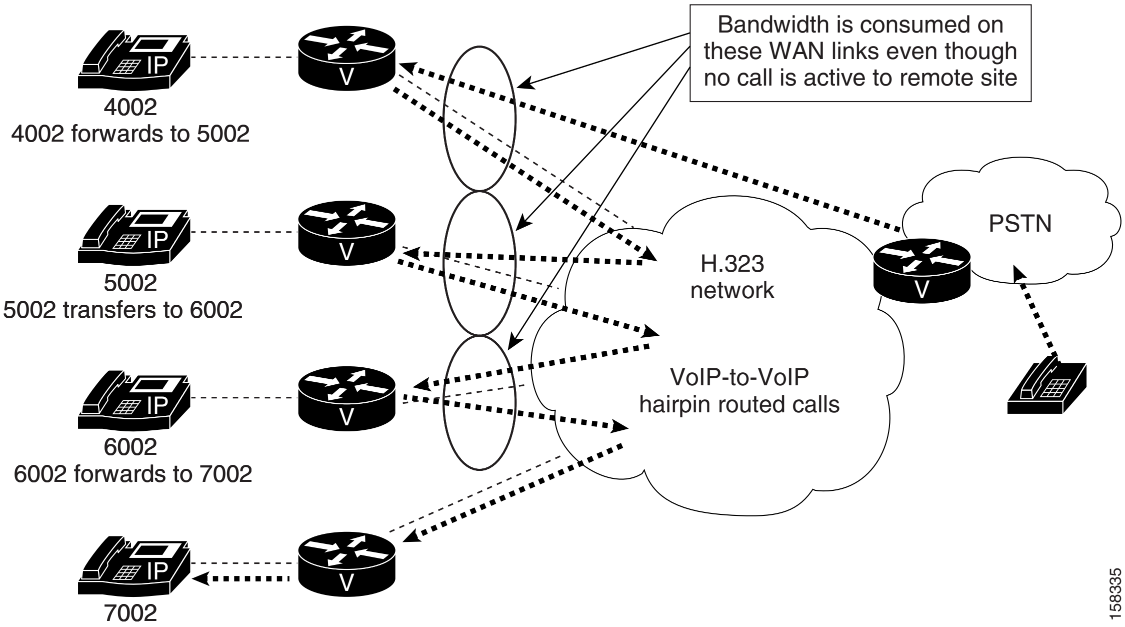
Figure 7-7 *Cisco Unified CallManager Forwarding with Multiple Cisco Unified CME Systems*


Cisco Unified CallManager
H.323
SCCP
M
IP
Cisco Unified CME
SCCP
IP
RTP media path
V
MTP
Call forward
H.323
RTP media path
Cisco Unified CME detects a H.323 call from the Cisco Unified CallManager, disables the H.450.2 forward mechanism, and invokes VoIP-to-VoIP call routing.
149579
SCCP
IP
Cisco Unified CME

For the special case of call forwarding to a voice mail system, note that the H.323 call setup for the forwarded call includes the original called number (the number of the forwarding phone). This can be used to provide integration with the voice mail system and to allow automatic selection of the voice mailbox that belongs to the forwarding phone.

Note There is an issue associate with chained hairpin transfers. See Figure 7-8. In this situation, excess end-to-end signaling and media delay can lead to scarce WAN bandwidth being used needlessly. In the scenario show in Figure 7-8, bandwidth is consumed on the WAN links even though no calls are active to a remote site.

Figure 7-8 The Problem with Chained Hairpin Calls


Bandwidth is consumed on these WAN links even though no call is active to remote site
IP
V
4002
4002 forwards to 5002
5002
5002 transfers to 6002
6002
6002 forwards to 7002
7002
H.323 network
VoIP-to-VoIP hairpin routed calls
PSTN
158335

Connected Party Name and Number Services

One of the reasons why Cisco Unified CME uses the H.450.2 call transfer and H.450.3 call forwarding mechanisms is that it provides a standard means to support updating of the originating phone’s display to track who the connected-to party is. Connected party display is often considered an important feature in business telephone networks. The connected party display is broader than the usual residential caller ID display you may be familiar with at home. Not only does it provide information about the calling party for inbound calls, but it also provides information about the called party for outbound calls. The connected party display can show you the name of the person you have called, for example. This is in contrast to simply displaying the number you dialed. Also, the standard caller ID display function provides a one-time indication of who the caller is only at the beginning of an incoming call. The connected party display feature allows for midcall updates of the connected party information that occur when the far end of the call performs a call transfer.

For example, after a caller has been transferred, the phone display can be updated to show the name and number of the extension he has been transferred to. Likewise, when you receive a call transferred to you by someone else, your phone display may initially show the caller ID of the person who is transferring the call to you. After the transfer is complete, your phone's display may update to show the caller ID of the transferee (caller).

When Cisco Unified CME disables the H.450.2 and H.450.3 mechanisms to interwork with Cisco Unified CallManager, this display update mechanism is unavailable. However, Cisco Unified CallManager has its own mechanism for performing connected party display updates. Cisco Unified CallManager uses H.323 display and information IEs. Cisco Unified CME also supports these IEs for performing connected party display updates.

The H.323 IE messages are carried as part of the H.323 signaling path. They are unaffected by the use of an MTP because they are informational messages only and do not generate changes to the call signaling state. This means that even when a Cisco Unified CallManager performs an internal call transfer hidden behind an MTP, the H.323 information and display IEs are received by the Cisco Unified CME system and are used to provide display updates. Not only can Cisco Unified CME receive display IEs from Cisco Unified CallManager, but it also sends display IEs to Cisco Unified CallManager when Cisco Unified CME performs internal transfer or forwarding.

Cisco Unified CME sends these display IE messages for all H.323 calls regardless of whether a Cisco Unified CallManager is involved in a call. This means that you can still get intersite connected-to party updates in Cisco Unified CME networks where you have chosen to globally disable H.450 services.

Using H.450.x Cisco IP-to-IP Gateway

One final point to understand in planning your Cisco Unified CallManager-to-Cisco Unified CME connections is the advantages that an H.450 Cisco IP-to-IP gateway can provide. You can insert an H.450 Cisco IP-to-IP gateway into the call path between your Cisco Unified CME network and Cisco Unified CallManager, and use it to mitigate some of the issues that arise from the use of VoIP-to-VoIP call paths. If an intersite call transfer or forward initiated by a Cisco Unified CME creates a VoIP hairpin call, you can often use an H.450 Cisco IP-to-IP gateway co-located with your Cisco Unified CallManager to avoid most of the voice path delay caused. Just hairpin the media stream through the Cisco Unified CME system located at the end of a narrow-bandwidth WAN link. See Chapter 6, "Connecting Multiple Cisco Unified CallManager Express Systems with VoIP," for more details about IP-to-IP gateways.

CHAPTER 8

Integrating External Applications with Cisco Unified CallManager Express

Cisco Unified CallManager Express (Cisco Unified CME) can be extended to interface with external applications offered by Cisco and other vendors. This chapter briefly reviews the external applications that you can integrate with Cisco Unified CME, such as applications that use the Telephony Application Programming Interface (TAPI) and Extensible Markup Language (XML) interfaces.

Although Cisco Unity Express is the integrated voice mail system we recommend for use with Cisco Unified CME you also have the option to deploy one of several external voice mail systems with Cisco Unified CME.

See the following documents for more information about Cisco Unity Express and integration with Cisco Unified CME:

- *Cisco Unity Express Design Guide*
  http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/design/design21/cuedg21.html
- *Excerpts from Cisco IP Communications Express: CallManager Express with Cisco Unity Express*
  http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/design/CP_CIPExpress/excerpts.html

Other external applications integrate with Cisco Unified CME by using Skinny Client Control Protocol (SCCP) connections. This chapter does not discuss these application because they appear to Cisco Unified CME as IP phones (SCCP endpoints) and not as an application using an application interface, such as TAPI or XML. SCCP applications register with Cisco Unified CME as IP phones do and communicate with the Cisco Unified CME call processing features via SCCP messages as any IP phone would. Applications in this category include softphone PC applications such as the Cisco IP Communicator and IP Blue Software Solutions softphone.

More information about IP Blue can be found at the following URL: http://www.ipblue.com/.

This chapter addresses integrating Cisco Unified CME to external application in the following sections:

- Cisco Unified CME External Voice Mail Options, page 8-2
- TAPI and XML Application Architecture, page 8-14
- TAPI Applications, page 8-15
- Extensible Markup Language Applications, page 8-19

Note For additional information, see the "Related Documents and References" section on page xii.

Cisco Unified CME External Voice Mail Options

Cisco Unity Express is the integrated voice mail system we recommend for use with Cisco Unified CME. However, you also have the option to deploy one of several external voice mail systems with Cisco Unified CME. You might want to consider one of these voice mail options for your office in the following situations:

- If you are using a Cisco Unified CME platform, such as the Cisco 1760-V, that does not support Cisco Unity Express (although you could use a separate router to house Cisco Unity Express as of 2.0)
- If your Cisco Unified CME router platform does not have any available slots to add the Cisco Unity Express hardware
- If you require features such as unified messaging that are not yet available with Cisco Unity Express
- If you want to deploy a centralized voice mail system to support multiple Cisco Unified CME sites instead of a distributed voice mail option at each site
- If you have an existing legacy voice mail system that you want to continue to use

This chapter briefly reviews the external voice mail options available for use with Cisco Unified CME. These options include the Cisco Unity voice mail system and several nonCisco systems that integrate with Cisco Unified CME via either H.323 Voice over IP (VoIP) or an analog phone interface.

Cisco Unity Voice Mail

Cisco Unity is a Microsoft Windows 2000 server-based IP unified messaging system. Cisco Unity scales up to several thousand users and typically is deployed in a central site of an enterprise network with a Cisco CallManager providing the call control.

Note Note that Cisco Unity and Cisco Unity Express are two different voice mail systems. Cisco Unity Express is a hardware module installed inside the Cisco Unified CME router scaling up to 100 voice mailboxes, whereas Cisco Unity is a separate Windows server platform scaling up to thousands of users.

Cisco Unity unified messaging capabilities allow you to integrate voice mail, e-mail, and faxes into the same end-user mailbox. The mailbox operation is highly customizable via call handlers. Cisco Unity provides options for integrating with the Microsoft Outlook or Lotus Notes mail architectures. Cisco Unity leverages Active Directory to access your network's user and location directory.

Although Cisco Unity unified messaging features provide many productivity-enhancing applications such as Cisco Personal Assistant and text-to-speech support, you can also choose to deploy it as a voice mail-only system. Cisco Personal Assistant is a telephony application suite that streamlines communications by helping users manage how and where they can be reached.

Different levels of licensing are available with Cisco Unity for a voice mail-only deployment or a full unified messaging system. Cisco Unity is a sophisticated messaging system with robust failover and networking options.

Cisco Unity uses IP as the transport and SCCP for call control, appearing to Cisco Unified CME as an IP phone (SCCP) endpoint. Cisco Unity can support a single Cisco Unified CME in a standalone deployment or can be deployed at a central site in your network with multiple Cisco Unified CMEs at remote sites in a centralized voice mail scenario. These architectures are discussed further in the following sections.

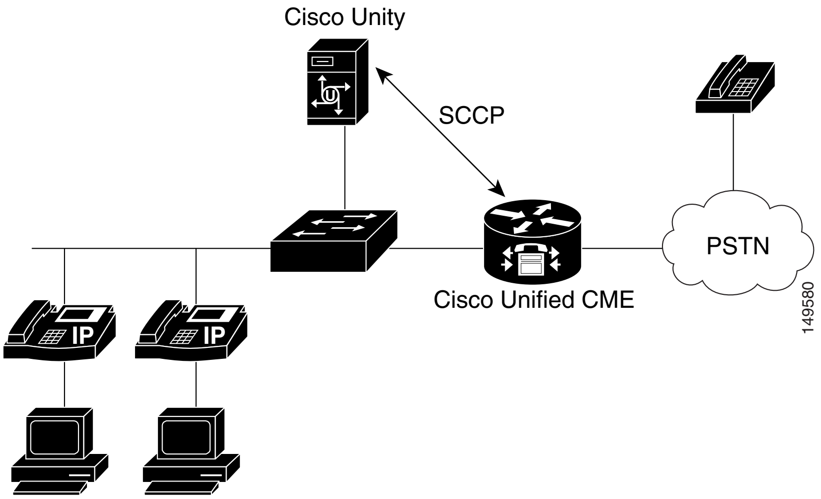
Note Cisco Unified CME is Cisco IOS software-based, whereas Cisco Unity is a Microsoft Windows 2000-based application; therefore, users considering this combination of applications should have a good working knowledge of both operating systems. Cisco Unity uses Microsoft Exchange (5.5, 2000, and 2003) or Lotus Domino mail stores, so familiarity with these technologies is also beneficial.

Standalone Cisco Unified CME System with Cisco Unity

You can connect a standalone Cisco Unified CME with a dedicated Cisco Unity system to provide unified or voice mail services to a single site. Although technically feasible, this is often not a cost-effective way to deploy Cisco Unity. Cisco Unity is an application designed to support large numbers of users, whereas Cisco Unified CME can support only up to 240 users. Figure 8-1 shows how Cisco Unified CME is connected to the Cisco Unity system.

Although Cisco Unified CME functions as the call control system for taking care of IP phone and PSTN calls, Cisco Unity provides the voice mail services. Cisco Unity communicates with Cisco Unified CME using SCCP emulating IP phone endpoints.

Figure 8-1 Standalone Cisco Unified CME with Cisco Unity Messaging



Multiple Cisco Unified CME Systems with a Centralized Cisco Unity System

A much more typical and cost-effective model of using Cisco Unity with Cisco Unified CME is as a centralized messaging system to several remote Cisco Unified CME sites. Figure 8-2 shows multiple Cisco Unified CME systems distributed across several smaller sites connected to a shared, centralized Cisco Unity system. A Cisco Unified CME system at the central site collocated with the Cisco Unity server is required. This Cisco Unified CME relays both voice and message waiting indicator (MWI) to the remote sites.

A centralized Cisco Unity system offers several advantages:

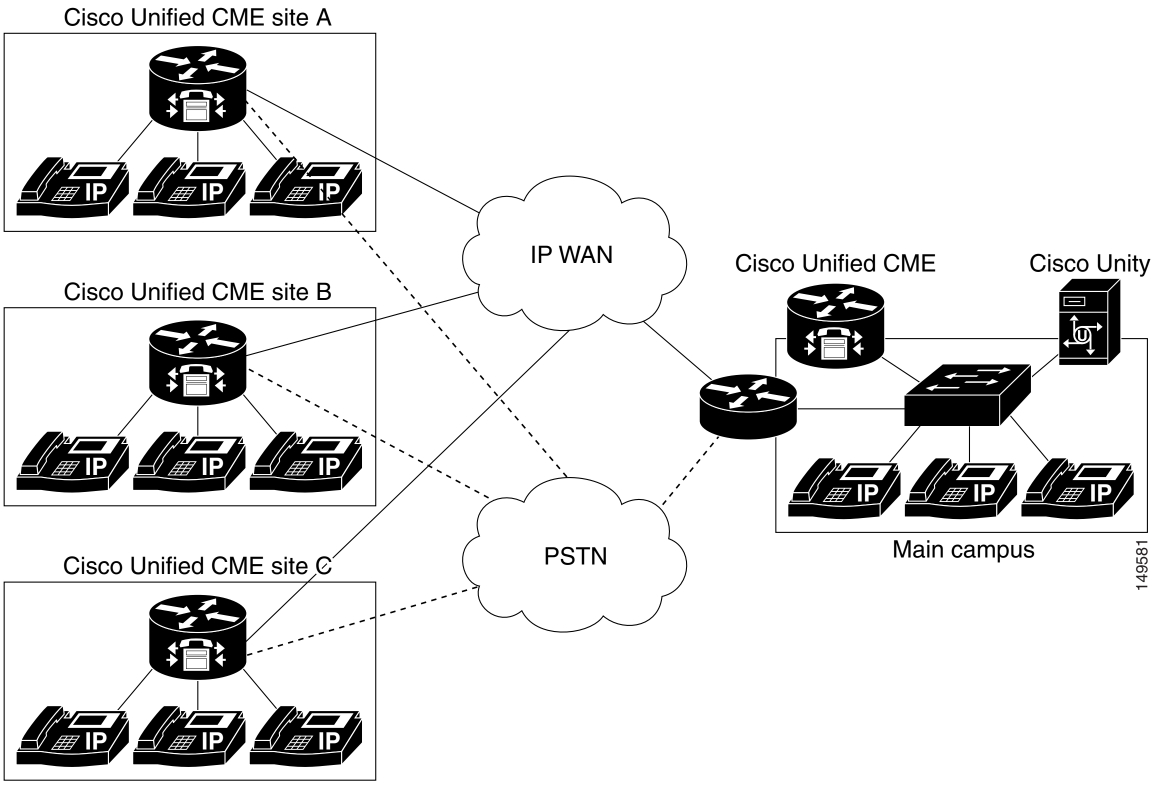
- It eases the management and provisioning of voice mail.

- It provides a single integrated user directory that eases sending voice mail and setting up distribution lists across users physically located at different sites.
- It facilitates forwarding and replying to voice messages without requiring networking of the distributed voice mail systems between the individual sites.
- It conserves valuable bandwidth by not forwarding and replying to voice mails between users resident at different sites.

Configuring Cisco Unified CME for Cisco Unity

Cisco Unity integrates with Cisco Unified CME as SCCP-controlled IP phone endpoints. Each voice mail port on Cisco Unity is configured as an ephone on Cisco Unified CME, and the voice mail pilot number is configured as an ephone-dn that appears on each of the phones (ports).

Figure 8-2 Multiple Cisco Unified CME Systems with Cisco Unity Messaging


Cisco Unified CME site A
IP
IP
IP
IP WAN
Cisco Unified CME
Cisco Unity
Cisco Unified CME site B
IP
IP
IP
IP
IP
IP
PSTN
Main campus
Cisco Unified CME site C
IP
IP
IP
149581

The Cisco Unity ports register with the Cisco Unified CME router using a voice mail device ID (vm-device-id) such as Cisco UM-VI2. The following example shows the Cisco Unified CME configuration for connecting to a four-port Cisco Unity voice mail system.

```
telephony-service
 voicemail 6800
!
ephone-dn 32
 number 6800
 name “VM Port 1”
 preference 0
 no huntstop
!
```

```
ephone-dn 33
 number 6800
 name "VM port 2"
 preference 1
 no huntstop
!
ephone-dn 34
 number 6800
 name "VM port 3"
 preference 2
 no huntstop
!
ephone-dn 35
 number 6800
 preference 3
 name "VM Port 4"

ephone 5
 vm-device-id CiscoUM-VI1
 button 1:32
!
ephone 6
 vm-device-id CiscoUM-VI2
 button 1:33
!
ephone 7
 vm-device-id CiscoUM-VI3
 button 1:34
!
ephone 8
 vm-device-id CiscoUM-VI4
 button 1:35
```

The **voicemail 6800** command defines the voice mail pilot number as extension 6800. You can define an ephone-dn for each of the four ports; these definitions control call routing to Cisco Unity. All the ephone-dns have 6800 as the extension and are tagged with **preference 0** to **preference 3**. You need four individual ephone-dns, one per port, to route and deliver four calls to the Cisco Unity system simultaneously. From the Cisco Unified CME system point of view, four IP phones have an appearance of extension 6800; therefore, four individual calls to 6800 can be busy at the same time.

The **preference** and **no huntstop** designations ensure that the Cisco Unified CME system hunts across the available phones if some of them are busy.

Each of the physical ports is defined as an ephone. To Cisco Unified CME, Cisco Unity ports look like an IP phone, and they register as such. The vm-device-id (for example, Cisco UM-VI2) defined for each ephone must match the device ID configured in the Cisco Unity configuration.

You configure call forwarding to voice mail on your employee's IP phones exactly as you would for Cisco Unity Express, as shown in the following example.

```
ephone-dn 1
 number 6001
 call-forward busy 6800
 call-forward noan 6800 timeout 10
```

With the configurations given in the previous examples, users on your system can press the messages button on their IP phones to retrieve their voice mail. They can also call the voice mail pilot number 6800 directly—for example, from the PSTN—to access their voice mail.

MWI

MWI with Cisco Unity is accomplished via outdial directory numbers (DNs), similar to the architecture with Cisco Unity Express (but not configured in exactly the same way). Cisco Unified CME defines two MWI DNs, one for turning on MWI and another for turning it off. Cisco Unity outdials to one of these numbers to control the phone's MWI state. This configuration is shown in the following example.

```
ephone-dn 30
 number 8000
 mwi on
!
ephone-dn 31
 number 8001
 mwi off
```

The extension for which MWI must be turned on or off is derived from the caller ID (the number of the call's originator) provided in the SCCP message received by Cisco Unified CME. Cisco Unity populates the appropriate caller ID in the SCCP message sent to Cisco Unified CME when it initiates the call to one of the MWI DNs. Cisco Unified CME then uses this caller ID to determine which IP phone on the system should receive MWI and sends a separate SCCP message to the phone(s) to turn its MWI on or off.

The MWI configuration for Cisco Unity differs from that of Cisco Unity Express in two important ways:

- For Cisco Unity Express, the MWI DN requires wildcard dots following the MWI extension number (as many dots as you have digits in your extensions). For four-digit extensions, the MWI DN for Cisco Unity Express would specify **number 8000....** instead of the **number 8000** command used for Cisco Unity.
- For Cisco Unity Express, the IP phone extension for which MWI must be turned on or off is derived from the digits that match the dots just described—that is, from the *called number* of the outgoing call to the MWI DN. For Cisco Unity, the IP phone extension is derived from the *calling number* of the outgoing call to the MWI DN.

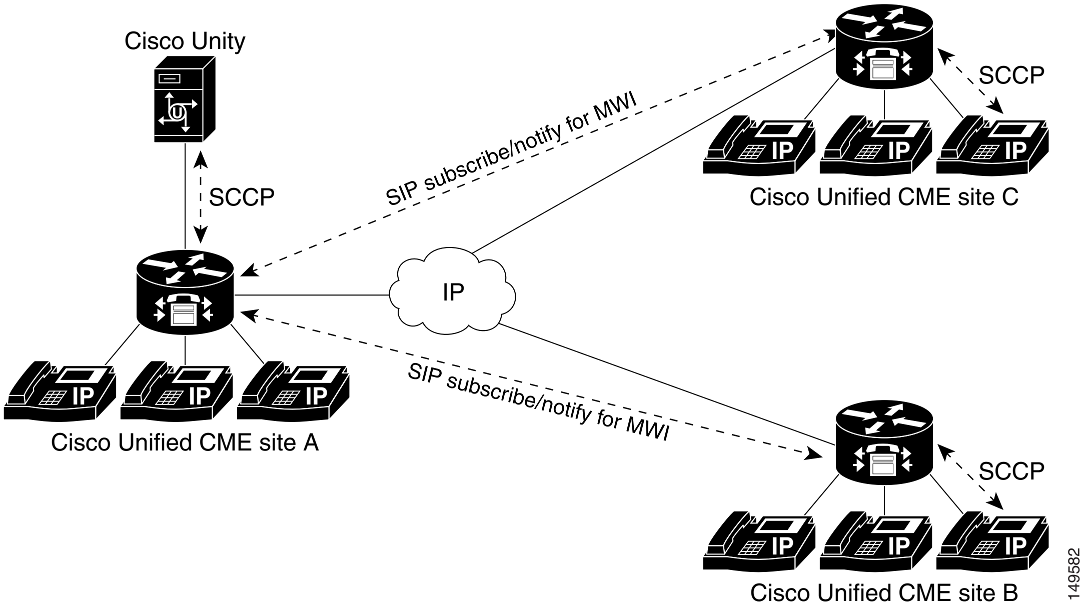
MWI Relay

Cisco Unity physically integrates only with the single Cisco Unified CME that is collocated with it. All the Cisco Unity ports register with this Cisco Unified CME system. To get Cisco Unity to support voice mail for users of Cisco Unified CME systems at remote sites, certain information must be relayed by the central Cisco Unified CME that is physically connected to Cisco Unity.

Calls to Cisco Unity to leave or retrieve messages can be freely routed across your network between the sites based on your dial plan. The relay mechanism comes into play only for getting MWI notifications to an IP phone at a remote site.

Cisco Unified CME contains an MWI relay mechanism that is configured at the central Cisco Unified CME (the one with the MWI DNs that Cisco Unity dials). The central Cisco Unified CME cannot send an SCCP message directly to an IP phone that is registered with a different Cisco Unified CME system. Instead, it uses a Session Initiation Protocol (SIP) subscribe/notify mechanism to notify the remote Cisco Unified CME of an MWI change. The remote Cisco Unified CME system (where the IP phone is registered) then sends an SCCP message to the phone to change its MWI state. This configuration is shown in Figure 8-3.

Figure 8-3 MWI Relay with Cisco Unity


Cisco Unity
SCCP
SIP subscribe/notify for MWI
IP
IP
IP
IP
Cisco Unified CME site A
SCCP
IP
IP
IP
Cisco Unified CME site C
SIP subscribe/notify for MWI
SCCP
IP
IP
IP
Cisco Unified CME site B
149582

The MWI relay configuration at the central Cisco Unified CME (site A) is shown in the following example.

```
telephony-service
   ip source-address 10.10.10.1
   mwi relay
   mwi expires 99999
   voicemail 6800
```

The **mwi relay** command lets the Cisco Unified CME router relay the MWI information to a remote IP phone. The **mwi expires** command sets the expiry timer for the SIP subscribe/notify registration.

The MWI relay configuration at one of the remote Cisco Unified CME sites (for example, site B) is shown in the following example.

```
telephony-service
   ip source-address 10.20.20.10
   mwi sip-server 10.10.10.1 transport tcp
!
ephone-dn 1
   number 2000
   mwi sip
   call-forward noan 6800 timeout 10
   call-forward busy 6800
!
dial-peer voice 101 voip
   destination-pattern 6800
   session target ipv4:10.10.10.1
   codec g711ulaw
   dtmf-relay h245-alphanumeric
   no vad
```

The **mwi sip-server** command instructs the Cisco Unified CME at site B to subscribe to the SIP server on Cisco Unified CME site A (IP address 10.10.10.1 in preceding example). Each of the ephone-dns at sites B and C must contain the **mwi sip** command to ensure that the controlling Cisco Unified CME system knows that this phone's MWI is controlled by a SIP notification from another site. As soon as the configuration is entered, a **show mwi relay clients** command executed at site A shows all the extensions subscribed to the Cisco Unified CME site A SIP server.

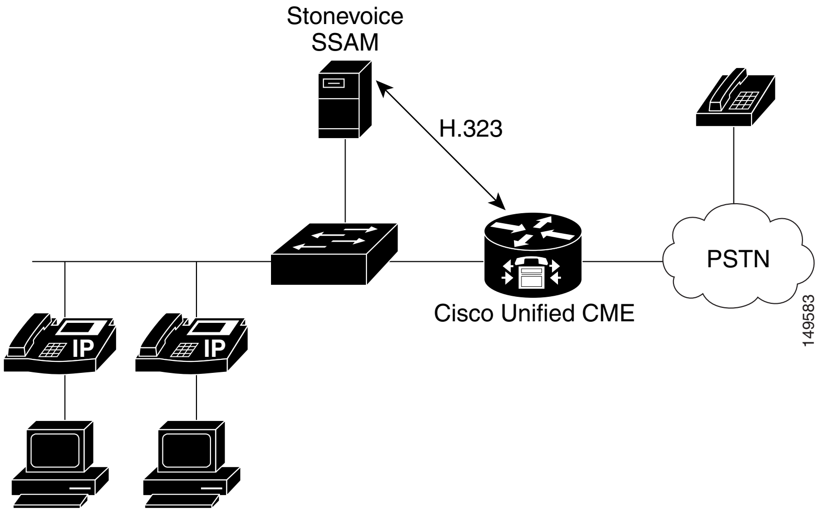
The dial peer shown in the preceding example ensures that users at site B can dial 6800 (the voice mail pilot number). The call is routed across VoIP to site A, where the Cisco Unity system is located.

Stonevoice Voice Mail

Cisco Unified CME can integrate with various nonCisco voice mail systems using H.323. One of the H.323 voice systems supported by Cisco Unified CME is the Stonevoice Switch Answering Machine (SSAM), a unified messaging system designed to provide access to and control over software-based voice mail services.

SSAM is a Windows 2000-based application that runs on an external PC. All traffic between Cisco Unified CME and SSAM uses H.323. Figure 8-4 shows how the Stonevoice SSAM application integrates with Cisco Unified CME.

Figure 8-4 Cisco Unified CME with Stonevoice SSAM Voice Mail



When integrated with Cisco Unified CME, SSAM supports the following:

- Direct access to voice mail
- Call forward no answer (CFNA) or call forward busy (CFB) to a personal greeting
- MWI

For more information on the SSAM system, go to http://www.stonevoice.com/.

The following sections provide more details on integrating a Stonevoice system with Cisco Unified CME, including

- Configuring Cisco Unified CME for Stonevoice, page 8-9
- MWI for Stonevoice, page 8-10

Configuring Cisco Unified CME for Stonevoice

Communication between Cisco Unified CME and SSAM is by H.323, so you have to configure an H.323 dial peer to direct calls into the SSAM system. You must configure a voice mail pilot number (for example, 9999) on SSAM for message retrieval and an individual voice mail number for each extension (ephone-dn). Because the original called number (the IP phone extension) is not preserved when the call is forwarded to SSAM via H.323, you must embed this information in the called number (the call forward number) delivered to SSAM.

The following example shows a sample Cisco Unified CME configuration defining a voice mail pilot number of 9999 (used when you press the messages button on your IP phone), voice mail number 9001 for extension 1001, and 9002 for extension 1002.

```
dial-peer voice 100 voip
 destination-pattern 9...
 session target ipv4:172.19.153.120
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
!
telephony-service
 voicemail 9999
!
ephone-dn 1
 number 1001
 call-forward busy 9001
 call-forward noan 9001 timeout 10
!
ephone-dn 2
  number 1002
  call-forward busy 9002
  call-forward noan 9002 timeout 10
```

The voice dial peer command **destination-pattern 9...** ensures that all calls to 9999, 9001, and 9002 are directed to SSAM via H.323. The IP address 172.19.153.120 in this example belongs to the SSAM system.

The **voicemail 9999** command under **telephony service** is the voice mail pilot number used when you press the messages button on your IP phone. This number must match the "Voicemail number" parameter on the SSAM Modify IP Telephony System window.

Individual voice mail forwarding numbers are defined for each extension. These are used in the **call-forward busy** and **call-forward noan** fields of the ephone-dn Cisco Unified CME configuration. These numbers must be configured on the SSAM system for each individual user. For example, for the person on ephone-dn 1, you configure his or her extension (1001) in the "First extension number" field, and configure 9001 in the "Voicemail number" field of the SSAM Account Management window for this user.

MWI for Stonevoice

MWI is controlled by the SSAM system outdialing with H.323 to a Cisco Unified CME MWI DN. The extension for which the MWI must be turned on or off is embedded in the dialed number. The Cisco Unified CME configuration for this is shown in the following example.

```
ephone-dn 11
 number 8000*....*1 secondary 8000*....*2
 mwi on-off
 no huntstop
!
ephone-dn 12
 number 8000*....*1 secondary 8000*....*2
 mwi on-off
 preference 1
```

You should configure as many of these MWI ephone-dns as you have "ports" on the SSAM system so that the maximum number of simultaneous calls can be handled correctly. Use the Cisco Unified CME **preference** and **no huntstop** command designations to make sure the Cisco Unified CME system hunts across any available MWI ephone-dns.

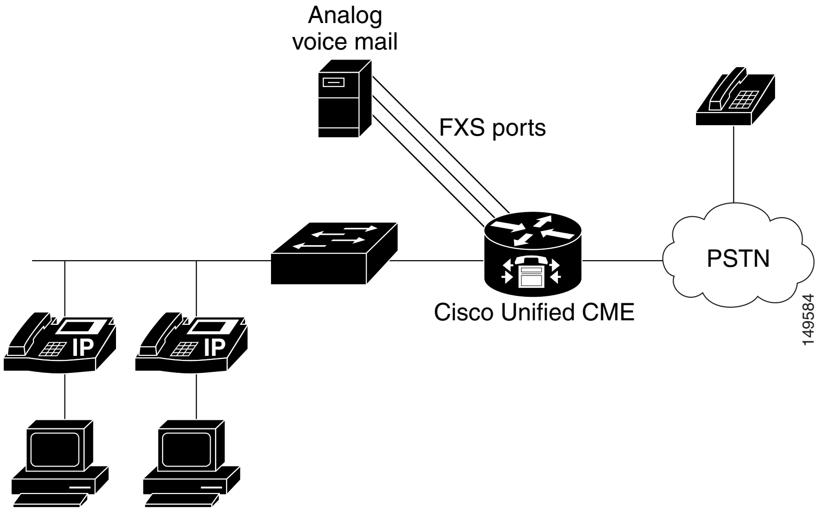
When the SSAM system makes an outgoing call to Cisco Unified CME, the MWI information is embedded in the called party's telephone number—for example, 8000*1001*1 or 8000*1001*2. The 8000 is the MWI DN's number, and the asterisks are used as delimiters. The extension for which MWI should be turned on or off is contained between the asterisks, and the final digit in the string specifies whether MWI is on (1) or off (2).

The notation 8000*....*1 in the ephone-dn definition accepts any extension number and represents the extension digits that Cisco Unified CME extracts to determine for which IP phone to turn MWI on or off. The MWI on (ending in digit 1) and MWI off (ending in digit 2) strings are given on the same ephone-dn as the primary and secondary extensions on that ephone-dn, as shown in the preceding example.

Analog Voice Mail

You can integrate Cisco Unified CME with analog systems to provide voice mail services, as shown in Figure 8-5. In general, these systems connect to the Cisco Unified CME via Foreign Exchange Station (FXS) analog phone interfaces. Each port is configured as a normal plain old telephone service (POTS) dial peer in Cisco Unified CME.

Figure 8-5 Cisco Unified CME with Analog Voice Mail



Cisco Unified CME interacts with the analog voice mail system via inband dual-tone multifrequency (DTMF) tones. All call routing and MWI information exchanged between Cisco Unified CME and the voice mail system also occurs via DTMF tones.

When integrated with Cisco Unified CME, an analog voice mail system provides the following:

- Direct access to voice mail
- CFNA or CFB to a personal greeting
- MWI

Many types of analog voice mail systems are available. The Octel system from Avaya and the Reception system from Active Voice, LLC are two of the more popular models. The following sections discuss Cisco Unified CME integration with these systems.

Octel

Integrating the Octel voice mail system with Cisco Unified CME requires configuration on both systems. The configuration sample in the following example shows how to configure the Cisco Unified CME.

```
call application voice bator flash:app-h450-transfer.2.0.0.9.tcl
call application voice bator language 1 en
call application voice bator set-location en 0 flash:/prompts
!
voice-port 1/0/0
 caller-id enable
!
voice-port 1/0/1
 caller-id enable
!
dial-peer voice 5000 pots
 application bator
 destination-pattern 5000.....
 port 1/0/0
!
telephony-service
 voicemail 5000
 transfer-system full-consult
!
vm-integration
```

```
 pattern direct 2 CGN
 pattern ext-to-ext no-answer 5 CGN * FDN
 pattern ext-to-ext busy 7 CGN * FDN
 pattern trunk-to-ext no-answer 5 CGN * FDN
 pattern trunk-to-ext busy 7 CGN * FDN
!
ephone-dn 1
 number 1000
 call-forward busy 5000
 call-forward noan 5000 timeout 5
 application bator
 no huntstop
!
ephone-dn 2
 number 1001
 call-forward busy 5000
 call-forward noan 5000 timeout 5
 application bator
!
ephone-dn 100
 number 3000*....*
 mwi on
!
ephone-dn 101
 number 3001*....*
 mwi off
```

The Tool Command Language (TcL) application (called *bator* in the preceding configuration) is used to support a hookflash operation on the FXS ports. FXS port 1/0/0 is used for voice mail access, so the POTS dial peer points to this port. Port 1/0/1 is used for MWI operation.

The series of **vm-integration** commands specifies the DTMF digit strings to be generated to the analog voice mail system to control feature operation, such as selecting which greeting (external or internal, or busy or no answer) to play to the caller. The MWI DNs have asterisk delimiters surrounding the wildcards that match the extension number for which MWI must be turned on or off.

Note the following restrictions when integrating an Octel system with Cisco Unified CME:

- One FXS port must be dedicated for MWI operation.
- The Octel system must have analog ports and must be configured for analog DTMF integration. Digital and Simplified Message Desk Interface (SMDI) integration with Unified CME is not supported.
- The Octel system does not distinguish between extension-to-extension and trunk-to-extension transfers. Thus, you must configure the DTMF patterns for these transfers with the same values on the Cisco Unified CME system.
- The MWI ephone-dn must use the . wildcard rather than the T wildcard to specify the exact extension length. Also, you must use an asterisk before and after configuring the called party ID (for example, **number 3000*....***).

Active Voice Reception

The Reception system from Active Voice, LLC is another popular voice mail system. To allow calls to be forwarded to the Reception system, you must configure Cisco Unified CME with four different DTMF patterns for the following four possible call flows:

- Extension-to-extension no answer
- Extension-to-extension busy

- Extension-to-trunk no answer
- Extension-to-trunk busy

When the Reception system receives the DTMF pattern, it plays the corresponding voice mail prompt.

The following example shows how to configure Cisco Unified CME to work with the Reception voice mail system.

```
voice-port 1/0/0
 caller-id enable
!
voice-port 1/0/1
 caller-id enable
!
dial-peer voice 5000 pots
 application bator
 destination-pattern 6800.....
 port 1/0/0
!
telephony-service
 voicemail 6800
!
vm-integration
 pattern direct 2 CGN *
 pattern ext-to-ext no-answer 5 FDN * CGN *
 pattern ext-to-ext busy 7 FDN * CGN *
 pattern trunk-to-ext no-answer 4 FDN * CGN *
 pattern trunk-to-ext busy 6 FDN * CGN *
!
phone-dn 2
 number 3002
 call-forward busy 6800
 call-forward noan 6800 timeout 10
!
ephone-dn 25
 number A1.....*
 mwi on
!
ephone-dn 26
 number A2.....*
 mwi off
```

PSTN-Based Voice Mail

Another option for voice mail with Cisco Unified CME is through your PSTN provider. The call flows to the voice mail from your PSTN provider are controlled by the central office (CO) PSTN switch. If the lines to your business are busy or don’t answer, the voice mail system at the CO picks up and stores the senders’ voice messages at the voice mail storage located at the CO. You do not need to configure Cisco Unified CME for this type of voice mail. You do need to configure MWI, however.

CO-based voice mail systems signal MWI by using stutter dial tone. When you go off-hook on your phone, you hear the tone and know you have a message. This works well if you use an analog phone directly connected to the CO and you, therefore, get dial tone from the CO. If you have a Cisco Unified CME system in your office with IP phones on, however, dial tone comes from the Cisco Unified CME system, not from the CO.

To hear stutter dial tone provided by a CO-based voice mail system, you can use the Cisco Unified CME 3.2 FXO Trunk Line Select feature by pressing a button on your IP phone. It directly selects a CO Foreign Exchange Office (FXO) line, which gets dial tone from the CO, and you can hear stutter dial tone.

The following example shows how to use the **trunk** command to create a direct connection to a CO line on an IP phone.

```
voice-port 1/0/0
   connection plaropx 1082
dial-peer voice 82 pots
   destination-pattern 82
   port 1/0/0
   forward-digits 0
ephone-dn 10
   number 1010
   name manager
ephone-dn 11
   number 1082
   name private-line
   trunk 82
ephone 1
   button 1:10 2:11
```

Example 11-10 shows the following sequence of events:

- You press the softkey 2 on your phone, and it automatically triggers the configuration for ephone-dn 11.
- ephone-dn 11 initiates a call to 82, which matches the dial peer that points to FXO line 1/0/0.
- When line 1/0/0 goes off-hook (as if you had picked up an analog phone set directly connected to the CO), it does not dial any digits. The impact is that you can hear the dial tone provided by the CO.

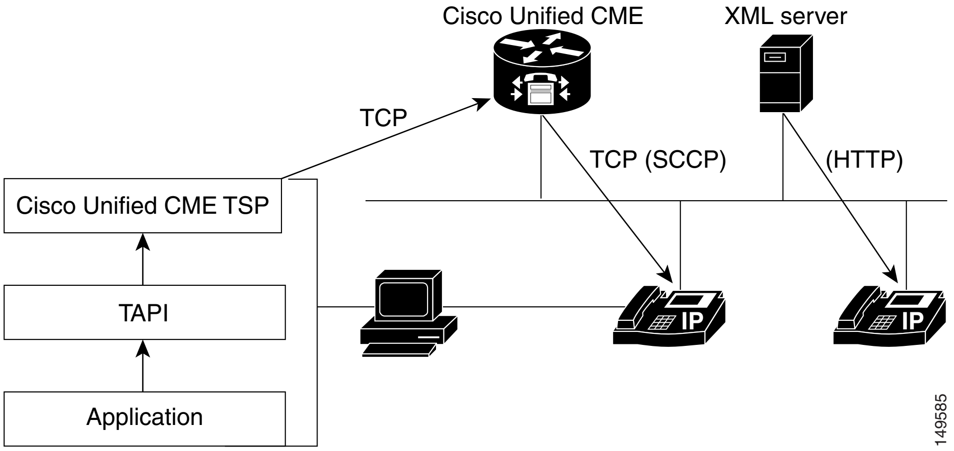
TAPI and XML Application Architecture

TAPI applications interface directly with the Cisco Unified CME call processing software to control the call processing signaling events that apply to an IP phone. For example, a TAPI application can answer a call on behalf of a phone, make the phone go off-hook, or disconnect a call. Microsoft Windows software-based screen-pop applications typically use TAPI.

XML applications interface directly with the IP phone and leverage its HTTP capabilities. The phone has one or more URLs as part of its software load that it accesses when buttons such as the services or directory keys are pressed. The XML application renders some text or graphics on the phone's display. Cisco Unified CME call processing is not involved in this application interchange. XML applications control the phone display while the phone is idle (that is, not on a call).

Figure 8-6 shows how TAPI and XML applications interface with Cisco Unified CME and its IP phones. The left side of the figure depicts a TAPI application. An employee has an IP phone and PC on the desktop. The PC runs a productivity application, such as a contact management application, that provides a screen pop based on caller ID whenever a call starts ringing. All messaging between the application and the phone passes through Cisco Unified CME and is interpreted by the Cisco Unified CME software. On the right side of the figure is an XML application. The phone has a URL that points to a server. The server application writes to the phone display using HTTP.

Figure 8-6 TAPI and XML Application Architecture



TAPI Applications

TAPI is a Microsoft software application interface for integrating-telephony-services into Microsoft Windows software-based PC applications. Cisco Unified CME provides telephony services by a TAPI Service Provider (TSP) interface to applications.

The TSP allows TAPI-based applications such as Microsoft Outlook and Microsoft Customer Relationship Management (CRM) to provide call control to the IP phones connected to Cisco Unified CME. Other TAPI-based applications are available in the industry, such as automatic dialers. You can use these applications to control an IP phone to make and receive calls via a computer or to trigger database lookups based on caller ID.

The following sections describe TAPI in more detail, including the following topics:

- Cisco Unified CME TAPI Light, page 8-15
- Cisco Unified CME TSP Functions, page 8-16
- Cisco CRM Communications Connector, page 8-18

Cisco Unified CME TAPI Light

Cisco Unified CME offers a TAPI Light capability, which is not a full TAPI implementation but a selection of the applicable components for Cisco Unified CME. The implementation consists of two parts: one part resides on the Windows platform, and the other part resides in Cisco Unified CME Cisco IOS software.

The interface between the TSP in the Microsoft Windows application and Cisco Unified CME uses SCCP over TCP. Cisco Unified CME listens on a standard TCP port, while the TAPI client authenticates to Cisco Unified CME by providing a username and password unique for each IP phone on Cisco Unified CME. The Microsoft Windows application's TSP must have the same username, password, and port number configured to be able to connect successfully with Cisco Unified CME and exert phone and call control. The username and password authentication provides a layer of security to Cisco Unified CME to enable authorized application development.

The following example shows the configuration of the username and password associated with the IP phone on Cisco Unified CME. This information must be quoted by the TAPI application during login to be able to control the phone. The **telephony-service ip source-address** command specifies the port number used for communication between Cisco Unified CME and the TAPI application.

```
telephony-service
  ip source-address 172.19.153.129 port 2000
!
ephone-dn 1
 number 3001
 description User1
 name User1
 call-forward busy 3105
 call-forward noan 3105 timeout 10
!
ephone 1
 username "User 1" password user1
 mac-address 0009.B7F7.5793
 speed-dial 4 3100 label "AA"
 button 1:1
```

You can verify IP phone TAPI application login status with the **show ephone login** Cisco Unified CME command.

Cisco Unified CME TSP Functions

The Cisco Unified CME TSP provides the following functions:

- Allows multiple addresses on a single line.
- Makes calls using address book dialing from applications.
- Answers or rejects calls.
- Holds calls using window pop-ups.
- Provides caller ID information to applications.
- Places calls on hold and switches between active calls.
- Transfers calls.

When using TAPI applications with Cisco Unified CME, consider the following restrictions:

- Media or voice termination is not supported. Media or voice traffic is sent to the phone. The TAPI application has access only to signaling events.
- TAPI clients can operate on only one phone line at a time.
- Multiple users and call handling of multiple calls on a single client are not supported.
- Java TAPI (JTAPI) is not supported.

We have partnered with independent TAPI developers to provide support for TAPI development.

Table 8-1 lists the TAPI and TSP functions supported in the Cisco Unified CME TSP.

Table 8-1 Supported Cisco Unified CME TAPI/TSP Functions

TAPI Function	TSP Function	Description
lineAnswer	TSPI_lineAnswer	Answers the specified offered call.
lineBlindTransfer	TSPI_lineBlindTransfer	Performs a blind or single-step transfer of the specified call to the specified destination address.
lineClose	TSPI_lineCloseCall	Closes the specified open line device after completing or aborting all outstanding calls and asynchronous operations on the device.
lineCompleteTransfer	TSPI_lineCompleteTransfer	Completes the transfer of the specified call to the party connected in the consultation call.
lineDial	TSPI_lineDial	Dials the specified dialable number on the specified call.
lineDrop	TSPI_lineDrop	Drops or disconnects the specified call.
lineGetAddressID	TSPI_lineGetAddressID	Returns the address identifier associated with the address in a different format on the specified line.
	TSPI_lineGetCallAddressID	Retrieves the address identifier for the indicated call.
lineGetCallInfo	TSPI_lineGetCallInfo	Returns detailed information about the specified call.
TAPI Function	TSP Function	Description of function.
lineGetCallStatus	TSPI_lineGetCallStatus	Returns the current status of the specified call.
lineGetDevConfig	TSPI_lineGetDevConfig	Returns a data structure object, the contents of which are specific to the line (service provider [SP]) and device class, giving the current configuration of a device associated one-to-one with the line device.
	TSPI_lineGetExtensionID	Returns the extension identifier that the SP supports for the indicated line device.
lineGetID	TSPI_lineGetID	Returns a device identifier for the specified device class associated with the selected line, address, or call.
	TSPI_lineGetNumAddressIDs	Retrieves the number of address identifiers supported on the indicated line.
lineHold	TSPI_lineHold	Places the specified call on hold.
lineMakeCall	TSPI_lineMakeCall	Places a call on the specified line to the specified destination address.
lineNegotiateExtVersion	TSPI_lineNegotiateExtVersion	Returns the highest extension version number the service provider can operate under for this device, given the range of possible extension versions.
	TSPI_lineNegotiateTSPIVersion	Returns the highest service provider interface (SPI) version the service provider can operate under for this device, given the range of possible SPI versions.
lineOpen	TSPI_lineOpen	Opens the line device whose device identifier is given, returning the service provider's handle for the device.
lineSetCallParams	TSPI_lineSetCallParams	Sets certain parameters for an existing call.
	TSPI_lineSetDefaultMedia Detection	Tells the service provider the new set of media types to detect for the indicated line, replacing any previous set.
TAPI Function	TSP Function	Description of function

Table 8-1 Supported Cisco Unified CME TAPI/TSP Functions

TAPI Function	TSP Function	Description
lineSetStatusMessages	TSPI_lineSetStatusMessages	Lets TAPI specify which notification messages the service provider should generate for events related to status changes for the specified line or any of its addresses.
lineSetupTransfer	TSPI_lineSetupTransfer	Initiates a transfer of a call.
lineUnhold	TSPI_lineUnhold	Retrieves the specified held call.

Cisco CRM Communications Connector

The Cisco CRM Communications Connector (Cisco CCC) integrates Cisco Unified CME with the Microsoft Business Solution Customer Relationship Management (Microsoft CRM) application. Cisco CCC provides an easy-to-use IP phone application using Microsoft Outlook or Internet Explorer as the PC client software for managing tasks and contacts.

Cisco CCC offers the following application capabilities:

- **Screen pop**—Opens a contact record and creates a new phone call activity record as a call arrives. Creates screen pops from click-to-dial calls and from manually dialed outbound calls.
- **Click-to-dial**—Allows the user to click a field on the PC window and have the PC automatically dial a number. This feature is available from a Microsoft CRM contact record on your desktop.
- **Call duration tracking**—Tracks the duration of a phone call and associates it with the phone activity record.
- **Call information capture**—Captures incoming and outgoing call information, including calling number, called number, and call start and end times.
- **Customer record creation**—Creates a new CRM customer record when a new customer call arrives.

Two pieces of software must be installed to activate the CRM application: one on the Microsoft CRM Server (Cisco CCC server software), and the other on each CRM client PC (Cisco CCC client software). In addition, the Cisco Unified CME TSP driver is installed on each client. The Microsoft CRM Client can use Microsoft Outlook or an HTML interface as the client software.

For information on the CRM Express Solution Specialization, go to the following URL:

http://www.cisco.com/web/partners/pr11/pr66/crm_express/partners_pgm_concept_home.html

For more information on the installation of Cisco CCC, go to Cisco.com, and search for “Cisco CRM Communications Connector for Cisco CallManager Express.”

Extensible Markup Language Applications

XML is a text markup language designed to control web-based documents. With XML, you can create web pages customized for specific application requirements.

This section briefly discusses the XML applications applicable to Cisco Unified CME IP phones. For more information on developing XML applications, go to the following URL:

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

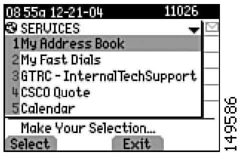
Or visit Cisco.com and search for "Developer Support Central."

General XML Phone Services

XML services on Cisco Unified IP phones give you another way to perform or access more business applications. Some examples of XML-based services on IP phones are user direct-dial directory, announcements, and advertisements.

The IP phones are equipped with a pixel-based display that can display full graphics instead of just text on the window. The pixel-based display capabilities allow you to use sophisticated graphical presentations for applications on Cisco IP phones and make them available at any desktop, counter, or location. In addition, you can select prepackaged applications. A sample phone display with applications is shown in Figure 8-7.

Figure 8-7 XML Application on a Cisco Unified IP Phone Display



Cisco Unified CME XML Phone Services

In a Cisco Unified CME application, XML between an XML server and the IP phones provides customized phone displays and services. The interaction between the IP phone and the XML server includes the following events:

- The IP phone sends an HTTP request to the application server.
- The server renders an XML document and sends it to the IP phone.
- The IP phone parses the XML document and renders the screen graphics on the IP phone display.

You can build applications particular to your business, such as a store inventory or stock quote lookup capability. These applications are especially useful to employees who do not have PCs or do not work at desks. You can also write more general applications, such as displaying a large-numbered clock on the IP phone (that displays when the phone is idle), and use this in conference rooms, lobbies, or break rooms instead of a wall clock.

You can find more information about XML-based IP phone services and productivity applications at the Cisco Applications Central web portal. To get to this site, go to Cisco.com and search for “IP Communications Applications Central.” This site also has application partner information and discussion forums.

XML Application Example

Cisco Unified CME runs standards-based XML scripts developed by any XML developer. This flexibility allows you to customize XML scripts for your specified requirements and enable applications for your particular environment.

The following example shows an XML script that provides a system-wide speed-dial feature on an IP phone. When you press the appropriate keys on the IP phone, the display shows the corresponding directory page of the desired party. You can dial the phone number by simply pressing a predefined button.

```
- <IPPhoneDirectory>
   <Title>XYZ Corp User Speed Dials</Title>
   <Prompt>Record 1 to 6 of 6</Prompt>
 - <DirectoryEntry>
    <Name>Directory Assistance</Name>
    <Telephone>95551212</Telephone>
  </DirectoryEntry>
 - <DirectoryEntry>
    <Name>XYZ Paging</Name>
    <Telephone>918007654321</Telephone>
   </DirectoryEntry>
 - <DirectoryEntry>
    <Name>Alan Anderson</Name>
    <Telephone>2001</Telephone>
   </DirectoryEntry>
 - <DirectoryEntry>
    <Name>Bill Brandy</Name>
    <Telephone>2003</Telephone>
   </DirectoryEntry>
 - <DirectoryEntry>
    <Name>Charles Cramer</Name>
    <Telephone>3214</Telephone>
   </DirectoryEntry>
 - <DirectoryEntry>
    <Name>Donna Davis</Name>
    <Telephone>3721</Telephone>
   </DirectoryEntry>
  </IPPhoneDirectory>
```

Cisco Unified CME Configuration for XML Applications

The XML application interacts directly with the IP phone. You can activate the application in one of three ways:

- By pressing the services button on the phone
- By pressing the directory button on the phone
- By specifying an idle URL that activates when the phone has been idle for a short time

The following shows the **telephony-service url** command you use to configure the URL accessed by each of the three modes of activating an XML application. This URL is resident on your XML server and can be any application or code of your choice.

```
router(config)# telephony-service

router(config-telephony)# url ?

  authentication  authentication url
  directories     directories url
  idle            idle url
  information     information url
  proxy-server    proxy-server url
  services        services url


router# show running-config

telephony-service
 load 7960-7940 P00303020214
...
 ip source-address 10.10.1.100 port 2000
 system message CUE System 2691
 create cnf-files version-stamp 7960 Jul 15 2003 13:48:12
```

You can have a services button, a directory button, and an idle phone application configured at the same time. Cisco Unified CME creates phone loads for the IP phones by using the **create cnf-files** command, shown in the preceding example. This pulls the URLs specified in the **telephony-service url** configuration into the phone load and allows the IP phone to access the correct URL immediately when the appropriate button is pressed on the keypad. If URL settings are changed, you must reset the phones for the changes to become effective.

CHAPTER 9

Cisco Unified CallManager Express Dial Plan

This chapter describes the key elements of your Cisco Unified CallManager Express (Cisco Unified CME) dial plan:

- POTS Dial Peers, page 9-1
- VoIP Dial Peers, page 9-2
- Extensions, page 9-2
- Digit Manipulation Features, page 9-3
- Other Cisco Unified CME Dial Plan Features, page 9-3

Note For additional information, see the "Related Documents and References" section on page xii.

POTS Dial Peers

POTS dial peers are router configuration structures that point calls to a particular voice interface based on whether the dialed number matches certain criteria (as specified in the dial peer's **destination-pattern**). The voice interface can be a PSTN trunk, an analog phone, a fax machine, or an IP phone. The following example shows several sample POTS dial peers, including some for PSTN trunks and one for an analog phone or fax machine.

```
!11-digit long-distance PSTN dialing with an access code of 9
dial-peer voice 1 pots
 preference 1
 destination-pattern 91..........
 port 2/0:23
 forward-digits 11
!
!7-digit local PSTN dialing with an access code of 9
dial-peer voice 4 pots
 destination-pattern 9[2-9]......
 port 2/0:23
 forward-digits 7
!
!Analog phone or fax machine
dial-peer voice 2701 pots
 destination-pattern 2701
 port 2/0/0
```

VoIP Dial Peers

VoIP dial peers are router configuration structures that point calls to a particular IP interface based on the same criteria that are used for POTS dial peers (that is, matching the dialed number to the dial peer's **destination-pattern**). IP interfaces can be H.323 or Session Initiation Protocol (SIP). The following example shows an H.323 dial peer that directs calls to another site where all the extensions start with three.

```
dial-peer voice 3000 voip
 destination-pattern 3...
 session target ipv4:172.19.153.41
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
```

Extensions

You can configure the extensions defined for your IP phones either by using the GUI or directly on the router using the **ephone-dn** command. As covered in Chapter 5, "Cisco Unified CallManager Express Call Transfer and Forward,"an ephone-dn has two components:

- A virtual POTS dial peer for directing calls to the phone
- A virtual voice port

Note The voice ports and dial peers automatically generated by ephone-dns do not appear on the Cisco Unified CME running configuration. They can be seen only using more specific **show** commands.

The following example shows the definition on an ephone-dn and its associated POTS dial peer and voice port.

```
router# show running-config

ephone-dn 1
 number 3001
 description User1
 name User1
 call-forward busy 3105
 call-forward noan 3105 timeout 10
!
router# show telephony-service dial-peer

dial-peer voice 20001 pots
 destination-pattern 3001
 huntstop
 call-forward busy 3105
 call-forward noan 3105
!
router# show telephony-service voice-port

voice-port 50/0/1
 station-id number 3001
 station-id name User1
 timeout ringing 10
 progress_ind setup enable 3
 port 50/0/1
```

Digit Manipulation Features

Having an internal dial plan such as calling from one IP phone to another using a short extension of three or four digits, while also calling the outside world through the PSTN using fully qualified E.164 numbers, requires a certain amount of digit manipulation to add or subtract leading digits to or from an extension.

Typically, you have a *trunk access* code for an IP phone user to specify that a call should be routed to the PSTN as opposed to another extension. This access code must be translated to a PSTN-recognizable number before delivering the call to the PSTN. In a previous example you saw 9 used as the PSTN access code. Because this number matches the dial peer **destination-pattern** explicitly, it is deleted from the digit string forwarded to the PSTN. You can also see **forward-digits** commands in those POTS dial peers. These control how many of the numbers dialed by the IP phone user are forwarded to the PSTN, thereby offering simple digit manipulation within the dial peer statement itself.

Chapter 4, “Voice Gateways,”covered more sophisticated digit manipulation features available in Cisco Unified CME, such as Cisco IOS translation rules.

Other Cisco Unified CME Dial Plan Features

Various other types of DNs or extensions also make up part of your dial plan in the sense that defining these features requires the definition of digits to dial to activate the feature. These features include speed dial, intercom, call park, and paging.

There are also other special types of numbers, such as the AA and voice mail pilot numbers, as well as MWI DNs. The **transfer-pattern** feature also plays a role in your dialing plan, because this definition determines what numbers your IP phone users can transfer calls to.

Class of Restriction (COR) and call blocking are features that determine which numbers might *not* be dialed on the system.

Note Dial plans are a wide topic that extends well beyond the scope of Cisco Unified CME. Visit the Cisco.com website and search for “Cisco Unified CME dial plans” for more information.

Cisco Unified CallManager Express Security Best Practices

Cisco Unified CallManager Express (Cisco Unified CME) provides integrated IP communications on Cisco IOS routers. Therefore, the same security best practices recommended for all Cisco IOS voice-enabled routers also apply to Cisco Unified CME. In addition, you should implement Cisco Unified CME system-specific security practices to provide additional security protection.

This chapter describes how you can set up the Cisco Unified CME using the CLI to prevent users from intentionally or accidentally gaining system-level control from the GUI and local or remote CLI access. Specific sections presented in this chapter address the following Cisco Unified CME security considerations:

- Securing GUI Access, page 10-1
- Using HTTPS for Cisco Unified CME GUI Management, page 10-2
- Configuring Basic Cisco Unified CME Access Security, page 10-3
- Cisco Unified CME Security for IP Telephony, page 10-8
- Cisco Unified CME with NAT and Firewall, page 10-13
- Secure SCCP Signaling via TLS, page 10-19
- Cisco Unified CME Commonly Used Ports, page 10-23

Note For additional information, see the "Related Documents and References" section on page xii.

Securing GUI Access

A Cisco IOS router authenticates an administrator CLI login against the enable password only, and the default setting for HTTP access is **ip http authentication enable**. If the system administrator, customer administrator, or phone user has the same password as the router's enable password, he or she can gain level 15 EXEC privilege access to Cisco IOS software by HTTP. A normal IP phone user can then accidentally change the Cisco Unified CME configuration, erase Flash, or reload the router when logging on to this URL:

http://*cme-ip-address*/

You should configure the following commands for Cisco Unified CME to use AAA or local authentication to prevent a normal user from gaining access to the enable password and therefore having access to the system administrator page:

ip http authentication aaa

or

ip http authentication local

System Administrator Account Authentication via AAA

Cisco Unified CME allows the system administrator username/password be authenticated by AAA. Use the following configuration to use AAA for system administrator user login:

```
ip http authentication
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.1.2.3
```

Note Normal username/password is not authenticated by AAA.

Using HTTPS for Cisco Unified CME GUI Management

HTTP over SSL (HTTPS) provides Secure Socket Layer (SSL) version 3.0 support for the HTTP 1.1 server and HTTP 1.1 client within Cisco IOS software. SSL provides server authentication, encryption, and message integrity to allow secure HTTP communications. SSL also provides HTTP client authentication. This feature is supported only in Cisco IOS software images that include the SSL feature. Specifically, SSL is supported in the Advanced Security, Advanced IP Services, and Advanced Enterprise Services images. Use the Advanced IP Services or Advanced Enterprise Services Cisco IOS images to get both the Cisco Unified CME and SSL features.

IP phones do not serve as HTTPS clients. If HTTPS is enabled on the Cisco Unified CME router, IP phones still attempt to connect to HTTP using port 80. Because the SSL default port is 443, the phones cannot display local directory and system speed dials. IP phones using HTTP can work with a system configured for SSL by enabling both HTTP and HTTPS, as shown in the following example.

```
ip http server
ip http secure-server
ip http secure-port port_number
!if https port is changed from default 443
ip http authentication AAA | TACACS | local
```

Use the following command to generate an RSA usage key pair with a length of 1024 bits or greater:

crypto key generate rsa usage 1024

If you do not generate an RSA usage key pair manually, an RSA usage key pair with a length of 768 bits is generated automatically when you connect to the HTTPS server for the first time. These auto generated RSA keys are not saved to the startup configuration; therefore, they are lost when the device is rebooted unless you save the configuration manually.

You should obtain an X.509 digital certificate with digital signature capabilities for the device from a certification authority (CA). If you do not obtain a digital certificate in advance, the device creates a self-signed digital certificate to authenticate itself.

If you change the device hostname after obtaining a device digital certificate, HTTPS connections to the device *fail* because the hostname does not match the hostname specified in the digital certificate. Obtain a new device digital certificate using the new hostname to fix this problem.

The **ip http secure-server** command prevents clear-text passwords from traveling across the network when a Cisco Unified CME administrator logs into the Cisco Unified CME GUI. However, communications between the phone and router remain in clear text.

The following are the suggested best practices for using HTTP interactive access to the Cisco Unified CME router:

- Use the **ip http access-class** command to allow only specified IP addresses to access the Cisco Unified CME GUI, thus restricting unwanted IP packets from connecting to Cisco Unified CME.
- Use the **ip http authentication** command with a central TACACS+ or RADIUS server for authentication purposes. Configuring authentication for the HTTP and HTTPS servers adds security to communication between clients and the HTTP and HTTPS servers on the device.
- Do not use the router enable password as a Cisco Unified CME login password (to prevent a regular user from gaining administrator privileges).

Configuring Basic Cisco Unified CME Access Security

This section summarizes the measures available to ensure only authorized users and systems can access Cisco Unified CME system-based resources. The following topics are addressed in this section:

- Setting Local and Remote System Access, page 10-3
- Restricting Access to tty, page 10-5
- Configuring SSH Access, page 10-5
- Using ACLs for SNMP Access, page 10-6
- Disabling Cisco Discovery Protocol, page 10-6
- Configuring COR for Incoming and Outgoing Calls, page 10-6
- Restricting Outgoing Calling Patterns, page 10-8

Setting Local and Remote System Access

When in privileged EXEC mode, the **configure terminal** and **telephony-service** commands take a user into Cisco Unified CME configuration mode. The **show running-config** and **show telephony-service** commands show all registered phones and users, extension numbers, usernames, and passwords for Cisco Unified CME GUI access. An initial step to security control is at the system access level. Password encryption, user authentication, and command auditing are all critical to prevent security breaches.

Enabling Secret and Encrypt Passwords

The Enable password is presented in cleartext to provide access control to privileged EXEC mode of the router. Use Enable Secret to encrypt the enable password.

The following example illustrates this configuration:

```
enable secret secretword1
no enable password
```

The **enable secret** command takes precedence over the **enable password** command if both are configured; they cannot be used simultaneously.

To increase security access, passwords can be encrypted to prevent any unauthorized users from viewing the passwords when packets are examined by protocol analyzers:

The following example illustrates this configuration:

```
Service password-encryption
```

Creating Multiple Privilege Levels

By default, Cisco IOS software has two levels of access to commands: User EXEC mode (level 1) and privileged EXEC mode (level 15). Configuring up to 16 privilege levels (from 0, the most restricted level, to 15, the least restricted level) to protect the system from unauthorized access. Use the **privilege** *mode* **level** command.

The following example illustrates this configuration:

```
privilege exec level 14
enable secret level 2 secretword2
```

Restrict Access to VTY

Allow only certain users/locations to Telnet to the router via vty by defining and applying an access list for permitting or denying remote Telnet sessions.

The following example illustrates this configuration:

```
line vty 0 4
 access-class 10 in
 access-list 10 permit 10.1.1.0 0.0.0.255
```

Using AAA to Secure Access

An authentication server can be used to validate user access to the system. The following commands allow an AAA server, TACACS+ server, to be used for authentication services.

The following example illustrates this configuration:

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
ip tacacs source-interface Loopback0
tacacs-server host 10.17.1.2
tacacs-server host 10.17.34.10
tacacs-server key xyz
! Defines the shared encryption key to be xyz
```

Configuring Accounting and Auditing on AAA

The following commands use a TACACS+ server for command accounting and auditing purposes.

```
aaa new-model
aaa authentication login default tacacs+ enable
```

(login uses TACACS+, if not available, use enable password)

```
aaa authentication enable default tacacs+ enable
aaa accounting command 1 start-stop tacacs+
(runs accounting for commands at the specified privilege level 1)
```

```
aaa accounting exec start-stop tacacs+
ip tacacs source-interface Loopback0
tacacs-server host 10.17.1.2
tacacs-server host 10.17.34.10
tacacs-server key xyz (defines the shared encryption key to be xyz)
```

The example command log shows the information contained in a TACACS+ command accounting record for privilege level 1.

```
Wed Jun 25 03:46:47 1997 192.168.25.15 fgeorge tty3 5622329430/4327528 stop
task_id=3 service=shell priv-lvl=1 cmd=show version <cr>
Wed Jun 25 03:46:58 1997 192.168.25.15 fgeorge tty3 5622329430/4327528 stop
task_id=4 service=shell priv-lvl=1 cmd=show interfaces Ethernet 0 <cr>
Wed Jun 25 03:47:03 1997 192.168.25.15 fgeorge tty3 5622329430/4327528 stop
task_id=5 service=shell priv-lvl=1 cmd=show ip route <cr>
```

Configuring Local User Authentication When AAA Is Not Available

You should always require login-based authentication of users—even when the external AAA server is unreachable.

The following example illustrates this configuration:

```
username joe password 7 045802150C2E
username jim password 7 0317B21895FE
!
line vty 0 4
login local
```

Restricting Access to tty

You can allow only certain users and locations to Telnet to the router by using its terminal (tty) or virtual terminal (vty) lines. Define and apply an access list for permitting or denying remote Telnet sessions to your Cisco Unified CME router as shown in the following example.

```
line vty 0 4
 access-class 10 in
 access-list 10 permit 10.1.1.0 0.0.0.255
```

Configuring SSH Access

Use the following command to generate RSA key pairs for the router:

crypto key generate rsa

By default the vty's transport is Telnet. The following command disables Telnet and supports only SSH to the vty lines.

```
line vty 0 4
transport input ssh
```

Using ACLs for SNMP Access

The community access string can be set up to permit access to the Simple Network Management Protocol (SNMP). The following example assigns the *changeme-rw* string to SNMP, allowing read-write access and specifies that IP access list 10 can use the community string:

```
access-list 10 remark SNMP filter
access-list 10 permit 10.1.1.0 0.0.0.255
snmp-server community changeme-rw RW 10
snmp-server community changeme-ro RO 10
```

Because read and write are two common community strings for read and write access, respectively, change the community strings to different ones.

Disabling Cisco Discovery Protocol

Because Cisco Discovery Protocol (CDP) automatically discovers the neighboring network devices supporting CDP, disable CDP in an untrusted domain so that Cisco Unified CME routers will not appear in the CDP table of other devices. Disable CDP with the following command:

no cdp run

If CDP is needed, then consider disabling CDP on a per-interface basis, as in the following example:

```
Interface FastEthernet0/0
no cdp enable
```

Configuring COR for Incoming and Outgoing Calls

One of the ways to restrict unauthorized incoming and outgoing calls is to use the Class or Restriction (COR) commands. The configuration shown in the following example defines two groups of users: *user* and *superuser*. *Superuser* is allowed to make any calls, including local, long-distance, 411 directory lookup, and 911 calls. *User* is restricted from making 900, 411, and international calls.

```
dial-peer cor custom
 name 911
 name 1800
 name local-call
 name ld-call
 name 411
 name int-call
 name 1900
!
dial-peer cor list call911
 member 911
!
dial-peer cor list call1800
 member 1800
!
dial-peer cor list calllocal
 member local-call
!
dial-peer cor list callint
 member int-call
!
dial-peer cor list callld
 member ld-call
```

```
!
dial-peer cor list call411
 member 411
!
dial-peer cor list call1900
 member 1900
!
dial-peer cor list user
 member 911
 member 1800
 member local-call
 member ld-call
!
dial-peer cor list superuser
 member 911
 member 1800
 member local-call
 member ld-call
 member 411
 member int-call
 member 1900
!
dial-peer voice 9 pots
 corlist outgoing callld
 destination-pattern 91..........
 port 1/0
 prefix 1
!
dial-peer voice 911 pots
 corlist outgoing call911
 destination-pattern 9911
 port 1/0
 prefix 911
!
dial-peer voice 11 pots
 corlist outgoing callint
 destination-pattern 9011T
 port 2/0
 prefix 011
!
dial-peer voice 732 pots
 corlist outgoing calllocal
 destination-pattern 9732.......
 port 1/0
 prefix 732
!
dial-peer voice 800 pots
 corlist outgoing call1800
 destination-pattern 91800.......
 port 1/0
 prefix 1800
!
dial-peer voice 802 pots
 corlist outgoing call1800
 destination-pattern 91877.......
 port 1/0
 prefix 1877
!
dial-peer voice 805 pots
 corlist outgoing call1800
 destination-pattern 91888.......
 port 1/0
 prefix 1888
!
```

```
dial-peer voice 411 pots
 corlist outgoing call411
 destination-pattern 9411
 port 1/0
 prefix 411
!
dial-peer voice 806 pots
 corlist outgoing call1800
 destination-pattern 91866.......
 port 1/0
 prefix 1866

ephone-dn  1
 number 2000
 cor incoming user

ephone-dv 2
 number 2001
 cor incoming superuser
```

Restricting Outgoing Calling Patterns

You might use the **after-hours block** command to restrict incoming or outgoing calls after certain hours. You can also use after-hours blocking to restrict calls to numbers or area codes known to be fraudulent calling patterns. The commands shown in the following example block all calls at all times for patterns 2 to 6. Pattern 7 is blocked only during the configured after-hours period.

```
telephony-service
after-hours block pattern 2 .1264 7-24
after-hours block pattern 3 .1268 7-24
after-hours block pattern 4 .1246 7-24
after-hours block pattern 5 .1441 7-24
after-hours block pattern 6 .1284 7-24
after-hours block pattern 7 9011
after-hours day Sun 19:00 07:00
after-hours day Mon 19:00 07:00
after-hours day Tue 19:00 07:00
after-hours day Wed 19:00 07:00
after-hours day Thu 19:00 07:00
after-hours day Fri 19:00 07:00
after-hours day Sat 19:00 07:00
```

Cisco Unified CME Security for IP Telephony

The following topics are addressed in this section:

- IP Phone Registration Control, page 10-9
- Monitoring IP Phone Registration, page 10-10
- Call Activity Monitoring and Call History Logging, page 10-10
- COR for Incoming/Outgoing Calls to Prevent Toll Fraud, page 10-10
- After-hours Blocking to Restrict Outgoing Calling Pattern-Toll Fraud, page 10-12

IP Phone Registration Control

Configure Cisco Unified CME to allow IP phones in the trusted domain for registration. Assuming that the local segment is a trusted domain, use the **strict-match** option in the **ip source-address** command, so that only locally attached IP phones will be able to register to the Cisco Unified CME router and get telephony services.

```
CME-3.0(config-telephony)# ip source-address 10.1.1.1 port 2000 strict-match
```

You can group a set of IP phones into one VLAN (such as 10.1.1.0/24), so that only IP phones in the specified VLAN can register to the Cisco Unified CME.

Block port 2000 access from the WAN side to prevent external SCCP phones from registering with Cisco Unified CME. Use the following **access-list** to block port 2000 access from WAN interfaces. The following example illustrates this configuration:

```
access-list 101 deny tcp any any eq 2000
```

You can also prevent unknown or unconfigured IP phones from being registered by disabling automatic registration using the following command:

```
CME-4.0(config-telephony)# no auto-reg-ephone
```

Note Disabling auto registration also disables the GUI ephone provisioning and Cisco Unified CME SRST Fallback. With Cisco Unified CME 3.x and prior releases, provision ephones before configuring the IP source address in order to workaround auto-registration behavior.

Prior to Cisco Unified CME 4.0, unknown phones or phones that are not configured in Cisco Unified CME are allowed to register with Cisco Unified CME by default for ease of management, but these phones do not provide a dial tone until you configure them by associating the buttons with the ephone-dns or configuring **auto assign** (from **telephony-service** configuration mode).

The following commands illustrates configuring ephone-dns with the **ephone-dn** command.

```
ephone-dn 1
number 1001

ephone-dn 2
number 1002

ephone 1
mac-address 1111.2222.3333
button 1:1 2:2
```

The following commands illustrate configuring the **auto assign** command:

```
CMEtest4-3745(config)# telephony-service
CMEtest4-3745(config-telephony)# auto assign 1 to 500
```

With Cisco Unified CME 4.0, you can configure **no auto-reg-ephone** in **telephony-service** configuration mode so that IP phones that are not explicitly configured with their MAC addresses in ephone configuration mode are prevented from automatically registering with the Cisco Unified CME system.

Monitoring IP Phone Registration

Cisco Unified CME 3.0 added the following syslog messages to generate and display all registration/deregistration events:

```
%IPPHONE-6-REG_ALARM
%IPPHONE-6-REGISTER
%IPPHONE-6-REGISTER_NEW
%IPPHONE-6-UNREGISTER_ABNORMAL
%IPPHONE-6-REGISTER_NORMAL
```

The following message indicates that a phone has registered and is not part of the explicit router configuration (ephone configuration has not been created or the MAC address has not been assigned):

```
%IPPHONE-6-REGISTER_NEW: ephone-3:SEP003094C38724 IP:10.4.170.6 Socket:1 DeviceType:Phone
has registered.
```

Note With Cisco Unified CME 4.0 and later releases, if you have configured the **no auto-reg-ephone** command, then the preceding message is not generated.

Cisco Unified CME allows unconfigured phones to register in order to make provisioning of the Cisco Unified CME system more convenient. By default, phones designated as “new” are not assigned phone lines and cannot make calls.

You can use the following configuration to enable syslogging to a router's buffer/console or a syslog server:

```
logging console | buffered
logging 192.168.153.129
! 192.168.153.129 is the syslog server
```

Call Activity Monitoring and Call History Logging

The Cisco Unified CME GUI provides call history table information so that a network administrator can monitor the call history information for unknown callers and use this information to disallow calling activities based on select calling patterns. The call history log should be configured to perform forensics and accounting and allow the administrator to track down fraudulent calling patterns. Configure the following commands to log call activity and call history:

```
dial-control-mib retain-timer 10080
dial-control-mib max-size 500
!
gw-accounting syslog
```

COR for Incoming/Outgoing Calls to Prevent Toll Fraud

The following configuration example illustrates COR. There are two classes of service in the configuration: user and superuser along with various permissions allowed such as local calling, long distance calling, 911 access, and 411 access. In this example, *superuser* has access to everything and *user* has access to all resources with the exception of toll 1900, directory assistance 411, and international calling.

```
dial-peer cor custom
 name 911
 name 1800
 name local-call
 name ld-call
 name 411
 name int-call
 name 1900

dial-peer cor list call911
 member 911
!
dial-peer cor list call1800
 member 1800
!
dial-peer cor list calllocal
 member local-call
!
dial-peer cor list callint
 member int-call
!
dial-peer cor list callld
 member ld-call
!
dial-peer cor list call411
 member 411
!
dial-peer cor list call1900
 member 1900

dial-peer cor list user
 member 911
 member 1800
 member local-call
 member ld-call
!
dial-peer cor list superuser
 member 911
 member 1800
 member local-call
 member ld-call
 member 411
 member int-call
 member 1900

dial-peer voice 9 pots
 corlist outgoing callld
 destination-pattern 91..........
 port 1/0
 prefix 1
!
dial-peer voice 911 pots
 corlist outgoing call911
 destination-pattern 9911
 port 1/0
 prefix 911
!
dial-peer voice 11 pots
 corlist outgoing callint
 destination-pattern 9011T
 port 2/0
 prefix 011
!
dial-peer voice 732 pots
 corlist outgoing calllocal
 destination-pattern 9732.......
 port 1/0
 prefix 732
!
dial-peer voice 800 pots
 corlist outgoing call1800
 destination-pattern 91800.......
 port 1/0
 prefix 1800
!
dial-peer voice 802 pots
 corlist outgoing call1800
 destination-pattern 91877.......
 port 1/0
 prefix 1877
!
dial-peer voice 805 pots
 corlist outgoing call1800
 destination-pattern 91888.......
 port 1/0
 prefix 1888
!
dial-peer voice 411 pots
 corlist outgoing call411
 destination-pattern 9411
 port 1/0
 prefix 411
!
dial-peer voice 806 pots
 corlist outgoing call1800
 destination-pattern 91866.......
 port 1/0
 prefix 1866

ephone-dn 1
 number 2000
 cor incoming user

Ephone-dn 2
 number 2001
 cor incoming superuser
```

After-hours Blocking to Restrict Outgoing Calling Pattern-Toll Fraud

After-hours blocking can be added to restrict incoming calls after certain hours. After-hours blocking can also be used to restrict calls to numbers/area codes known as fraudulent calling patterns. The following configuration example can be used to restrict calls to certain area codes:

```
telephony-service
 after-hours block pattern 1 .1242
 after-hours block pattern 2 .1264
 after-hours block pattern 3 .1268
 after-hours block pattern 4 .1246
 after-hours block pattern 5 .1441
 after-hours block pattern 6 .1284
 after-hours block pattern 7 .1345
 after-hours block pattern 8 .1767
 after-hours block pattern 9 .1809
 after-hours block pattern 10 .1473
 after-hours block pattern 11 .1876
 after-hours block pattern 12 .1664
 after-hours block pattern 13 .1787
```

```
after-hours block pattern 14 .1869
after-hours block pattern 15 .1758
after-hours block pattern 16 .1900
after-hours block pattern 17 .1976
after-hours block pattern 18 .1868
after-hours block pattern 19 .1649
after-hours block pattern 20 .1340
after-hours block pattern 21 .1784
after-hours block pattern 22 .1684
after-hours block pattern 23 .1590
after-hours block pattern 24 .1456
after-hours day Sun 00:00 23:59
after-hours day Mon 00:00 23:59
after-hours day Tue 00:00 23:59
after-hours day Wed 00:00 23:59
after-hours day Thu 00:00 23:59
after-hours day Fri 00:00 23:59
after-hours day Sat 00:00 23:59
```

Cisco Unified CME with NAT and Firewall

The following topics are addressed in this section:

- Cisco Unified CME with NAT, page 10-13
- Remote Phones with Public IP Addresses, page 10-14
- Remote Phones with Private IP Addresses, page 10-14
- Remote Phones over VPN, page 10-15
- Cisco Unified CME with Cisco IOS Firewall Implementation Considerations, page 10-16

Cisco Unified CME with NAT

Typically, Cisco Unified CME router's LAN interface (Ethernet interface) is used as a source IP address used by the IP phones and the Cisco Unified CME router to communicate with each other. However, when an internal switch module is used to connect IP phones, the VLAN's IP address can be used as a source IP address. A loopback interface's IP address is another option for a source IP address.

The IP addresses of the IP phones are internal addresses to the Cisco Unified CME router and are in a different segment that is not visible by the external devices or callers. Other devices including Cisco gateways or gatekeeper use the Cisco Unified CME router's IP address to communicate instead of directly communicating with the IP phones. The Cisco Unified CME router translates IP addresses back and forth for the traffic to route to the IP phones or outside of the network area. Therefore, no NAT configuration is needed for two-way voice/audio from/to the IP phones locally attached to the Cisco Unified CME router. We recommend that NAT be deployed for data traffic only with Cisco Unified CME.

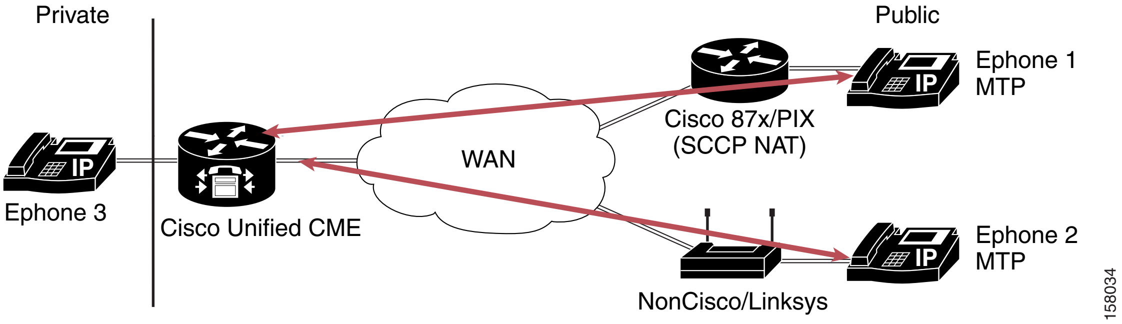
NAT may be required for IP phones deployed remotely which do not have routable IP addresses.

Note Cisco Unified CME IP address used as the source IP address needs to be routable and may be a loopback IP address in all the scenarios described in this section. Also, the UDP/TCP ports must be open between remote IP phones and Cisco Unified CME source address.

Remote Phones with Public IP Addresses

Remote phone support introduced in Cisco Unified CME 4.0 allows IP phones to be connected to Cisco Unified CME across a WAN link such as Frame Relay, DSL, and cable. Figure 10-1 shows a typical scenario for this connectivity arrangement.

Figure 10-1 Remote Phones with Public IP Addresses



In the scenario in Figure 10-1, *ephone 3* is in a private VLAN and uses Cisco Unified CME to reach *ephone 1* and *ephone 2* in remote sites with public IP addresses. However, because media streams are sent between the phones connected to the same Cisco Unified CME, Media Termination Point (MTP) should be configured on the remote phones in order to have Cisco Unified CME terminate the media stream—thereby ensuring two-way audio between *ephone 3* and *ephone 1* or *ephone 2*. Codec G729r8 is required for the remote phones. The configuration on *ephone 1* or *ephone 2* is as follows:

```
ephone 1
 mtp
 codec g729r8
```

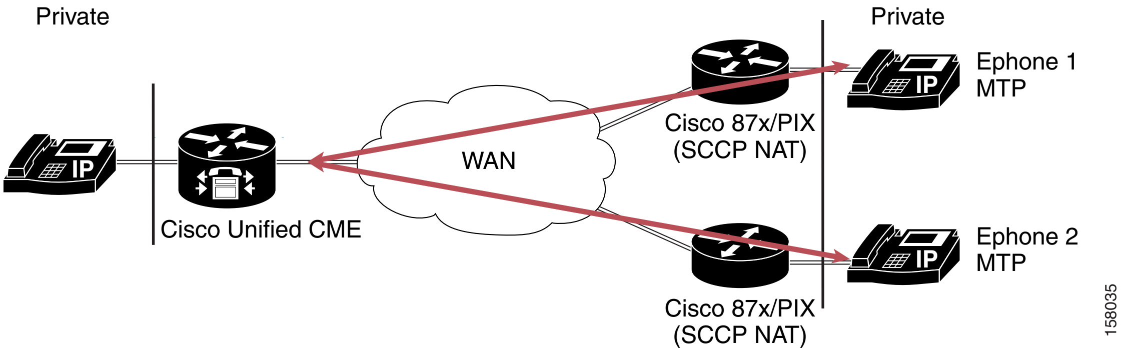
The *MTP* option under *ephone 1* causes the Cisco Unified CME router to act as a proxy. The Cisco Unified CME forwards media packets to other IP phones with the Cisco Unified CME router's address in the source address field. If another phones in the call is not an IP phone, Cisco Unified CME forwards the media packets.

Note If all phones have public IP addresses, then MTP configuration is not required and media will flow between phones (rather than through the Cisco Unified CME). Unless MTP is required for your implementation, we recommend that you do not use it. As in the prior scenario, the UDP/TCP ports must be open between remote IP phones and the Cisco Unified CME source address.

Remote Phones with Private IP Addresses

Figure 10-2 illustrates a typical scenario when remote phones are deployed with private IP addresses in the remote site.

Figure 10-2 Remote Phone Connection with Private IP Addresses



Remote phones can be connected via a traditional Cisco router (such as Cisco 87x or Cisco PIX) or using an alternative routing device (such as Linksys router). Both implementation require that NAT be configured if routable IP addresses are not used on the remote phones. NAT SCCP support is required to implement two-way audio between IP phones connected to the Cisco Unified CME. With NAT allowing for the translation of the embedded IP addresses and port numbers presented in the SCCP messages, a full NAT entry can be created to allow RTP traffic to flow between IP Phones. As a result, two-way voice/audio is permitted between the IP phones being connected via NAT. For a device such as Linksys router, which is not SCCP aware, a one-way audio issue exists between the two IP phone endpoints. A workaround is to connect the remote IP phone attached to the Linksys via a DMZ port with routable IP addresses or to establish a VPN connection to the Cisco Unified CME router to avoid having a one-way audio issue.

Caveats:

- NAT SCCP support is available in Cisco IOS Release 12.3(11)T and later in Cisco IOS routers.
- MTP is required to be configured on the remote phones.
- Remote phones attached through a Cisco router with SCCP NAT support also require the configuration of MTP in order to support two-way audio.
- Remote phones attached to a nonCisco SCCP NAT router will encounter a one-way audio issue even if MTP is configured on the remote phones. A workaround is to use VPN between Cisco Unified CME and the a nonCisco SCCP NAT router or obtain public IP addresses for the remote phones.

Note As in the prior examples, the UDP/TCP ports must be open between remote IP phones and Cisco Unified CME source address.

Remote Phones over VPN

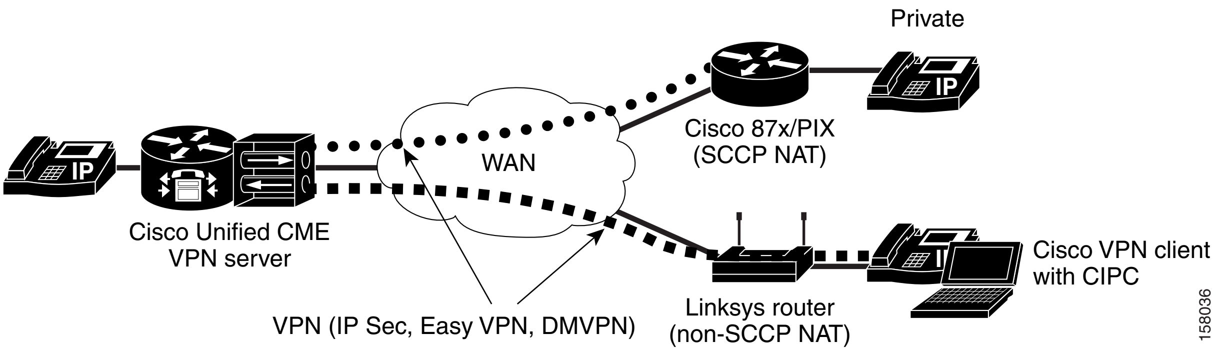
Remote phones with private IP addresses can be connected to phones attached to a Cisco Unified CME using a nonCisco router. However, in order to support two-way audio between these privately addressed remote phones and phones attached to a Cisco Unified CME (which have public IP addresses), a VPN IP Sec tunnel must be established between Cisco Unified CME and the nonCisco router.

VPN can also be used to connect Cisco Unified CME and Cisco SCCP NAT aware routers such as Cisco 87x/PIX, allowing for connections supported by QoS and VPN acceleration.

Figure 10-3 illustrates examples of these VPN-related environments.

Note As in the prior examples, the UDP/TCP ports must be open between remote IP phones and Cisco Unified CME source address.

Figure 10-3 Remote Phone Connection using VPN



Cisco Unified CME with Cisco IOS Firewall Implementation Considerations

This description of the Cisco Unified CME implementation with Cisco IOS firewall addresses the following topics:

- Overview of Cisco IOS Firewall with Cisco Unified CME, page 10-16
- Previous Problems on Cisco Unified CME with Cisco IOS Firewall, page 10-17
- Cisco Unified CME and Cisco IOS Firewall on the Same Router, page 10-18
- Other Alternatives for Ensuring Cisco Unified CME Security, page 10-19

Overview of Cisco IOS Firewall with Cisco Unified CME

The Cisco IOS Firewall, running on Cisco IOS routers, provides a network-based firewall solution with the functionality of Context-based Access Control (CBAC) or protocol inspection, Cisco Intrusion Detection System (Cisco IDS), authentication proxy, and URL filtering. A firewall provides access control between internal and external networks. It identifies networks as inside (private) or outside (public) in which packets can get from the inside to the outside, be blocked by default from outside to inside, and packets associated with an inside-originated connection are allowed to pass in. Many firewalls work only if all outside traffic originates from well-known sockets and do not handle asymmetric traffic (such as UDP media). Cisco IOS firewalls allow packets to pass through based on source and destination IP addresses and the configured firewall policy.

Cisco Unified CME is a software feature added to the Cisco IOS routers that provides call processing for IP phones using Skinny Client Control Protocol (SCCP) for branch/SMB, and managed SP environments. There can be instances of SMB or branch office implementations in which a single router is required to provide Internet access, IP telephony service, and Cisco IOS Firewall functions. Cisco Unified CME requires that all IP phones be attached to the Cisco Unified CME router locally —before remote phone support was introduced.

Therefore, H.323 and SCCP support on the Cisco IOS Firewall are needed for locally generated traffic.

Previous Problems on Cisco Unified CME with Cisco IOS Firewall

SCCP is a Cisco proprietary small version of H.323. H.323 traffic can be classified into call signalling, call control, and media communication. H.323 uses Q.931, H.225, and H.245 to set up, manage/control, and tear down calls. The following descriptions address how signaling and media streams are affected by the Cisco IOS firewall.

Signaling Stream

An H.323 call requires a TCP connection for H.245 signalling that does not have an associated well-known port. The H.245 port is dynamically assigned. Because this port is not known ahead of time and cannot be configured when defining firewall policy, the Cisco IOS Firewall will block the H.245 message and the call signalling procedure will fail. When NAT is used in the H.323 signalling path, an inside IP address (which is behind the NAT and is not known to the rest of the world), will be used as the “calling party” information element in the H.225 signalling stream. As a result, an incoming call (attempts to make an H.225 connection back to that address) will fail.

Media Streams (RTP streams)

RTP streams run on top of UDP and do not have any fixed ports associated with them. Each type of media stream has one or more channels with dynamically assigned source, destination, and port numbers, which are not known ahead of time and cannot be preconfigured in the firewall policy. For the media stream to traverse the firewall, the firewall must open many UDP ports with source and destination pairs for each call session. This can open vulnerabilities to the network behind the firewall.

Because the Cisco IOS Firewall does not allow outside traffic to transverse to the inside destinations, VoIP calls (inbound calls) will fail. Furthermore, dynamic RTP/RTCP ports used by the endpoints are not automatically opened and allowed without modification of the security policy. The problems are summarized as follows:

- The firewall only looks at Layer 3 addresses.
- VoIP signalling protocols embed IP addresses at Layer 4 and above
  - RTP/RTCP works at Layer 5.
  - By default, firewalls do not allow outside to inside traffic.
  - Cisco IOS firewall feature set and NAT and PIX have application functionality called the Application Layer Gateway (ALG), or fixup, protocol which helps resolve these issues.
- The VoIP application is composed of a dynamic set of protocols.
  - SIP, MGCP, H.323, and SCCP for signalling
  - SDP, H.225, and H.245 for capability exchange
  - RTP/RTCP for control and audio media
  - RTP/RTCP both use a dynamic port for the audio media ranging from 16384 to 32767 for all Cisco products

Note The Cisco IOS Firewall did not previously support Skinny inspection, because outgoing packets are converted to H323 or SIP. As a result, there is no need for Skinny inspection. However, ACLs can be used to filter out unwanted packets/traffic as a way to support incoming Skinny packet inspection. Cisco IOS Firewall has added H.323 inspection support for any locally generated traffic, thus making it possible to deploy Cisco Unified CME and IOS Firewall on the same router.

Cisco Unified CME and Cisco IOS Firewall on the Same Router

As long as Cisco IOS Firewall is not applied to the interfaces that have voice traffic (signaling and media) coming in, Cisco Unified CME and Cisco IOS Firewall can co-exist on the same router. The inspection of router-generated traffic, available in Cisco Release IOS 12.3(14) T and later, enhances Cisco IOS Firewall functionality to inspect TCP, UDP, and H.323 connections that have a router or firewall as one of the connection endpoints. Inspection of TCP and UDP channels initiated from the router enables dynamic opening of pinholes on the interface access control list (ACL) to allow return traffic. Inspection of local H.323 connections enables the deployment of Cisco Unified CME and Cisco IOS Firewall on the same router. This also simplifies ACL configuration on Cisco Unified CME interface through which H.323 connections are made. Before this feature, multiple ACLs were required to allow all dynamically negotiated data and media channels—in addition to ACLs required to allow H.323 connections on a standard port such as 1720. With this feature, you configure the ACLs to allow H.323 control channels on port 1720. The Cisco IOS Firewall inspects all the traffic on the control channel and opens pinholes to allow dynamically negotiated data and media channels.

The following procedure illustrates ACL configuration to support this capability:

Step 1 Create the ACL. In this example, TCP traffic from subnet 10.168.11.1, 192.168.11.50, and 192.168.100.1 is permitted.

```
access-list 120 permit tcp host 10.168.11.1 any eq 1720
access-list 121 permit tcp host 192.168.11.50 host 10.168.11.1 eq 1720
access-list 121 permit tcp host 192.168.100.1 host 10.168.11.1 eq 1720
```

Step 2 Create the Cisco IOS Firewall inspection rule LOCAL-H323. This allows for the inspection of the protocol traffic specified by the rule. This inspection rule sets the timeout value to 180 seconds for each protocol (except for RPC). The timeout value defines the maximum time that a connection for a given protocol can remain active without any traffic passing through the router. When these timeouts are reached, the dynamic ACLs that are inserted to permit the returning traffic are removed, and subsequent packets (possibly even valid ones) are not permitted.

```
ip inspect name LOCAL-H323 tftp timeout 180
ip inspect name LOCAL-H323 h323 router-traffic timeout 180
```

Step 3 Apply the inspection rule and ACL. In this example, the inspection rule LOCAL-H323 is applied to traffic at interface Serial0/3/0:

```
interface Serial0/3/0
 ip address 10.168.11.2 255.255.255.0
 ip access-group 121 in
 ip access-group 120 out
 ip inspect LOCAL-H323 in
 ip inspect LOCAL-H323 out
 encapsulation frame-relay
frame-relay map ip 10.168.11.1 168 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
```

Step 4 The Cisco IOS Firewall supports only version 2 of the H.323 protocol. Configure the following in the Cisco Unified CME to support only version 2 features:

```
voice service voip
h323
session transport tcp calls-per-connection 1
h245 tunnel disable
h245 caps mode restricted
h225 timeout tcp call-idle value 0
```

Other Alternatives for Ensuring Cisco Unified CME Security

The following are four alternative solutions that you can use to provide security to the Cisco Unified CME users:

- Run Cisco IOS Firewall on a different router—it is not required to be on the same Cisco Unified CME.
- Set up a maximum number of connections in the Cisco Unified CME. This is available with the regular H.323 implementation in Cisco IOS software and can help control the maximum number of H.323 (H225 setup Inbound + Outbound) calls that will be processed (such as `dial-peer voice 10 voip; max-conn 5` limits calls to five connections).
- Set up ACLs to accept H.225 connections only from the gatekeeper (GK) if the GK in the network is using routed signaling.
- Use H.235 security to authenticate the callers and provide additional call security

Secure SCCP Signaling via TLS

Cisco Unified CME 4.0 introduced in Cisco IOS Release 12.4(4)XC provides phone authentication and secure SCCP signalling with Transport Layer Security (TLS).

Phone authentication is a security infrastructure for providing secure SCCP between Cisco Unified CME and IP phones. Phone authentication addresses the following security needs:

- Establishing the identity of each endpoint in the system
- Authenticating devices
- Providing signaling-session privacy
- Providing protection for configuration files

Note Secure RTP is not supported in Cisco Unified CME 4.0.

The secure phone authentication feature is supported in the following two Cisco IOS feature sets:

- Advanced IP Services (such as c3725-advipservicesk9-mz.124-4.XC.bin)
- Advanced Enterprise Services (c3725-adventerprisek9-mz.124-4.XC.bin)

Supported phones are Cisco Unified IP Phone 7911G, Cisco Unified IP Phone 7941G, Cisco 7961G, and Cisco Unified IP Phone7970/71G-GE.

Key considerations for secure SCCP signaling via TLS are as follows:

- Certificate Trust List (CTL) client is used to create the CTL file and makes it available in the TFTP directory The CTL file (CTLfile.tlv) contains the public key information of all the servers with which the IP phone will interact.
- A digitally signed configuration file (SEP<MAC-addr>.cnf.xml.sgh) is created by the telephony-service module in Cisco IOS software. The router’s private key is used for signing this document.
- Certificate Authority Proxy Function (CAPF)—a proxy between the IP phone and the Certification Authority (CA)—is used to request for a certificate on behalf of the phone. It is through the CAPF protocol that the CAPF server gets all the required information from the phone (including the public key and phone ID). CAPF configuration status resides in the CNF file.

- Phone authentication occurs between the Cisco Unified CME and a supported device when each entity accepts the certificate of the other entity, and when a secure connection between the entities occurs. Phone authentication relies on the creation of a CTL file.
- File authentication validates digitally signed files that a phone downloads from a TFTP server: config files, ringist files, and locale and CTL files. When receiving these types of the files, the phone validates the file signatures to verify that file tampering did not occur after the files were created.
- Signaling authentication, also known as signaling integrity, uses the TLS protocol to validate that signaling packets have not been tampered with during transmission. Signaling authentication relies on the creation of the CTL file.

Use the following procedure to configure support for SCCP signaling using TLS:

Step 1 Configure NTP or manually set the software clock using the **clock set** command as in the following example:

```
clock timezone PST -8
clock summer-time PDT recurring
ntp clock-period 17247042
ntp server 171.68.10.80
ntp server 171.68.10.150
```

Step 2 Configure a Cisco IOS Certification Authority (CA) —The CA issues certificates to Cisco Unified CME, CAPF, TFTP, and SAST server functions:

The CA can be on the same Cisco Unified CME router or on an external router. The following example illustrates configuring a CA on the same Cisco Unified CME router:

```
crypto pki server laverda-ca
 grant auto
 database url flash:
!
crypto pki trustpoint laverda-ca
 enrollment url http://192.168.1.1:80
 revocation-check crl
 rsakeypair laverda-ca
```

Step 3 Certificate provisioning for Cisco Unified CME functions: *capf server*, *cme server*, *tftp server*, *sast1*, and *sast2* as illustrated in the following configuration examples.

a. Obtain a certificate for *capf server*:

```
!configuring a trust point
 crypto pki trustpoint capf-server
 enrollment url http://192.168.1.1:80
 revocation-check none
!authenticate w/ the CA and download its certificate
crypto pki authenticate capf-server
! enroll with the CA and obtain this trustpoint's certificate
 crypto pki enrollment capf-server
```

b. Obtain a certificate for *cme server*:

```
crypto pki trustpoint cme-server
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate cme-server
crypto pki enrollment cme-server
```

c. Obtain a certificate for the *tftp server*:

```
crypto pki trustpoint tftp-server
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate tftp-server
crypto pki enrollment tftp-server
```

d. Obtaining a certificate for *sast1*:

```
crypto pki trustpoint sast1
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate sast1
crypto pki enrollment sast1
```

e. Obtaining a certificate for *sast2*:

```
crypto pki trustpoint sast2
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate sast2
crypto pki enrollment sast2
```

Step 4 Configure Telephony Service with the following steps:

a. Configure the trustpoint label used for secure signaling:

```
secure-signaling trustpoint cme-server
```

b. Configure the TFTP server credentials (trustpoint) used for signing the configuration files:

```
tftp-server-credentials trustpoint tftp-server
```

c. Configure the security mode for the endpoints

```
 server-security-mode secure
 device-security-mode authenticated
```

The *authenticated* option will instruct the device to establish a TLS connection with no encryption. In this mode, there is no SRTP in the media path.

The *encrypted* option will instruct the device to establish a encrypted TLS connection to secure Media path using SRTP.

Note Use the *authenticated* option until SRTP is supported in the future.

d. Configure the system to generate the phone configuration XML files for each endpoint:

```
cnf-file perphone
```

e. Configure any ephone. For example:

```
ephone 1
 device-security-mode authenticated
```

Step 5 Configure the CTL client on a local Cisco Unified Cisco Unified CME in order to create a CTL file containing a list of known, trusted certificates and tokens.

The CTL client can either be run on the same Cisco Unified CME router or another standalone router. Here is an example for a CTL client on a local Cisco Unified CME router:

```
ctl-client
 server capf 192.168.1.1 trustpoint capf-server
 server tftp 192.168.1.1 trustpoint tftp-server
 server cme 192.168.1.1 trustpoint cme-server
 sast1 trustpoint sast1
 sast2 trustpoint sast2
```

After you have configured all the info above, use the **regenerate** command to create the CTL file:

regenerate

Step 6 Configure the CAPF server:

```
capf-server
 port 3804
 auth-mode null-string
 cert-enroll-trustpoint laverda-ca password 1 1511021F07257A767B
 trustpoint-label capf-server
 source-addr 192.168.1.1
!
```

Troubleshooting and Debugging

Use the following commands for troubleshooting and debugging your secure SCCP signaling via TLS setup:

- **show ephone registered**
- **show ctl-client**
- **show capf-server sessions**
- **show capf-server auth-strings**
- **show capf-server summary**
- **debug ctl-client**
- **debug credentials**
- **debug capf-server all|messages|error|events**

Note For details about these diagnostic commands, see your specific Cisco Unified CallManager Express command reference. The following is an example:

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_command_reference_book09186a00805b6c70.html

Cisco Unified CME Commonly Used Ports

Table 10-1 and Table 10-2 illustrate Cisco Unified CME commonly used ports.

Table 10-1 Commonly Used Ports for Voice on Cisco Unified CME

Protocol	Port	Usage
SCCP	TCP 2000	Call control for SCCP phones
SIP	TCP 5060	Call control for SIP endpoints
RTP	UDP 16384-32767	Media from Cisco Unified CME to H.323/SIP endpoint, including Cisco Unity Express
RTP	UDP 2000	Media from Cisco Unified CME to SCCP phone
H.225	TCP 1720	H.323 Call Setup
H.245	TCP 11000-65535	H.323 Call control, port assignment random
H.323 RAS	UDP 1718	GK Discovery
H.323 RAS	UDP 1719	GK Call Control
H.323 RAS	UDP 223.0.1.4	GK Multicast discovery
TLS	TCP 3804	CAPF Authentication Request
TLS	TCP 2443	Secure Call control for SCCP phones

Table 10-2 Commonly Used Ports for Data on Cisco Unified CME

Protocol	Port	Usage
DHCP	UDP 67	IP addressing for IP phones
HTTP	TCP 80	Cisco Unified CME GUI access, IP phone local directory access
HTTPS/SSL	TCP 443	Secure Cisco Unified CME GUI access
NTP	UDP 123	Time sync for Cisco Unity Express, IP Phones
Radius	UDP 1645	Authentication for Cisco Unified CME CLI/GUI users
Radius	UDP 1646	CDR accounting
SNMP	UDP 161	Traps for Cisco Unified CME monitoring
SSH	TCP 22	Secure Cisco Unified CME CLI access
Syslog	UDP 514	System monitoring, CDR accounting
Telnet	TCP 23	Cisco Unified CME CLI access

CHAPTER 11

Managing and Monitoring Cisco Unified CallManager Express Systems

This chapter addresses managing and monitoring Cisco Unified CallManager Express (Cisco Unified CME). The following specific sections describe utilities available for monitoring and management Cisco Unified CME:

- Configuring and Monitoring via Network Management Systems Using the Cisco Unified CME AXL/SOAP Interface, page 11-1
- Monitoring Cisco Unified CME, page 11-4
- Managing Cisco Unified CME Systems, page 11-10

Note For additional information, see the "Related Documents and References" section on page xii.

Configuring and Monitoring via Network Management Systems Using the Cisco Unified CME AXL/SOAP Interface

You can integrate Cisco Unified CME with network management applications by using the Cisco Unified CME XML Layer (AXL) application programming interface (API). The AXL API provides a mechanism for inserting, retrieving, updating, and removing data from the Cisco Unified CallManager database using an XML SOAP interface. The AXL API allows programmatic access to Cisco Unified CallManager data in XML form instead of using a binary library or a Dynamic Link Library (DLL). The AXL API methods, or requests, are performed using a combination of HTTP and SOAP. The HTTP payload is encapsulated in SOAP, which is essentially an XML remote procedure call protocol. User requests send XML data to the Cisco Unified CallManager server, which returns an AXL response encapsulated in a SOAP message.

Cisco Unified CME extends the AXL/SOAP capabilities by providing XML APIs for monitoring and configuring IP phones and extensions. A Network Management System (NMS) might use the Cisco Unified CME AXL/SOAP APIs to poll the Cisco Unified CME network elements (NEs), including IP phones and extensions. As with the AXL protocol, communication between an NMS and Cisco Unified CME is based on an HTTP data exchange and can be initiated only by polling from the NMS. However, Cisco Unified CME can enable or disable the sending of data, and also control the polling interval.

Note AXL/SOAP APIs for NMS configuration and monitoring are supported only by Cisco Unified CME, not by Cisco Unity Express.

The next sections describe the features supported by the Cisco Unified CME AXL/SOAP APIs and a test procedure to check if your Cisco Unified CME is set up properly to respond to the AXL/SOAP queries.

Cisco Unified CME 4.0 XML Interface Enhancements

The following updates to the Cisco Unified CME XML interface were adopted with Cisco Unified CME 4.0:

- CME4.0 XML runs on top of IXI engine to replace the previous backend processing of AXL requests for better scalability; parser and transport layers are separated from the application itself.

  Note For backward compatibility, the old interface can still be used by configuring with the old CLIs.

- Cisco Unified CME XML support for configuration and monitoring
  - Monitoring requests—XML message payload is in the format of XML text-monitoring
  - Configuration requests—XML message payload is in the format of CLI list to be saved on a router as CLI commands

  Note The supported functionality of the XML interface remains unchanged.

- The IXI CLI is used to configure the XML interface

The Cisco Unified CME AXL/SOAP Interface

The Cisco Unified CME AXL/SOAP APIs provide many capabilities for monitoring and configuring IP phones and extensions.

For monitoring, Cisco Unified CME AXL/SOAP APIs support the following:

- Getting static information
  - ISgetGlobal—Gets global information
  - ISgetDevice—Gets device information
  - ISgetExtension—Gets extension information
- Getting dynamic information
  - ISgetEvtCounts—Gets the number of events recorded in the buffer
  - ISgetDevEvts—Gets device events if IP phones are in the register, unregister, or decease state
  - ISgetExtEvts—Gets extension events (the virtual voice port is up or down)
- Setting information (configuring) and executing CLI
  - ISsetKeyPhones—Sets the “key” phone

  - ISexecCLI—Executes the CLI

The following are supported CLI commands that can be executed by the ISexecCLI API. You might execute all the subcommands under each of these configuration mode commands with the ISexecCLI API.

- **telephony-service**
- **ephone**
- **ephone-dn**
- **vm-integration**
- **ephone-hunt**
- **dial-peer voice**

Note CME AXL/SOAP APIs were first used by NetIQ's Vivinet Manager or AppManager for VoIP management solutions.

Testing the Cisco Unified CME AXL/SOAP Interface

You might use the test page (xml-test.html) that is available with the Cisco Unified CME GUI files to verify that the Cisco Unified CME router is set up correctly to respond to AXL/SOAP requests. The following are the steps to set up and run the test page:

Step 1 Load xml-test.html into Flash.

Step 2 Configure the following on the Cisco Unified CME router:

```
Router(config)# ip http server
Router(config)# ip http path:flash
Router(config)# telephony-service mode
Router(config)# log password abcd
Router(config)# xmltest
```

Step 3 Enter the following URL in the browser:

http://*ip-address of router*/ISApi/AXL/V1/soapisapi.is

Step 4 When the Login window opens, log on as follows:

Username: **any non-empty string**

Password: **abcd**

Step 5 In the test page, input content into the form. The XML request is written to the form at the bottom. Go to the bottom of the page and click **Submit**.

Step 6 Try the preceding steps on your system. If you receive any errors, the following debugs on the router might help:

```
Router# debug ip http appinout
Router# debug ip http appdetail
```

The xml-test.html file is a test program for you to check that the Cisco Unified CME router can respond to AXL/SOAP requests. You must disable the test program when polling from an NMS using the Cisco Unified CME AXL APIs with the following configuration:

Router(config)# **telephony-service**

Router(config-telephony)# **no xmltest**

Note A polling request from an NMS must be sent in clear-text format.

Note For more information about Cisco Unified CME XML provisioning, see this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_programming_reference_guide09186a00801c5fab.html

For developer services support, go to the Cisco Developer Support site at http://www.cisco.com/cgi-bin/dev_support/access_level/product_support. You must be a Cisco.com registered user to access this site.

Cisco Unified CME 4.0 XML Configuration Example

The following is an example Cisco Unified CME 4.0 XML configuration:

```
ip http server
! Enables http server

ixi transport http
 no shutdown
! Assigns http as the transport method of IXI

ixi application cme
 no shutdown
! Enables IXI's CME application

telephony-service
 xml user admin password cisco 15
! Configures privilege for CME XML interface
```

Use the following debug command to troubleshoot Cisco Unified CME XML configurations:

debug cme-xml

Monitoring Cisco Unified CME

You might monitor the Cisco Unified CME system with syslog messages and Simple Network Management Protocol (SNMP) Management Information Base (MIB). You also can monitor call activity information through syslog messages and call detail records (CDR).

Monitoring IP Phones Using Cisco Unified CME Syslog Messages

Cisco Unified CME 3.0 introduced type 6 syslog messages, as shown in the following example, for IP phone registration and deregistration events. These syslog messages are useful for a central NMS to manage Cisco Unified CME systems and IP phones.

```
%IPPHONE-6-REG_ALARM
%IPPHONE-6-REGISTER
%IPPHONE-6-REGISTER_NEW
%IPPHONE-6-UNREGISTER_ABNORMAL
%IPPHONE-6-REGISTER_NORMAL

Example Message:
 %IPPHONE-6-REGISTER_NEW: ephone-3:SEP003094C38724 IP:1.4.170.6 Socket:1
  DeviceType:Phone has registered.
```

The IPPHONE-6-REGISTER_NEW message shown in preceding configuration example indicates that a phone has registered and that it is not part of the explicit router configuration. However, the ephone configuration has not yet been created. Cisco Unified CME allows unconfigured phones to register to make provisioning of the Cisco Unified CME system more convenient. By default, phones designated as new are not assigned phone lines; therefore, they cannot make calls until they are configured into the system.

Enable the Cisco IOS logging capability to log all the syslog events into the buffer on the Cisco Unified CME router, or send the syslog messages to a syslog server for offline management, as shown in the following example.

```
Telephony-service#(config)# service timestamps log datetime msec localtime
Telephony-service #(config)# aaa new-model
Telephony-service #(config)# aaa authentication login default none
Telephony-service #(config)# aaa accounting connection H.323 start-stop radius
Telephony-service #(config)# gw-accounting syslog
Telephony-service #(config)# logging 10.10.10.1
!!! 10.10.10.1 is the ip address of syslog server, multiple servers might also be
  specified
```

To synchronize your Cisco Unified CME system to an external NTP server, use the following:

```
ntp server ip-address
 !!! ip address - IP address of the time server providing the clock
  synchronization
```

If there is no external NTP time source, use the internal router clock as the time source:

ntp master

To ensure that the time stamps are correct, set the router clock to the correct time:

clock set 15:15:00 might 31 2001

You can specify multiple syslog servers for redundancy, because syslog uses UDP as the underlying transport mechanism and data packets are unsequenced and unacknowledged.

In addition to the syslog messages from Cisco Unified CME, you can also set up Cisco Unity Express for logging to an external syslog server in addition to logging a message locally to its own storage. Use the following command:

```
CUE(config)# log server 10.10.10.1
```

Monitoring Call Activity

NMS systems can retrieve CDRs and call history information in any of the following ways:

- Cisco Unified CME GUI
- Syslog or RADIUS servers
- SNMP CISCO-DIAL-CONTROL-MIB and CISCO-VOICE-DIAL-CONTROL-MIB
- Voice performance statistics from Cisco Unified CME

The next sections describe how you can monitor call activities, CDR logs, billing records, and voice performance statistics in more detail.

Monitoring Cisco Unified CME Call History

The Cisco Unified CME GUI provides call history information in the **Reports** > **Call History** window so that a network administrator can monitor for unknown callers or disallowed calling activities based on calling patterns. Configure the call history log to perform any forensics and accounting to track down fraudulent calling patterns, as shown in the following example.

```
dial-control-mib retain-timer 10080
dial-control-mib max-size 500
!
gw-accounting syslog
logging 10.10.10.1
```

Logging CDR to External Servers

You might follow the same method discussed earlier in the "Monitoring IP Phones Using Cisco Unified CME Syslog Messages" section on page 11-5 to allow syslog messages to be logged to an external server and to log CDRs to an external server. Cisco Unified CME allows you to log CDRs for accounting or billing purposes to an external AAA server (RADIUS or TACACS). This provides CDR logging, post call record processing, and a billing report generation facility. You can use a MindCTI (http://www.mindcti.com/) RADIUS server or a Cisco Secure Access Control Server (Cisco Secure ACS) to provide billing support and view CDR details.

To configure RADIUS on your Cisco Unified CME router, perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. You must configure AAA if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use the **line** and **interface** commands to allow the defined method lists to be used.

The following example is a sample configuration that allows the Cisco Unified CME router to generate and send VoIP CDRs to an external RADIUS server.

```
aaa new-model
aaa authentication login default group radius
!! Login Authentication using RADIUS server
aaa authorization config-commands
aaa authorization exec default if-authenticated group radius
aaa authorization network default group radius
!! Authorization for network resources
aaa authorization configuration default group radius
!! Authorization for global config mode
```

```
aaa accounting send stop-record authentication failure
!! Start-Stop Accounting services
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!! For local Authentication
aaa accounting connection default start-stop group radius
!! For local Authentication
aaa accounting connection h323 start-stop group radius
!! For Voice Call Accounting
aaa accounting system default start-stop group radius
aaa accounting resource default start-stop group radius
aaa session-id common
!
gw-accounting h323
!!  H.323 gateway Accounting
gw-accounting syslog
!! Optional - for system log information
gw-accounting voip
!! VoIP call Accounting
!
Router RADIUS Server configuration:
radius-server host 11.11.11.1 auth-port 1645 acct-port 1646
!! RADIUS Server host address
radius-server retransmit 30
!!  RADIUS messages update interval
radius-server key cisco
!! RADIUS server secure key
```

Using Account Codes for Billing

Cisco Unified CME provides account code support into CDRs, which a RADIUS server or customer billing server then can use for the billing process. The Cisco Unified IP Phone 7960 and Cisco Unified IP Phone 7940 both support an account softkey so that users can enter an account code from an IP phone during the call ringing (alerting) or active (connected) states. This account code is also added to the Cisco-VOICE-DIAL-CONTROL-MIB SNMP MIB.

You can view the Account Code field in the **show call active voice** log, as shown in Example 14-41.

```
Router# show call active voice
Telephony call-legs: 2
SIP call-legs: 0
H.323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 2
!
GENERIC:
SetupTime=97147870 ms
Index=1
PeerAddress=2001
!
TELE:
AccountCode 1234
```

Monitoring Voice Performance Statistics

If you are running Cisco IOS release 12.3(4)T or later, you can take advantage of the Cisco Voice Performance Statistics to collect voice call signaling statistics and VoIP AAA accounting statistics based on user-configured time ranges. The statistics can be displayed on your console or can be formatted and archived to an FTP or syslog server. This feature can help you diagnose performance problems on the network, and identify impaired voice equipment.

The following example shows an example of the amount of memory used for accounting and signaling call statistics records (CSR) by fixed interval and following a reset or reboot. It also shows the estimated memory allocated for future use.

```
Router# show voice statistics memory-usage csr
*** Voice Call Statistics Record Memory Usage ***
        Fixed Interval Option -
                CSR size: 136 bytes
                Number of CSR per interval: 9
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 10
        Since Reset Option -
                CSR size: 136 bytes
                Total count of CSR: 9
                Used memory size (proximate): 1224

*** Voice Call Statistics Accounting Record Memory Usage ***
        Fixed Interval Option -
                ACCT REC size: 80 bytes
                Number of ACCT REC per interval: 1
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 25
        Since Reset Option -
                ACCT REC size: 80 bytes
                Total count of ACCT REC: 1
                Used memory size (proximate): 80
```

Using Cisco Unified CME Supported SNMP MIBs

You might leverage Cisco SNMP router MIBs for Cisco Unified CME management. The following are examples of supported MIBs:

- **CISCO-DIAL-CONTROL-MIB**—Contains information for CDRs and call history
- **CISCO-VOICE-DIAL-CONTROL-MIB**—Extends call detail information to telephony and VoIP dial peers/call legs
- **CISCO-VOICE-IF-MIB**—Allows access to voice interface parameters such as loss and gain values and echo cancellation status
- **CISCO-CDP-MIB**—Lets you manage CDP
- **CISCO-SYSLOG-MIB**—Allows access to syslog messages
- **CISCO-CCME-MIB**—Provides IP phone registration status, fault monitoring parameters and trap notifications.

For more information about Cisco Unified CME MIB support, see the following URLs:

- *Cisco CallManager Express 3.4 SNMP MIB Support*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_mib_quick_reference_book09186a008056b4ec.html

- *CISCO-CCME-MIB Overview*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_mib_quick_reference_chapter09186a00805567ba.html#wp1192528

Note **CISCO-CCME-MIB** is supported by the Cisco Unified Operations Manager to provide fault monitoring.

Managing Cisco Unified CME Systems

This section addresses management of Cisco Unified CME systems in the following separate sections:

- Cisco Unified CME Management Overview, page 11-10
- Managing a Standalone Cisco Unified CME System, page 11-10
- Cisco Zero Touch Deployment, page 11-11
- Managing Multisite Cisco Unified CME Networks, page 11-13
- Managing Cisco Unified CME Systems with Cisco Network Management Tools, page 11-13
- Managing Cisco Unified CME Systems with Cisco Partner Applications, page 11-15

Cisco Unified CME Management Overview

Service providers (SP) normally deploy Cisco Unified CME systems as one of the following:

- Standalone, single-site managed services
- Large-scale, multisite managed services

A managed-services solution with Cisco Unified CME offers two opportunities for value-added services:

- The customer premises equipment (CPE) router
- Network management support

SPs offer their customers the Cisco Unified CME systems at the end customer's site. They also install, set up, maintain, and manage the systems.

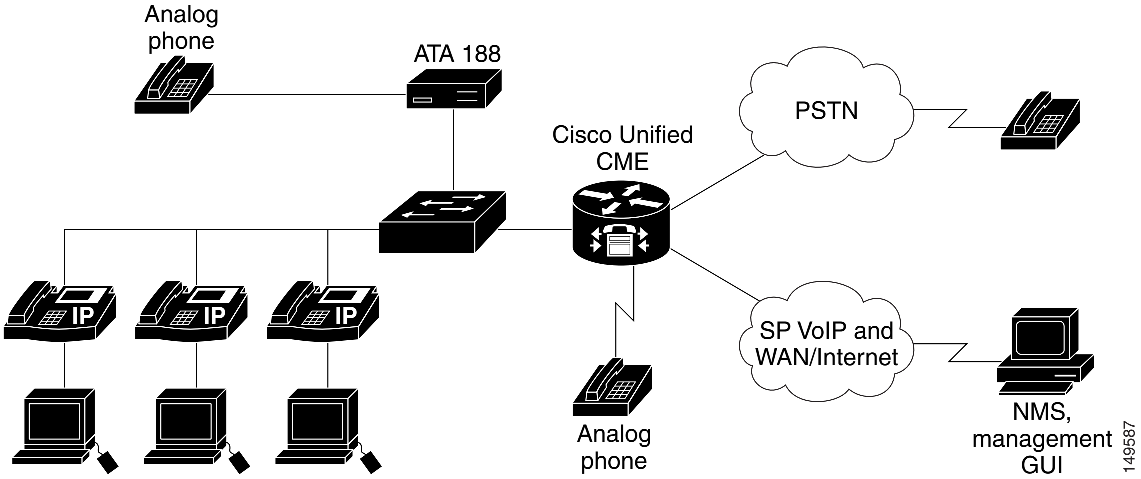
Most of the network management systems (NMS) used by SPs to deploy Cisco Unified CME in a managed-services model also apply to enterprise networks. The difference between a managed-services model and an enterprise model is who offers, owns, and manages the core network.

Note Note that this section covers only management capabilities for Cisco Unified CME systems, not for the larger IP telephony solutions and products offered by Cisco in general. The next sections describe how you can manage standalone or multisite Cisco Unified CME systems. They also cover some general information on the typical Cisco Voice Network Management Solutions that are applicable to Cisco Unified CME.

Managing a Standalone Cisco Unified CME System

Figure 11-1 shows a deployment in which a single Cisco Unified CME system in a branch office connects to a SP VoIP network. All voice and data traffic can be routed over the SP network, or calls can be routed by the PSTN if the destination (called party) cannot be reached via the SP IP network.

Figure 11-1 Managing a Standalone Cisco Unified CME System



To manage a standalone Cisco Unified CME system, we recommend that you provision or configure the system by using the Cisco Unified CME Quick Configuration Tool (QCT) 3.0 to setup your system with basic functionality. You can, as option, use the CLI, the Cisco Unified CME setup utility, or the Cisco Unified CME GUI. This is sufficient for simple moves, adds, changes to the phones, and basic configuration changes for a standalone or single-site deployment. However, you might also use the Zero Touch deployment, monitoring, accounting, and billing management capabilities for multisite Cisco Unified CME deployments.

Cisco Zero Touch Deployment

Cisco Networking Services technology provides the infrastructure for automated configuration of large numbers of network devices. Based on Cisco Networking Services event and configuration agents, it eliminates the need for an on-site technician to initialize the devices. The Cisco Networking Services Zero Touch feature provides a deployment solution in which the router contacts a Cisco Networking Services Configuration Engine to retrieve its full configuration automatically. This capability is made possible through a single generic bootstrap configuration file common across all SP end customers subscribing to the services. Within the Cisco Networking Services framework, customers can create this generic bootstrap configuration without device-specific or network-specific information, such as interface type or line type.

Understanding Cisco Zero Touch Deployment Components

Cisco Zero Touch deployment consists of the following three components:

- Cisco Networking Services Configuration Express, page 11-11
- Cisco Networking Services Configuration Engine, page 11-12
- Cisco Networking Services Configuration Engine, page 11-12

Cisco Networking Services Configuration Express

Cisco Configuration Express is an online ordering system and customizable inline manufacturing process that lets SPs easily deploy customer premises equipment (CPE)-based managed services to their small-to-medium sized business and enterprise customers. When ordering Cisco products, SPs use Cisco

Configuration Express to specify the shipping instructions, including the Cisco IOS software version and a bootstrap configuration, which are configured, tested, and shipped with the CPE. The resulting fully configured CPE is shipped either directly to the end customer site or to the SP warehouse.

The bootstrap configuration integrates with Cisco Networking Services Configuration Engine the moment the CPE devices are plugged into the network at the end-customer site.

Cisco Networking Services Configuration Engine

Cisco Networking Services Configuration Engine runs on the Cisco Networking Services 2100 series Intelligence Engine (Cisco Networking Services IE 2100) hardware platform as well as customer UNIX servers. It is a secure and scalable deployment and configuration management application that provides an intelligent network interface to applications and users supporting up to 5000 Cisco CPE devices.

Cisco Networking Services Configuration Engine includes the Configuration Service and Configuration Server. The Configuration Server communicates with the Cisco Networking Services Configuration Agent running on the managed Cisco Unified CME via HTTP and transfers data in XML format parsed by the Cisco Networking Services Configuration Agent on the Cisco Unified CME router using its own parser.

The Cisco Networking Services Configuration Service delivers device and service configurations to Cisco IOS devices for initial configuration and mass reconfiguration by logical groups. Routers receive their initial configuration from the Cisco Networking Services Configuration Service when they start up on the network the first time. The Cisco Networking Services Configuration Service uses the Cisco Networking Services Event Service to send and receive events required to apply configuration changes and to send success and failure notifications.

The templates created on the Cisco Networking Services Configuration Engine are automatically pushed to the CPE devices running the bootstrap configuration.

For more information on Cisco Networking Services Configuration Engine, see the following URL:
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

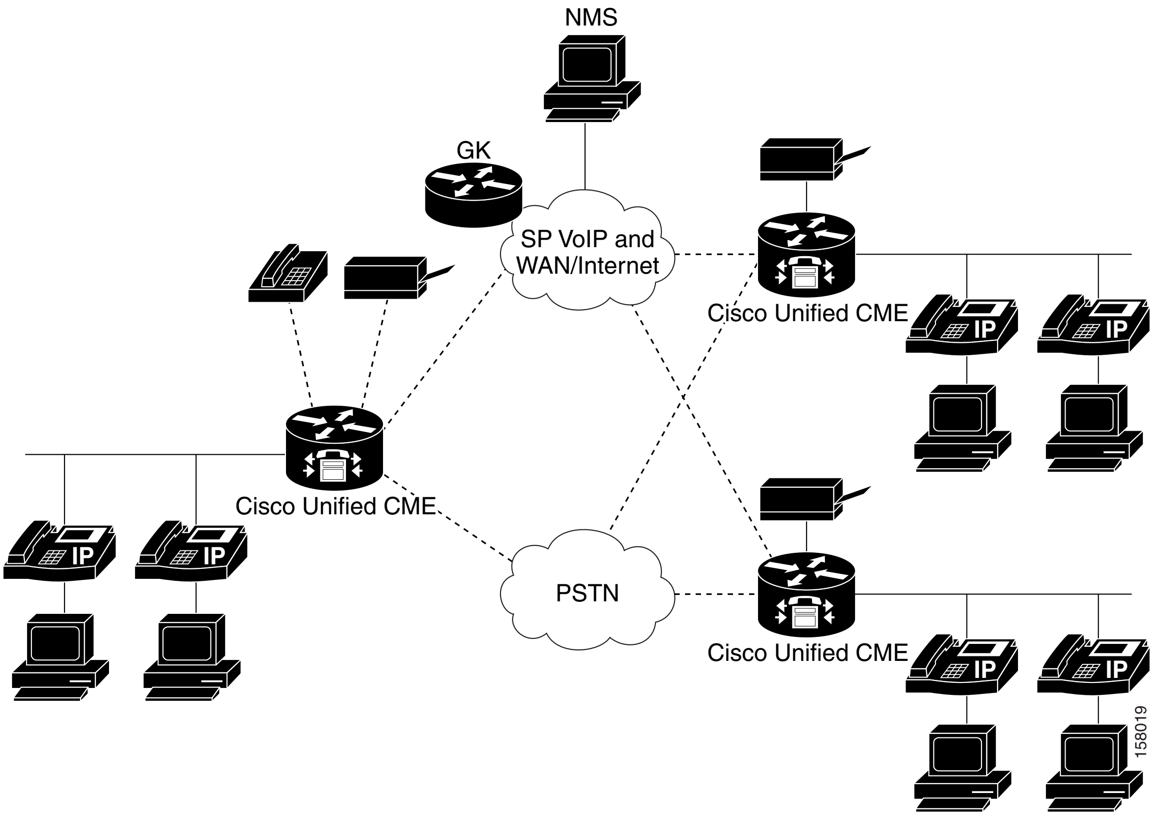
Cisco Networking Services Agent

The Cisco Networking Services Agent is built into Cisco IOS devices to provide intelligence to connect to the Cisco Networking Services Configuration Engine. Using its bootstrap configuration, the CPE device, such as Cisco Unified CME, polls the network and provides inventory to the Cisco Networking Services Configuration Engine.

Managing Multisite Cisco Unified CME Networks

You can also deploy Cisco Unified CME in large-scale enterprise networks or in managed-services networks. Figure 11-2 shows multiple small and medium business or enterprise branch office Cisco Unified CME sites connected to the SP VoIP network.

Figure 11-2 Managing a Multisite Cisco Unified CME Network



When deploying Cisco Unified CME systems in a multisite environment, provisioning, configuring, and managing only one Cisco Unified CME system at a time is insufficient.

Managing Cisco Unified CME Systems with Cisco Network Management Tools

The following sections summarize the Cisco tools that we recommends for managing your Cisco Unified CME systems:

- Cisco Unified CME Quick Configuration Tool, page 11-13
- Cisco Unified Operations Manager and Cisco Unified Service Monitor, page 11-14

Cisco Unified CME Quick Configuration Tool

We recommend using the Cisco Unified CME Quick Configuration Tool (QCT) to install and initialize Cisco Unified CME. For information about the Cisco Unified CME QCT, see the following URLs:

- *Cisco Unified CME QCT Data Sheet*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_data_sheet0900aecd802e9be9.html
- *Configuring Your System Using Cisco IPC Express Quick Configuration Tool*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_guide_chapter09186a0080527133.html

Use the following link to download the Cisco Unified CME QCT software:

- http://www.cisco.com/pcgi-bin/tablebuild.pl/cme-qct

Cisco Unified Operations Manager and Cisco Unified Service Monitor

We recommend using the Cisco Unified Operations Manager and Cisco Unified Service Monitor to manage and monitor Cisco Unified CME systems.

Cisco Unified Operations Manager

The Cisco Unified Operations Manager is a separate software application that does not use any agents on any Cisco Unified Communications device or application. It resides on a separate server and uses standards-based access mechanisms, such as SNMP polling, HTTP polling, trap processing, and other diagnostic tests to ascertain the current operational status of the Cisco Unified Communications deployment and makes that information available via either the Cisco Unified Operations Manager user interfaces or other interfaces such as syslogs, SNMP traps or emails.

Cisco Unified Operations Manager provides fault monitoring and management of Cisco Unified CME with the following capabilities:

- Cisco Unified CME in Service Level Views
- Real-time alerts on Cisco Unified CME hardware and software status
- Real-time service quality alerts on calls supported by Cisco Unified CME
- Discovery of Cisco Unified CME and the inventory details,
- Version, maximum number of ephones, extensions, and conference calls
- Current status (Cisco Unified CME enabled/disabled)
- Phone details (phone status and status changes)
- Phone utilization (percentage of ephones registered, key ePhones registered)
- Synthetic tests (phone registration, dial-tone, and end-to-end call)
- SNMP traps processed

You can use Cisco Unified Service Monitor in conjunction with Cisco Unified Operation Manager, by configuring Cisco Unified Operations Manager as a trap receiver for Cisco Unified Service Monitor. Cisco Unified Operations Manager can generate events for Service Monitor traps, display the events on the *Service Quality Alerts* dashboard, and store event history for up to 31 days.

For more information, see the following URLs:

- Cisco Unified Operations Manager data sheets:
  http://www.cisco.com/en/US/products/ps6535/products_data_sheets_list.html
- Technical documentation for Cisco Unified Operations Manager:
  http://www.cisco.com/en/US/products/ps6535/tsd_products_support_series_home.html

Cisco Unified Service Monitor

Cisco Unified Service Monitor analyzes data that it receives from Cisco 1040 Sensors (Cisco 1040s) installed in your voice network. Each licensed instance of Cisco Unified Service Monitor acts as a primary Cisco Unified Service Monitor for multiple Cisco 1040s. A Cisco Unified Service Monitor can also be configured to act as a secondary and tertiary Cisco Unified Service Monitor for Cisco 1040s that are managed by other licensed instances of Cisco Unified Service Monitor. When a Cisco Unified Service Monitor becomes unavailable, Cisco 1040s fail over to secondary or tertiary Cisco Unified Service Monitors temporarily until the primary Cisco Unified Service Monitor becomes available again.

Cisco Unified Service Monitor examines the data it receives from Cisco 1040s, comparing Mean Opinion Scores (MOS)—computed by Cisco 1040s for each RTP stream—against a user-specified threshold value. When MOS drops below the threshold, Service Monitor generates SNMP traps and sends them to up to four trap receivers. Optionally, Service Monitor stores the call metrics it receives from Cisco 1040s to disk files.

Cisco Unified Service Monitor provides real-time measurement of voice quality and mean opinion score (MOS) reporting to provide the following capabilities:

- Unified dashboard to monitor the whole system and to rapidly troubleshoot problems
- Real-time view of Cisco Unified Communications System
- Alerting and diagnostics
- Phone and device inventory reports (phone status and phone tracking)

For more information, see the following URLs:

- Cisco Unified Service Monitor data sheets:
  http://www.cisco.com/en/US/products/ps6536/products_data_sheets_list.html
- Technical documentation for Cisco Unified Service Monitor:
  http://www.cisco.com/en/US/products/ps6536/tsd_products_support_series_home.html

Managing Cisco Unified CME Systems with Cisco Partner Applications

In addition to the Cisco management solutions discussed in the previous sections, various Cisco partners offer management solutions. This section describes these solutions:

- NetIQ Vivinet Manager, page 11-15
- Stonevoice, page 11-21
- ISI Telemanagement Solutions Inc. Infortel Select, page 11-28
- Integrated Research Prognosis, page 11-29

NetIQ Vivinet Manager

NetIQ's Vivinet Manager allows you to gain access to Cisco Unified CME data, and then analyze and manage Cisco Unified CME systems. With NetIQ Vivinet Manager for Cisco Unified CME, you gain easy access to a new set of tools you can leverage to gather a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

NetIQ Vivinet Manager for Cisco Unified CME is an add-on module to NetIQ Vivinet Manager version 2.1. Equipped with Cisco Unified CME AXL/SOAP API support, you can use Knowledge Scripts included in Vivinet Manager for Cisco Unified CME to create jobs that monitor the health, availability, and performance of key devices. These scripts allow you to monitor and manage crucial device properties at a depth unparalleled by any other solution. You can configure each Knowledge Script to send an alert, collect data for reporting, and perform automated problem management when an event occurs.

The Vivinet Manager Knowledge Scripts let you monitor phone status (registered, unregistered, and deceased), reset IP phones, specify key phones, monitor for duplicate extensions, and show inventory information for phones attached to Cisco Unified CME systems. The following are the supported Knowledge Scripts for the Cisco Unified CME module:

- **CiscoCME_Device_Reset**—Resets Cisco Unified CME IP phones for reasons such as troubleshooting or picking up new default firmware. Use this script in conjunction with CiscoCME_Device_Status to ensure that the selected phones have upgraded successfully.
- **CiscoCME_Device_Status**—Monitors the status of key Cisco Unified CME phones.
- **CiscoCME_Extension_Check**—Monitors for duplicate phone extension numbers. This script looks for all phones configured in Cisco Unified CME, regardless of whether they are registered.
- **CiscoCME_Phone_Inventory**—Generates an inventory of the phone details for phones that are attached to Cisco Unified CME.
- **CiscoCME_Set_Key_Phones**—Designates one or more "key" phones. After you designate key phones, you can choose to monitor only key phones.

The following features are provided by NetIQ Vivinet Manager for Cisco Unified CME:

- It discovers Cisco Unified CME systems with Cisco Unified CME version and device information.
- It provides Knowledge Scripts for day-to-day and diagnostic monitoring.
- It monitors Cisco Unified CME resources, including CPU, memory, flash memory, power supplies, and temperature sensors.
- It supports Cisco Unified CME 3.0 and later.
- It monitors and reports scripts in the Network Device module in addition to the scripts created especially for the Cisco Unified CME module.

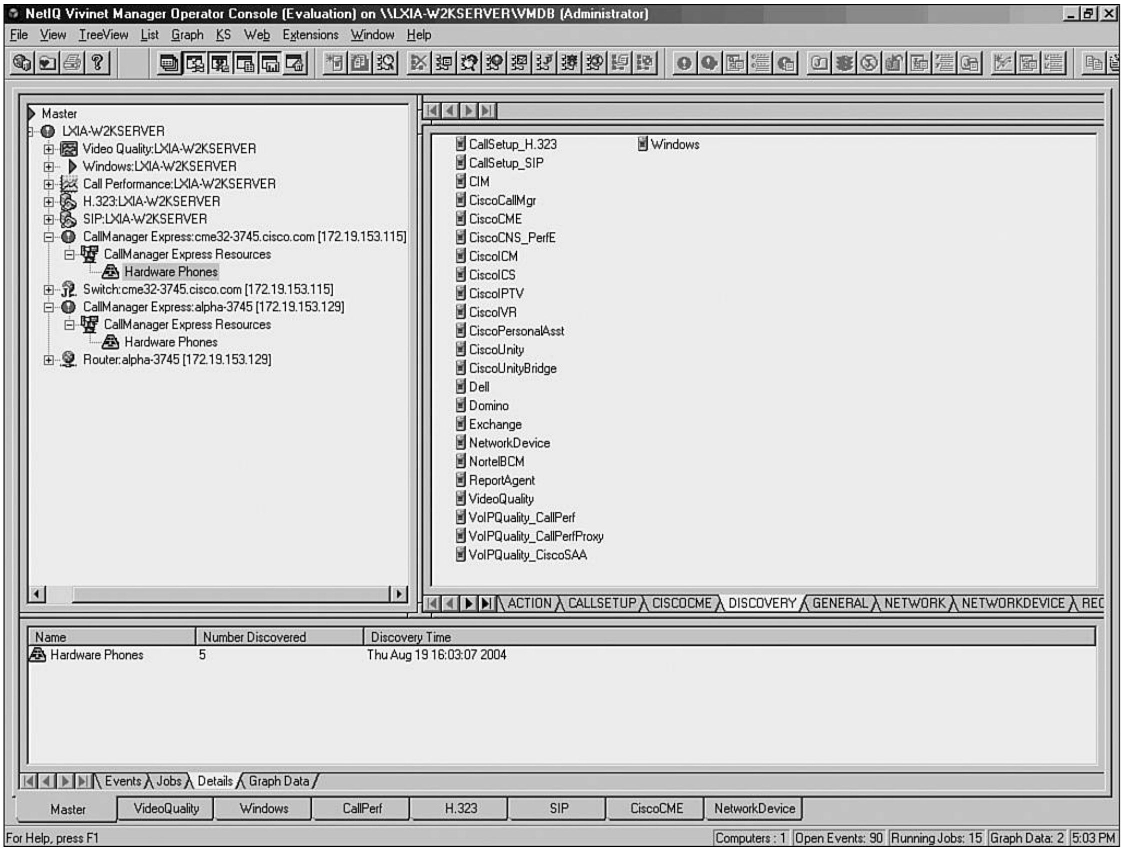
NetIQ for Cisco Unified CME is an add-on module to the NetIQ Vivinet Manager. Get the installation CD-ROM from NetIQ (http:/www.netiq.com/products/vm/) for Cisco Unified CME, and install it to the NetIQ Vivinet Manager.

The following example shows the required configuration on a Cisco Unified CME system.

```
snmp-server community public RO
! Set up the community string
!
telephony-service
   log password abcd
   no xmltest
   ! doesn't show when "no xmltest" is configured
   no xmlschema
   ! doesn't show when "no xmlschema" is configured
```

Figure 11-3 shows the operator console of NetIQ Vivinet Manager for Cisco Unified CME.

Figure 11-3 *NetIQ Vivinet Manager Operator Console for Cisco Unified CME*


NetIQ Vivinet Manager Operator Console (Evaluation) on \\LXIA-W2KSERVER\VMDB (Administrator)
File View TreeView List Graph KS Web Extensions Window Help
ACTION CALLSETUP CISCOCME DISCOVERY GENERAL NETWORK NETWORKDEVICE REC
Events Jobs Details Graph Data
Master VideoQuality Windows CallPerf H.323 SIP CiscoCME NetworkDevice
For Help, press F1
Computers : 1 Open Events: 90 Running Jobs: 15 Graph Data: 2 5:03 PM
149548

Master
- LXIA-W2KSERVER
  - Video Quality:LXIA-W2KSERVER
  - Windows:LXIA-W2KSERVER
  - Call Performance:LXIA-W2KSERVER
  - H.323:LXIA-W2KSERVER
  - SIP:LXIA-W2KSERVER
  - CallManager Express:cme32-3745.cisco.com [172.19.153.115]
    - CallManager Express Resources
      - Hardware Phones
  - Switch:cme32-3745.cisco.com [172.19.153.115]
  - CallManager Express:alpha-3745 [172.19.153.129]
    - CallManager Express Resources
      - Hardware Phones
  - Router:alpha-3745 [172.19.153.129]

CallSetup_H.323
CallSetup_SIP
CIM
CiscoCallMgr
CiscoCME
CiscoCNS_PerfE
CiscoICM
CiscoICS
CiscoIPTV
CiscoIVR
CiscoPersonalAsst
CiscoUnity
CiscoUnityBridge
Dell
Domino
Exchange
NetworkDevice
NortelBCM
ReportAgent
VideoQuality
VoIPQuality_CallPerf
VoIPQuality_CallPerfProxy
VoIPQuality_CiscoSAA
Windows

Name	Number Discovered	Discovery Time
Hardware Phones	5	Thu Aug 19 16:03:07 2004

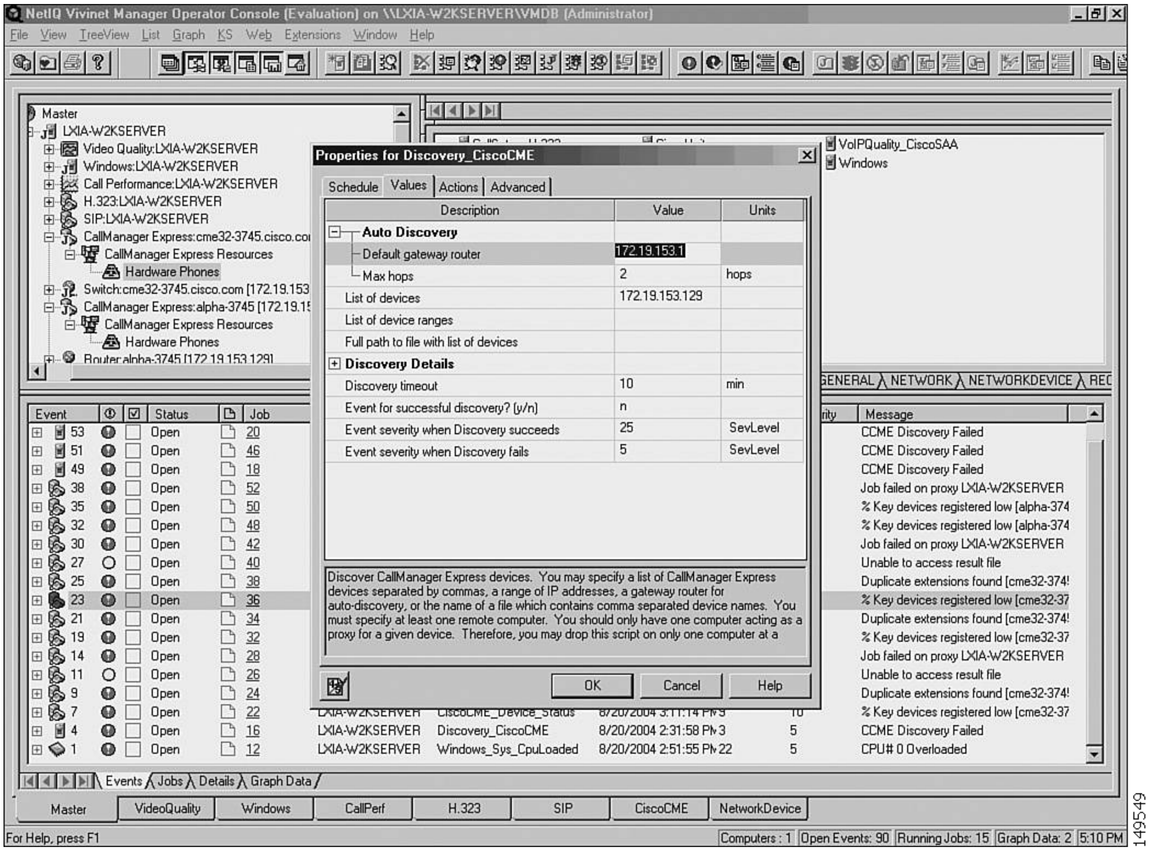
The following sections provide some highlights of how you can use the NetIQ Vivinet Manager for Cisco Unified CME.

Discovery of Cisco Unified CME

You might use the Discovery script (Discovery_CiscoCME) found on the Discovery tab of the Knowledge Script pane to discover the Cisco Unified CME managed object on a device in the TreeView pane of the Operator Console.

From the Discovery tab of the Knowledge Script pane, drag and drop the Discovery_CiscoCME script onto a proxy computer in the TreeView pane. Set the Values tab parameters, as shown in Figure 11-4.

Figure 11-4 Discovery Property


NetIQ Vivinet Manager Operator Console (Evaluation) on \\LXIA-W2KSERVER\VMDB (Administrator)
File View TreeView List Graph KS Web Extensions Window Help
Master
LXIA-W2KSERVER
Video Quality:LXIA-W2KSERVER
Windows:LXIA-W2KSERVER
Call Performance:LXIA-W2KSERVER
H.323:LXIA-W2KSERVER
SIP:LXIA-W2KSERVER
CallManager Express:cme32-3745.cisco.co
CallManager Express Resources
Hardware Phones
Switch:cme32-3745.cisco.com [172.19.153
CallManager Express:alpha-3745 [172.19.1
CallManager Express Resources
Hardware Phones
Router:alpha-3745 [172.19.153.129]
VoIPQuality_CiscoSAA
Windows
GENERAL NETWORK NETWORKDEVICE REC
Properties for Discovery_CiscoCME
Schedule Values Actions Advanced
OK Cancel Help
Events Jobs Details Graph Data
Master VideoQuality Windows CallPerf H.323 SIP CiscoCME NetworkDevice
For Help, press F1
Computers : 1 Open Events: 90 Running Jobs: 15 Graph Data: 2 5:10 PM
149549

Description	Value	Units
Auto Discovery		
Default gateway router	172.19.153.1	
Max hops	2	hops
List of devices	172.19.153.129	
List of device ranges		
Full path to file with list of devices		
Discovery Details		
Discovery timeout	10	min
Event for successful discovery? (y/n)	n	
Event severity when Discovery succeeds	25	SevLevel
Event severity when Discovery fails	5	SevLevel

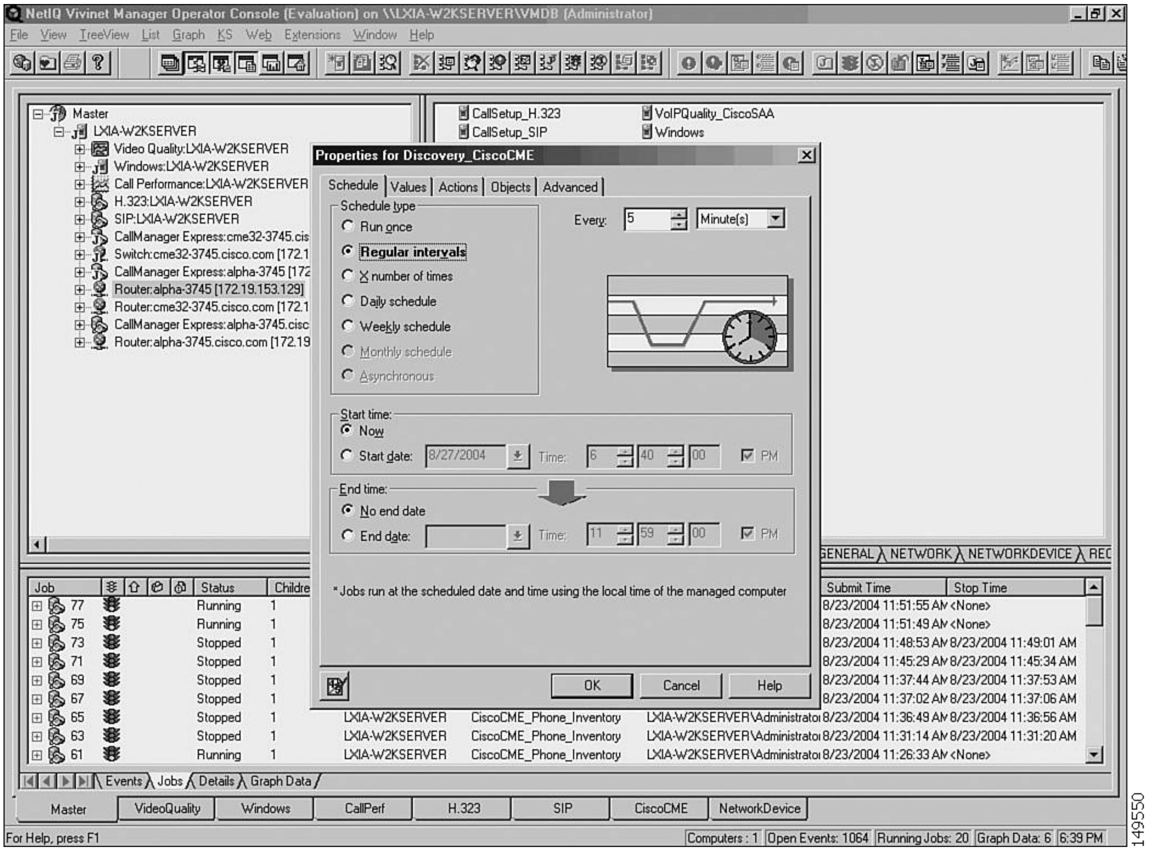
Discover CallManager Express devices. You may specify a list of CallManager Express devices separated by commas, a range of IP addresses, a gateway router for auto-discovery, or the name of a file which contains comma separated device names. You must specify at least one remote computer. You should only have one computer acting as a proxy for a given device. Therefore, you may drop this script on only one computer at a

Event	Status	Job	Message
53	Open	20	CCME Discovery Failed
51	Open	46	CCME Discovery Failed
49	Open	18	CCME Discovery Failed
38	Open	52	Job failed on proxy LXIA-W2KSERVER
35	Open	50	% Key devices registered low [alpha-374
32	Open	48	% Key devices registered low [alpha-374
30	Open	42	Job failed on proxy LXIA-W2KSERVER
27	Open	40	Unable to access result file
25	Open	38	Duplicate extensions found [cme32-374!
23	Open	36	% Key devices registered low [cme32-37
21	Open	34	Duplicate extensions found [cme32-374!
19	Open	32	% Key devices registered low [cme32-37
14	Open	28	Job failed on proxy LXIA-W2KSERVER
11	Open	26	Unable to access result file
9	Open	24	Duplicate extensions found [cme32-374!
7	Open	22	% Key devices registered low [cme32-37
4	Open	16	CCME Discovery Failed
1	Open	12	CPU# 0 Overloaded

LXIA-W2KSERVER CiscoCME_Device_Status 8/20/2004 3:11:14 PM 9 10
LXIA-W2KSERVER Discovery_CiscoCME 8/20/2004 2:31:58 PM 3 5
LXIA-W2KSERVER Windows_Sys_CpuLoaded 8/20/2004 2:51:55 PM 22 5

To set when you want to run the Discovery script, click the Schedule tab which will then result in the popup window shown in Figure 11-5.

Figure 11-5 Scheduling a Job


NetIQ Vivinet Manager Operator Console (Evaluation) on \\LXIA-W2KSERVER\VMDB (Administrator)
File View TreeView List Graph KS Web Extensions Window Help
Master
LXIA-W2KSERVER
Video Quality:LXIA-W2KSERVER
Windows:LXIA-W2KSERVER
Call Performance:LXIA-W2KSERVER
H.323:LXIA-W2KSERVER
SIP:LXIA-W2KSERVER
CallManager Express:cme32-3745.cis
Switch:cme32-3745.cisco.com [172.1
CallManager Express:alpha-3745 [172
Router:alpha-3745 [172.19.153.129]
Router:cme32-3745.cisco.com [172.1
CallManager Express:alpha-3745.cisc
Router:alpha-3745.cisco.com [172.19
CallSetup_H.323
CallSetup_SIP
VoIPQuality_CiscoSAA
Windows
Properties for Discovery_CiscoCME
Schedule
Values
Actions
Objects
Advanced
OK
Cancel
Help
GENERAL
NETWORK
NETWORKDEVICE
REC
Events
Jobs
Details
Graph Data
Master
VideoQuality
Windows
CallPerf
H.323
SIP
CiscoCME
NetworkDevice
For Help, press F1
Computers : 1
Open Events: 1064
Running Jobs: 20
Graph Data: 6
6:39 PM
149550

Schedule type
○ Run once
● Regular intervals
○ X number of times
○ Daily schedule
○ Weekly schedule
○ Monthly schedule
○ Asynchronous

Every: 5 Minute(s)

Start time:
● Now
○ Start date: 8/27/2004 Time: 6 40 00 ☑ PM

End time:
● No end date
○ End date: Time: 11 59 00 ☑ PM

*Jobs run at the scheduled date and time using the local time of the managed computer

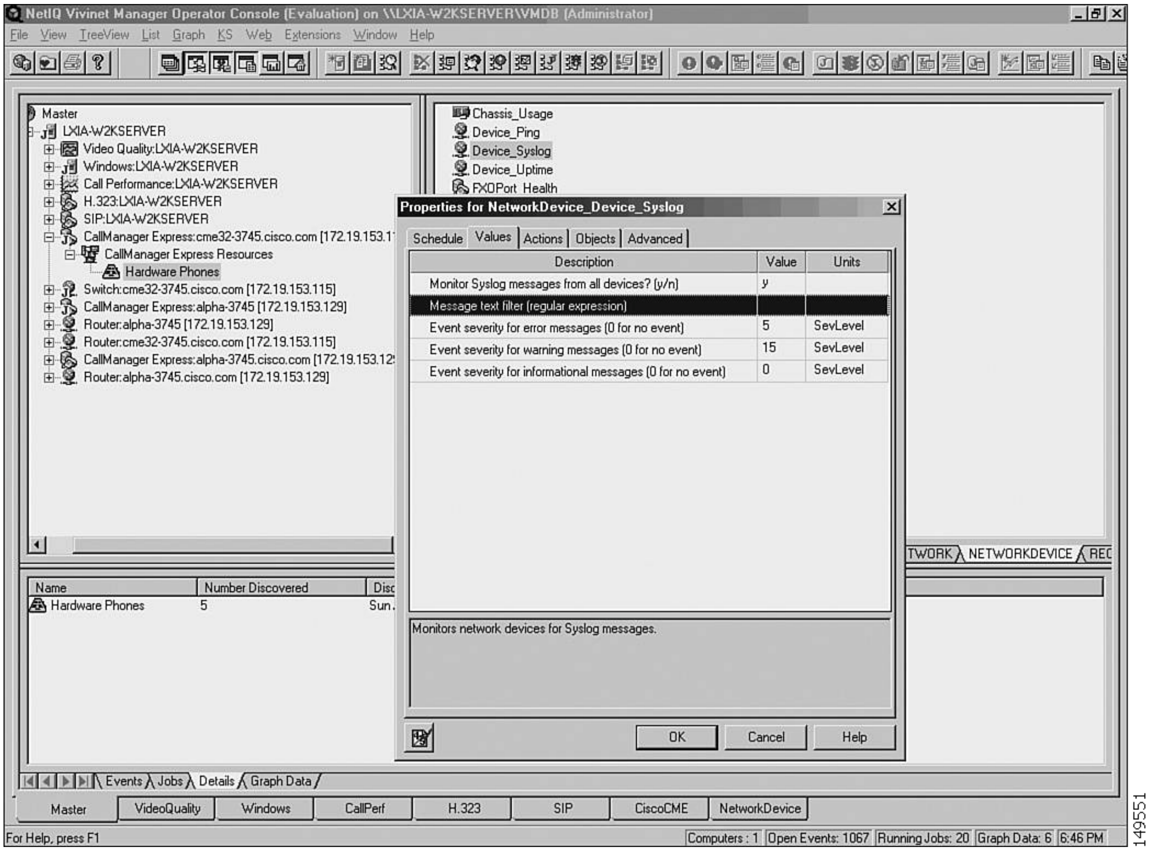
Job	Status	Childre				Submit Time	Stop Time
77	Running	1				8/23/2004 11:51:55 AM	<None>
75	Running	1				8/23/2004 11:51:49 AM	<None>
73	Stopped	1				8/23/2004 11:48:53 AM	8/23/2004 11:49:01 AM
71	Stopped	1				8/23/2004 11:45:29 AM	8/23/2004 11:45:34 AM
69	Stopped	1				8/23/2004 11:37:44 AM	8/23/2004 11:37:53 AM
67	Stopped	1				8/23/2004 11:37:02 AM	8/23/2004 11:37:06 AM
65	Stopped	1	LXIA-W2KSERVER	CiscoCME_Phone_Inventory	LXIA-W2KSERVER\Administrato	8/23/2004 11:36:49 AM	8/23/2004 11:36:56 AM
63	Stopped	1	LXIA-W2KSERVER	CiscoCME_Phone_Inventory	LXIA-W2KSERVER\Administrato	8/23/2004 11:31:14 AM	8/23/2004 11:31:20 AM
61	Running	1	LXIA-W2KSERVER	CiscoCME_Phone_Inventory	LXIA-W2KSERVER\Administrato	8/23/2004 11:26:33 AM	<None>

Choose the Schedule type to run once, at regular intervals, or on a daily/weekly schedule. Select a Start time and End time, and then click **OK** to schedule a job. The job scheduled is displayed in the Jobs tab as Running or as Stopped if the job is complete.

Monitoring New Phones

You can use the NetworkDevice_Device_Syslog script to inform you when a configured phone (known) or a new phone (unknown) registers with a Cisco Unified CME. In the NETWORKDEVICE pane, drag and drop Device_Syslog onto a Cisco Unified CME router in the TreeView panel. The Properties for NetworkDevice_Device_Syslog window appears, as shown in Figure 11-6.

Figure 11-6 Device Syslog Setup


NetIQ Vivinet Manager Operator Console (Evaluation) on \\LXIA-W2KSERVER\VMDB (Administrator)
File View TreeView List Graph KS Web Extensions Window Help
Master
LXIA-W2KSERVER
Video Quality:LXIA-W2KSERVER
Windows:LXIA-W2KSERVER
Call Performance:LXIA-W2KSERVER
H.323:LXIA-W2KSERVER
SIP:LXIA-W2KSERVER
CallManager Express:cme32-3745.cisco.com [172.19.153.1
CallManager Express Resources
Hardware Phones
Switch:cme32-3745.cisco.com [172.19.153.115]
CallManager Express:alpha-3745 [172.19.153.129]
Router:alpha-3745 [172.19.153.129]
Router:cme32-3745.cisco.com [172.19.153.115]
CallManager Express:alpha-3745.cisco.com [172.19.153.12
Router:alpha-3745.cisco.com [172.19.153.129]
Chassis_Usage
Device_Ping
Device_Syslog
Device_Uptime
FXOPort_Health
Name
Number Discovered
Disc
Hardware Phones
5
Sun.
TWORK
NETWORKDEVICE
REC
Events
Jobs
Details
Graph Data
Master
VideoQuality
Windows
CallPerf
H.323
SIP
CiscoCME
NetworkDevice
For Help, press F1
Computers : 1
Open Events: 1067
Running Jobs: 20
Graph Data: 6
6:46 PM
149551

Properties for NetworkDevice_Device_Syslog

Schedule
Values
Actions
Objects
Advanced
OK
Cancel
Help

Description	Value	Units
Monitor Syslog messages from all devices? (y/n)	y	
Message text filter (regular expression)		
Event severity for error messages (0 for no event)	5	SevLevel
Event severity for warning messages (0 for no event)	15	SevLevel
Event severity for informational messages (0 for no event)	0	SevLevel

Monitors network devices for Syslog messages.

In the Values tab, change the value for Monitor Syslog messages from all devices? (y/n) to y, and change other values if needed. You might configure an action to be taken (in the Actions tab) when events or errors occur.

As described in the "Monitoring IP Phones Using Cisco Unified CME Syslog Messages" section on page 11-5, a syslog message is generated when an IP phone registers with Cisco Unified CME. In addition, a different syslog message is generated when a new or unknown phone requires Cisco Unified CME to create an ephone configuration entry. You can configure NetworkDevice_Device_Syslog to watch for these entries and to generate events as needed.

When a new phone registers and has no ephone configuration entry, the register message is IPPHONE-6-REGISTER_NEW. When a configured phone registers, the register message is simply IPPHONE-6-REGISTER. The following example gives a sample registration message.

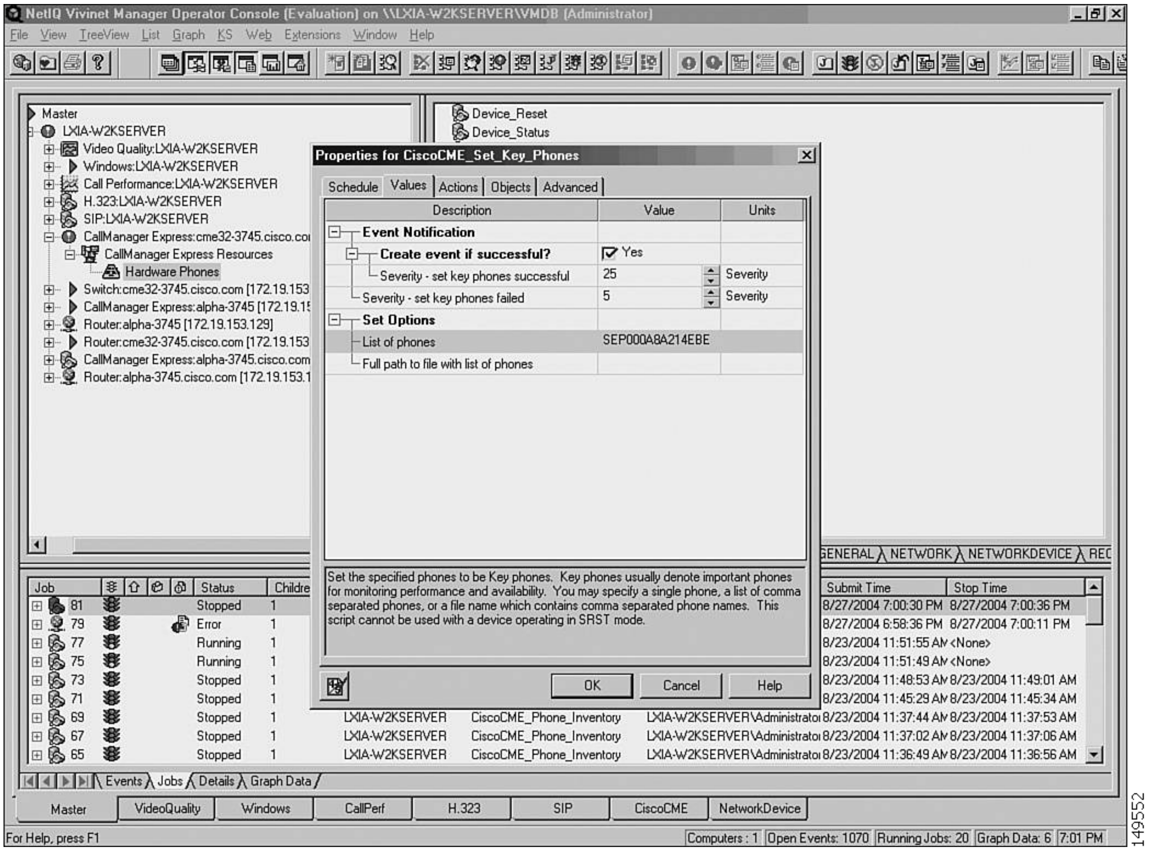
```
1w2d: %IPPHONE-6-REG_ALARM: 25: Name=SEP00036B7FFF59 Load=3.2(2.14)Last=
  Initialized
1w2d: %IPPHONE-6-REGISTER_NEW: ephone-4: SEP00036B7FFF59 IP:192.168.1.16 Socket:3
  DeviceType:Phone has registered. Reseting SEP00036B7FFF59
1w2d: %IPPHONE-6-UNREGISTER_NORMAL: ephone-4: SEP00036B7FFF59 IP:192.168.1.16 Soc
ket:3 DeviceType:Phone has unregistered normally.
1w2d: %IPPHONE-6-REG_ALARM: 22: Name=SEP00036B7FFF59 3 Load=3.2(2.14)Last=
  Reset-Reset
1w2d: %IPPHONE-6-REGISTER: ephone-4: SEP00036B7FFF59 IP:192.168.1.16 Socket:3
  DeviceType:Phone has registered.
```

Managing Key Phones

You might set certain phones as key phones so that you monitor only a selected set of important phones. You can use the CiscoCME_Set_Key_Phones Knowledge Script to designate one or more phones as key phones. Although you can use a Knowledge Script to set a key phone, you must use the CLI to remove a key designation from a phone.

Drag and drop Set_Key_Phone on the Cisco Unified CME Resource in the TreeView. Configure the MAC address of the phone you want to set as a key phone, or configure a filename with a full path if multiple phones are being established as key phones, as shown in Figure 11-7.

Figure 11-7 Setting Key Phones



NetIQ Vivinet Manager Operator Console (Evaluation) on \\LXIA-W2KSERVER\VMDB (Administrator)
File View TreeView List Graph KS Web Extensions Window Help
Master
LXIA-W2KSERVER
Video Quality:LXIA-W2KSERVER
Windows:LXIA-W2KSERVER
Call Performance:LXIA-W2KSERVER
H.323:LXIA-W2KSERVER
SIP:LXIA-W2KSERVER
CallManager Express:cme32-3745.cisco.co
CallManager Express Resources
Hardware Phones
Switch:cme32-3745.cisco.com [172.19.153
CallManager Express:alpha-3745 [172.19.1
Router:alpha-3745 [172.19.153.129]
Router:cme32-3745.cisco.com [172.19.153
CallManager Express:alpha-3745.cisco.com
Router:alpha-3745.cisco.com [172.19.153.1
Device_Reset
Device_Status
Properties for CiscoCME_Set_Key_Phones
Schedule
Values
Actions
Objects
Advanced
OK
Cancel
Help
GENERAL
NETWORK
NETWORKDEVICE
REC
Events
Jobs
Details
Graph Data
Master
VideoQuality
Windows
CallPerf
H.323
SIP
CiscoCME
NetworkDevice
For Help, press F1
Computers : 1
Open Events: 1070
Running Jobs: 20
Graph Data: 6
7:01 PM
149552

Description	Value	Units
Event Notification		
Create event if successful?	☑ Yes	
Severity - set key phones successful	25	Severity
Severity - set key phones failed	5	Severity
Set Options		
List of phones	SEP000A8A214EBE	
Full path to file with list of phones		

Set the specified phones to be Key phones. Key phones usually denote important phones for monitoring performance and availability. You may specify a single phone, a list of comma separated phones, or a file name which contains comma separated phone names. This script cannot be used with a device operating in SRST mode.

Job	Status	Childre				Submit Time	Stop Time
81	Stopped	1				8/27/2004 7:00:30 PM	8/27/2004 7:00:36 PM
79	Error	1				8/27/2004 6:58:36 PM	8/27/2004 7:00:11 PM
77	Running	1				8/23/2004 11:51:55 AM	<None>
75	Running	1				8/23/2004 11:51:49 AM	<None>
73	Stopped	1				8/23/2004 11:48:53 AM	8/23/2004 11:49:01 AM
71	Stopped	1				8/23/2004 11:45:29 AM	8/23/2004 11:45:34 AM
69	Stopped	1	LXIA-W2KSERVER	CiscoCME_Phone_Inventory	LXIA-W2KSERVER\Administrato	8/23/2004 11:37:44 AM	8/23/2004 11:37:53 AM
67	Stopped	1	LXIA-W2KSERVER	CiscoCME_Phone_Inventory	LXIA-W2KSERVER\Administrato	8/23/2004 11:37:02 AM	8/23/2004 11:37:06 AM
65	Stopped	1	LXIA-W2KSERVER	CiscoCME_Phone_Inventory	LXIA-W2KSERVER\Administrato	8/23/2004 11:36:49 AM	8/23/2004 11:36:56 AM

Stonevoice

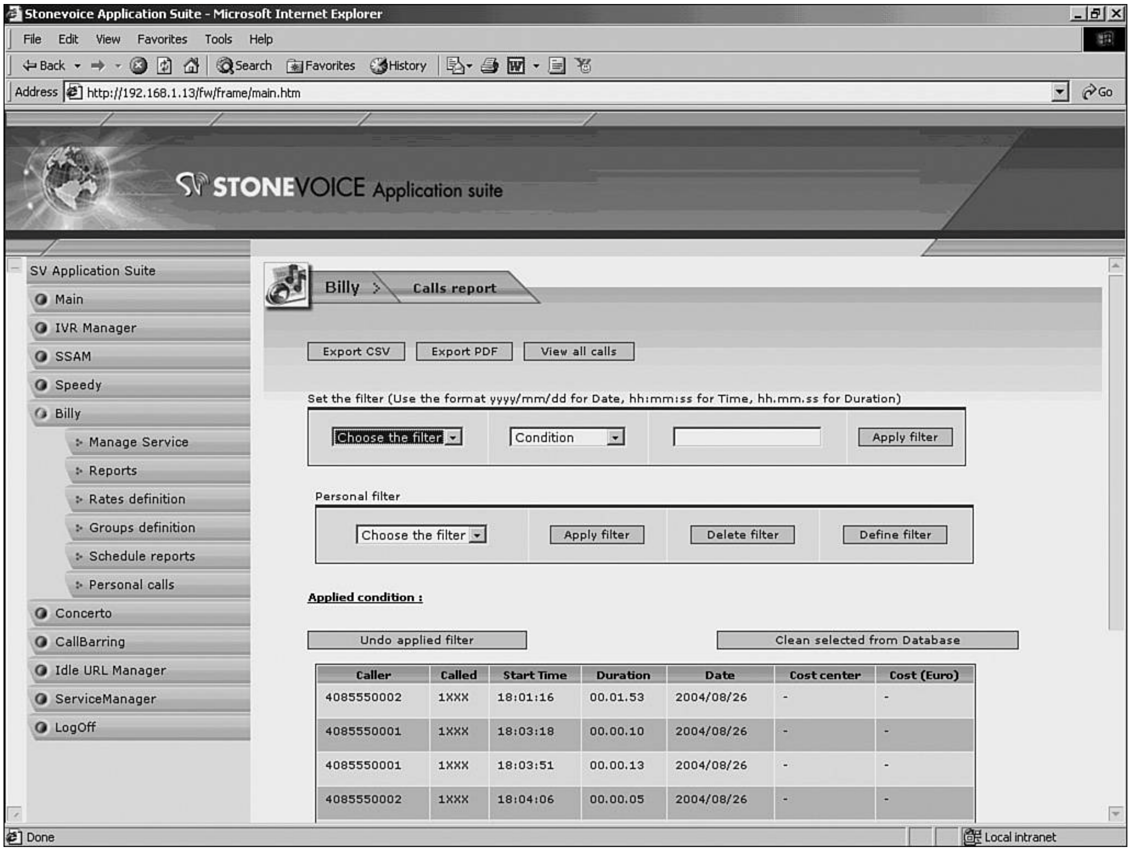
Stonevoice, a business unit of Computer Design in Italy, offers an application suite for Cisco Unified CME IP Telephony Solutions with the following capabilities:

- **Switch Answering Machine (SSAM)**—Manages voice mail integration with Cisco Unified CME via H.323.
- **Billy**—A call accounting and reporting tool based on CDR records (see Figure 11-8).
- **IVR Manager**—Equipped with canned scripts and prompts.
- **Concerto**—An MOH server to change a music file on-the-fly.

- **Speedy**—A directory manager that lets users add, delete, or modify public and personal directories.
- **CallBarring**—Call blocking and restriction based on time and day.
- **Service Manager**—An embedded tool to manage XML services and user subscriptions.
- **Idle URL Manager**—Displays text and images on the phone display when the phone is idle.

The View Call Report window associated with the Stonevoice Billy accounting application is shown in Figure 11-8.

Figure 11-8 View Call Report Window Associated with Billy Accounting Application


Stonevoice Application Suite - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go
STONEVOICE Application suite
SV Application Suite
Main
IVR Manager
SSAM
Speedy
Billy
Manage Service
Reports
Rates definition
Groups definition
Schedule reports
Personal calls
Concerto
CallBarring
Idle URL Manager
ServiceManager
LogOff
Billy
Calls report
Export CSV
Export PDF
View all calls
Choose the filter
Condition
Apply filter
Personal filter
Choose the filter
Apply filter
Delete filter
Define filter
Undo applied filter
Clean selected from Database
Done
Local intranet
149553

Address http://192.168.1.13/fw/frame/main.htm

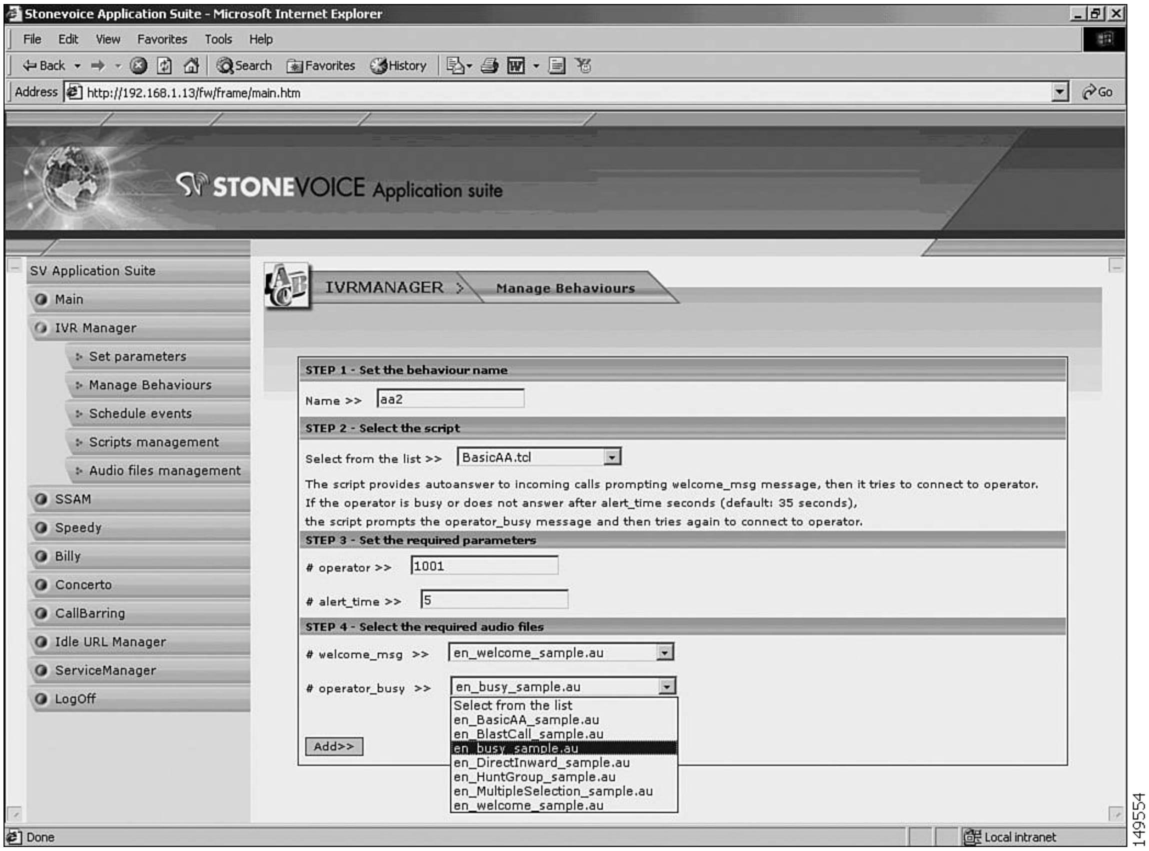
Set the filter (Use the format yyyy/mm/dd for Date, hh:mm:ss for Time, hh.mm.ss for Duration)

Applied condition :

Caller	Called	Start Time	Duration	Date	Cost center	Cost (Euro)
4085550002	1XXX	18:01:16	00.01.53	2004/08/26	-	-
4085550001	1XXX	18:03:18	00.00.10	2004/08/26	-	-
4085550001	1XXX	18:03:51	00.00.13	2004/08/26	-	-
4085550002	1XXX	18:04:06	00.00.05	2004/08/26	-	-

Figure 11-9 shows the IVR Manager window through which you can set up different system behaviors.

Figure 11-9 Using IVR Manager to Set Up Behaviors


Stonevoice Application Suite - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.13/fw/frame/main.htm
Go
STONEVOICE Application suite
SV Application Suite
Main
IVR Manager
Set parameters
Manage Behaviours
Schedule events
Scripts management
Audio files management
SSAM
Speedy
Billy
Concerto
CallBarring
Idle URL Manager
ServiceManager
LogOff
IVRMANAGER
Manage Behaviours
Add>>
Done
Local intranet
149554

STEP 1 - Set the behaviour name

Name >> aa2

STEP 2 - Select the script

Select from the list >> BasicAA.tcl

The script provides autoanswer to incoming calls prompting welcome_msg message, then it tries to connect to operator.
If the operator is busy or does not answer after alert_time seconds (default: 35 seconds),
the script prompts the operator_busy message and then tries again to connect to operator.

STEP 3 - Set the required parameters

operator >> 1001

alert_time >> 5

STEP 4 - Select the required audio files

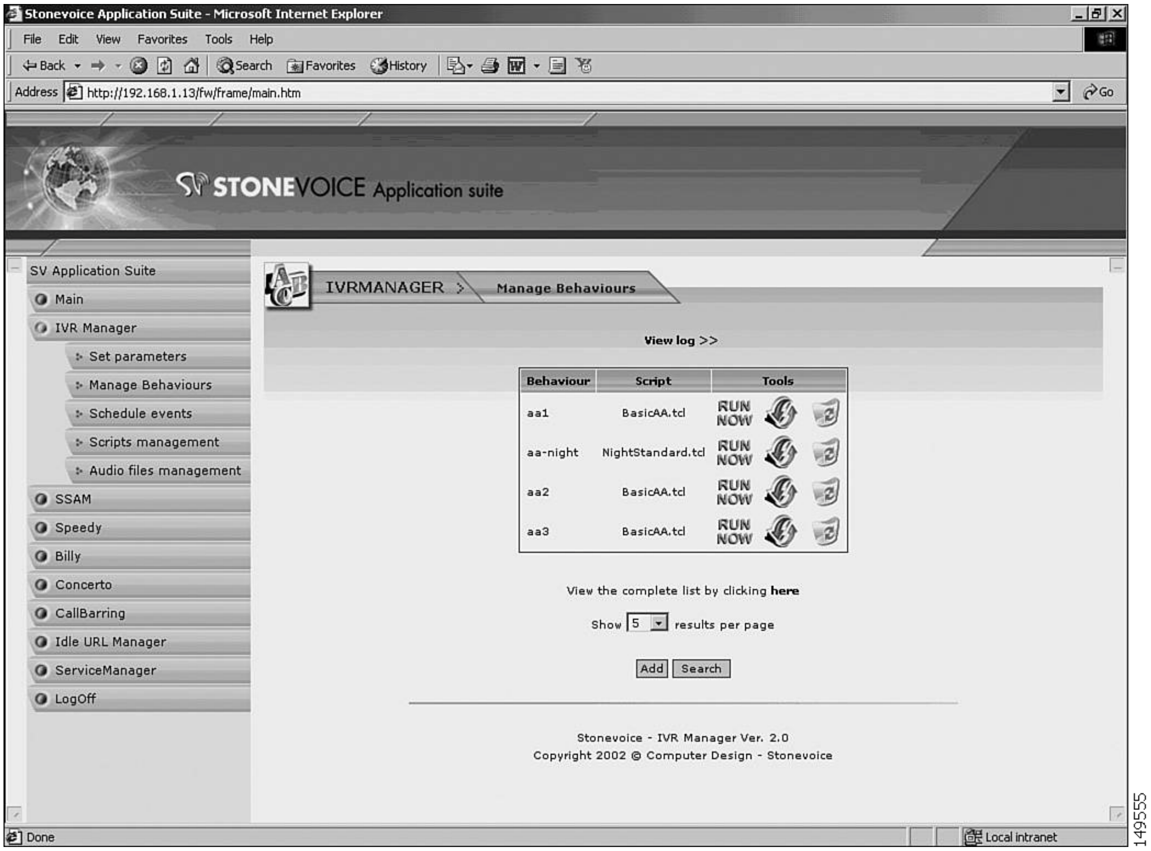
welcome_msg >> en_welcome_sample.au

operator_busy >> en_busy_sample.au

- Select from the list
- en_BasicAA_sample.au
- en_BlastCall_sample.au
- en_busy_sample.au
- en_DirectInward_sample.au
- en_HuntGroup_sample.au
- en_MultipleSelection_sample.au
- en_welcome_sample.au

Figure 11-10 shows the IVR Manager window through which you can review the TCL scripts in your system and where you can run a particular TcL script.

Figure 11-10 Viewing TcL scripts using IVR Manager:


Stonevoice Application Suite - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
STONEVOICE Application suite
SV Application Suite
Main
IVR Manager
Set parameters
Manage Behaviours
Schedule events
Scripts management
Audio files management
SSAM
Speedy
Billy
Concerto
CallBarring
Idle URL Manager
ServiceManager
LogOff
IVRMANAGER >
Manage Behaviours
View log >>
RUN NOW
Add
Search
Done
Local intranet
149555

Address: http://192.168.1.13/fw/frame/main.htm

Behaviour	Script	Tools
aa1	BasicAA.tcl	RUN NOW
aa-night	NightStandard.tcl	RUN NOW
aa2	BasicAA.tcl	RUN NOW
aa3	BasicAA.tcl	RUN NOW

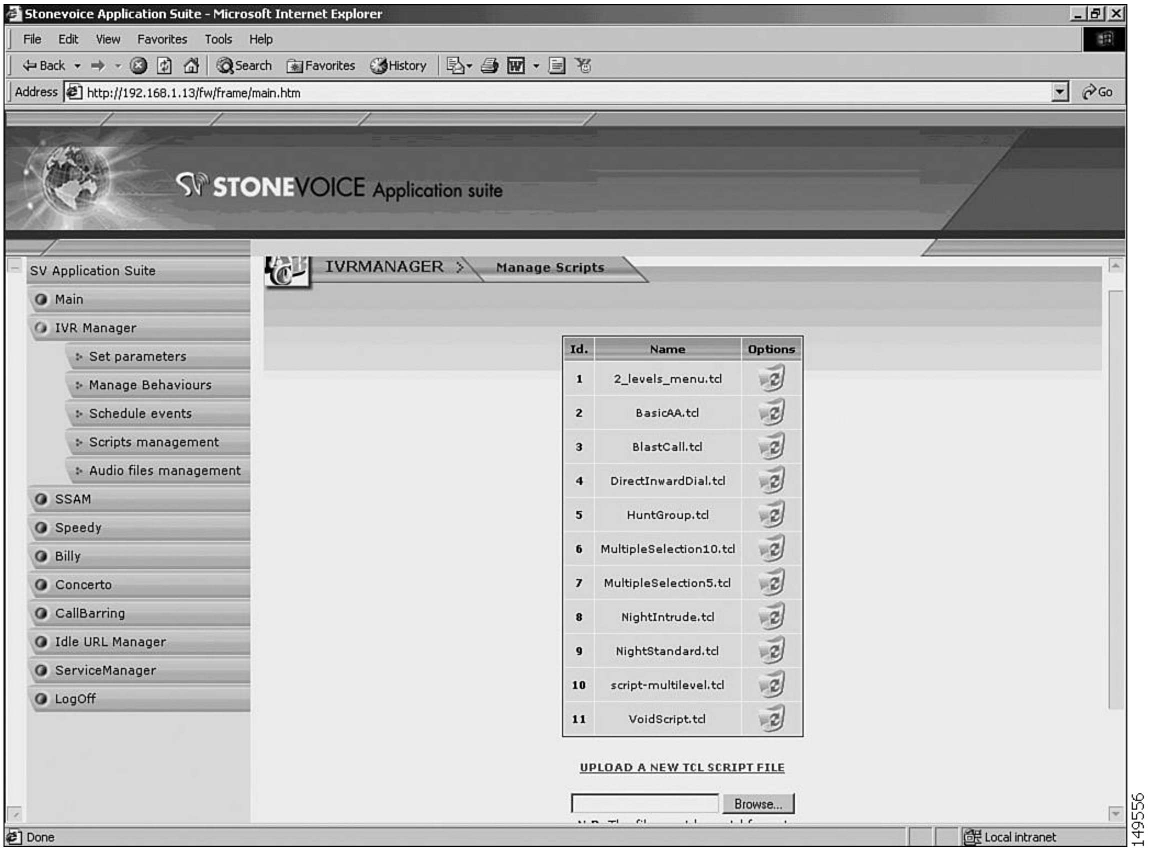
View the complete list by clicking **here**

Show 5 results per page

Stonevoice - IVR Manager Ver. 2.0
Copyright 2002 © Computer Design - Stonevoice

Figure 11-11 shows the IVR Manager window through which you can manage TcL scripts.

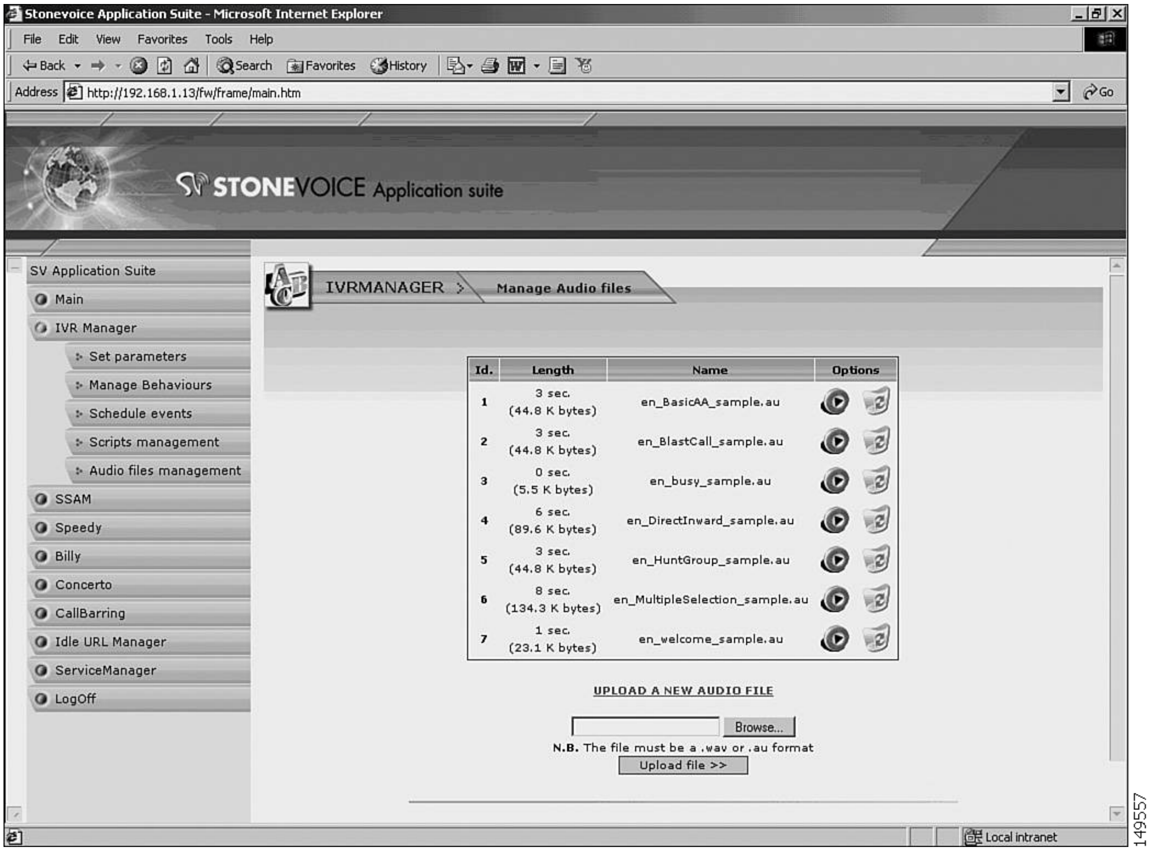
Figure 11-11 Managing TcL scripts using IVR Manager


Stonevoice Application Suite - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.13/fw/frame/main.htm
Go
STONEVOICE Application suite
SV Application Suite
Main
IVR Manager
Set parameters
Manage Behaviours
Schedule events
Scripts management
Audio files management
SSAM
Speedy
Billy
Concerto
CallBarring
Idle URL Manager
ServiceManager
LogOff
IVRMANAGER > Manage Scripts
UPLOAD A NEW TCL SCRIPT FILE
Browse...
Done
Local intranet
149556

Id.	Name	Options
1	2_levels_menu.tcl	
2	BasicAA.tcl	
3	BlastCall.tcl	
4	DirectInwardDial.tcl	
5	HuntGroup.tcl	
6	MultipleSelection10.tcl	
7	MultipleSelection5.tcl	
8	NightIntrude.tcl	
9	NightStandard.tcl	
10	script-multilevel.tcl	
11	VoidScript.tcl	

Figure 11-12 shows the IVR Manager window through which you can manage .wav and .au audio files on your system.

Figure 11-12 Managing Audio Files using IVR Manager


Stonevoice Application Suite - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.13/fw/frame/main.htm
Go
STONEVOICE Application suite
SV Application Suite
Main
IVR Manager
Set parameters
Manage Behaviours
Schedule events
Scripts management
Audio files management
SSAM
Speedy
Billy
Concerto
CallBarring
Idle URL Manager
ServiceManager
LogOff
IVRMANAGER
Manage Audio files
Browse...
Upload file >>
Local intranet
149557

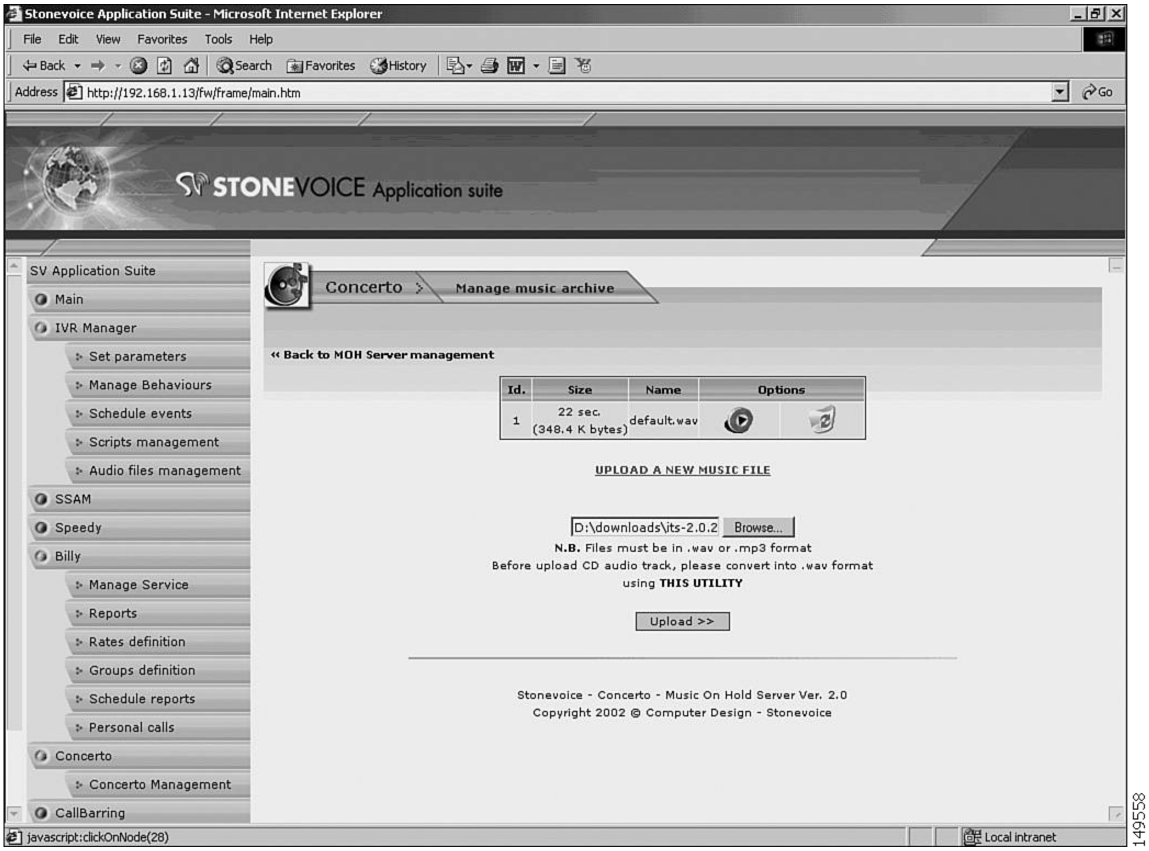
Id.	Length	Name	Options
1	3 sec. (44.8 K bytes)	en_BasicAA_sample.au	
2	3 sec. (44.8 K bytes)	en_BlastCall_sample.au	
3	0 sec. (5.5 K bytes)	en_busy_sample.au	
4	6 sec. (89.6 K bytes)	en_DirectInward_sample.au	
5	3 sec. (44.8 K bytes)	en_HuntGroup_sample.au	
6	8 sec. (134.3 K bytes)	en_MultipleSelection_sample.au	
7	1 sec. (23.1 K bytes)	en_welcome_sample.au	

UPLOAD A NEW AUDIO FILE

N.B. The file must be a .wav or .au format

Figure 11-13 illustrates the Concerto MOH management application window.

Figure 11-13 Uploading a MOH File using Concerto


Stonevoice Application Suite - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.13/fw/frame/main.htm
Go
STONEVOICE Application suite
SV Application Suite
Main
IVR Manager
Set parameters
Manage Behaviours
Schedule events
Scripts management
Audio files management
SSAM
Speedy
Billy
Manage Service
Reports
Rates definition
Groups definition
Schedule reports
Personal calls
Concerto
Concerto Management
CallBarring
Concerto
Manage music archive
Browse...
Upload >>
javascript:clickOnNode(28)
Local intranet
149558

« Back to MOH Server management

Id.	Size	Name	Options
1	22 sec. (348.4 K bytes)	default.wav	

UPLOAD A NEW MUSIC FILE

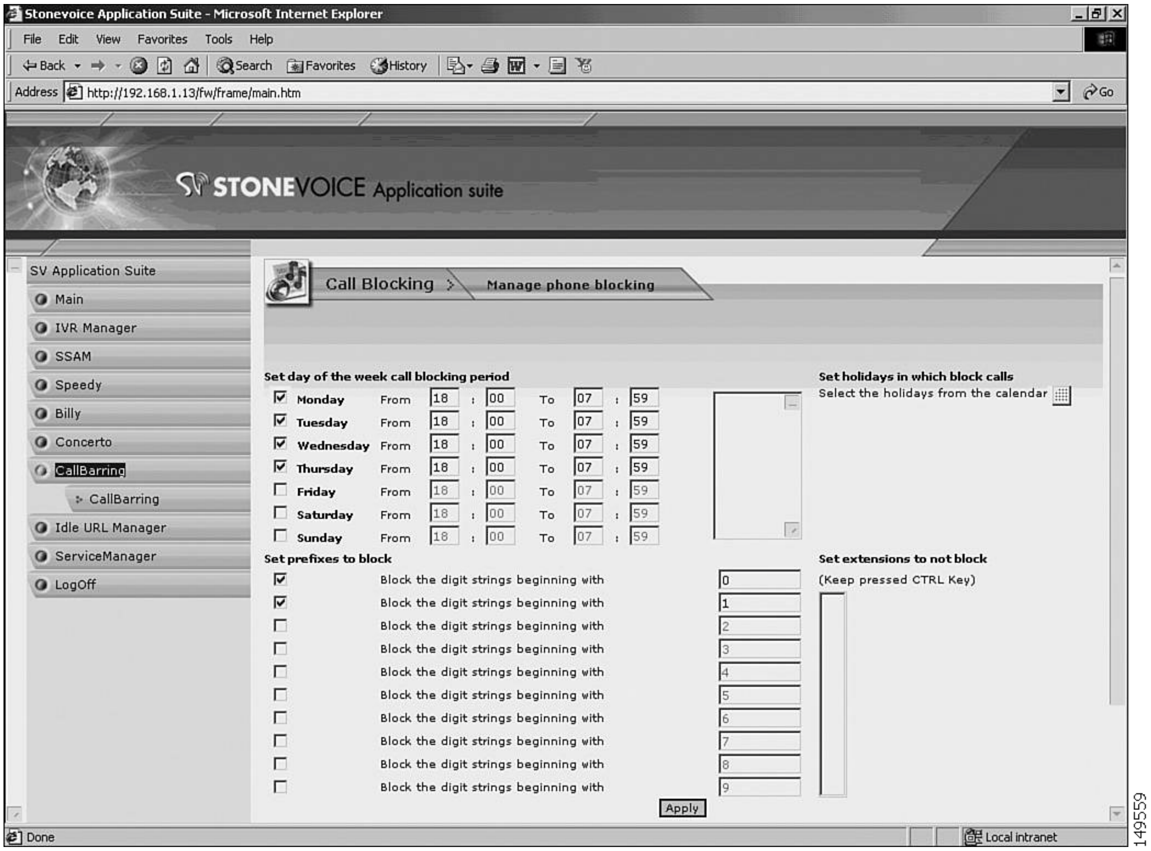
D:\downloads\its-2.0.2

N.B. Files must be in .wav or .mp3 format
Before upload CD audio track, please convert into .wav format
using **THIS UTILITY**

Stonevoice - Concerto - Music On Hold Server Ver. 2.0
Copyright 2002 © Computer Design - Stonevoice

Figure 11-14 shows the CallBarring application window, which lets you set up digit strings that might not be called.

Figure 11-14 Setting Up Call Blocking using CallBarring


Stonevoice Application Suite - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.13/fw/frame/main.htm
Go
STONEVOICE Application suite
SV Application Suite
Main
IVR Manager
SSAM
Speedy
Billy
Concerto
CallBarring
CallBarring
Idle URL Manager
ServiceManager
LogOff
Call Blocking
Manage phone blocking
Done
Local intranet
149559

Set day of the week call blocking period

	Day		From			To		
☑	Monday	From	18	:	00	To	07	: 59
☑	Tuesday	From	18	:	00	To	07	: 59
☑	Wednesday	From	18	:	00	To	07	: 59
☑	Thursday	From	18	:	00	To	07	: 59
☐	Friday	From	18	:	00	To	07	: 59
☐	Saturday	From	18	:	00	To	07	: 59
☐	Sunday	From	18	:	00	To	07	: 59

Set holidays in which block calls
Select the holidays from the calendar

Set prefixes to block

☑	Block the digit strings beginning with	0
☑	Block the digit strings beginning with	1
☐	Block the digit strings beginning with	2
☐	Block the digit strings beginning with	3
☐	Block the digit strings beginning with	4
☐	Block the digit strings beginning with	5
☐	Block the digit strings beginning with	6
☐	Block the digit strings beginning with	7
☐	Block the digit strings beginning with	8
☐	Block the digit strings beginning with	9

Set extensions to not block
(Keep pressed CTRL Key)

Apply

ISI Telemanagement Solutions Inc. Infortel Select

Infortel Select from ISI Telemanagement Solutions, Inc.can be used for tracking billing information for Cisco Unified CME. ISI provides the following functions:

- Infortel Select provides leading call accounting solutions
- Infortel Select helps you manage costs, improve productivity and increase profitability through control of your telecom environment
- Usage-based allocation of variable and fixed telecommunications expenses
- Identification of potential abuse or misuse
- Analysis of telephone-related employee productivity
- Analysis of traffic and trunk utilization for troubleshooting and facility planning
- Investigation of corporate security concerns
- Historical archive of call activity

Note For more information, see this URL: http://www.isi-info.com/

Integrated Research Prognosis

Integrated Research's *Prognosis* tool can be used for monitoring Cisco Unified CME and Cisco Unity Express. Prognosis provides the following monitoring functions:

- Call quality monitoring—Monitors latency, packet loss, jitter and MOS scoring
- Availability monitoring —Monitors dash board view of phone, device and call availability; monitors percentage of phones and devices up and down
- Call detail metrics—Monitors call types and route patterns, origin and duration of calls
- Key phone metrics—Monitors offhook, registration, mac-address data
- Configuration metrics—Monitors phone, h323 gateway, dial-peer, telephony-service, software/hardware inventory
- Systems and protocol monitoring—Monitors CPU and process memory, software version, application/voice traffic

Note For more information, see this URL: http://www.prognosis.com/

CHAPTER 12

IP Telephony Endpoints for Cisco Unified CallManager Express

This chapter summarizes various types of Cisco Unified IP Telephony endpoints along with their features, related design considerations, and QoS recommendations. The following sections provide information relevant to implementing Cisco Unified IP Telephony endpoints in a Cisco Unified CallManager Express (Cisco Unified CME) environment:

- Analog Gateway, page 12-2
- Cisco Unified IP Phone, page 12-3
- Wireless Endpoint, page 12-4
- Cisco Unified IP Conference Station, page 12-8
- QoS Recommendations, page 12-8
- Endpoint Features Summary, page 12-17

Note For additional information, see the "Related Documents and References" section on page xii.

Analog Gateway

The Cisco Unified CallManager Express (Cisco Unified CME) provides support for analog phones using Cisco Analog Telephone Adapter (ATA) or VG 224 gateway in SCCP mode. The analog gateway is usually used to connect analog devices, such as fax machines, modems, TDD/TTYs, and analog phones, to the VoIP network so that the analog signal can be packetized and transmitted over the IP network.

Cisco VG224 Gateway

The Cisco VG224 analog gateway is a Cisco IOS software-based, high-density 24-port gateway for connecting analog devices to the IP telephony network. It supports Cisco IOS Release 12.3.4-XD and higher. The Cisco VG224 connects with Cisco Unified CallManager using MGCP, and it has built-in MGCP failover to an H.323 connection to an Cisco Unified SRST router. The Cisco VG224 integrates with Cisco Unified CME using either H.323 or SIP. The Cisco VG224 supports Cisco Unified CME 3.1 and later releases. The Cisco VG224 is best used with high-density analog devices connecting to the IP network with limited call features, and it is more cost-effective than the Cisco VG248 for deployments of up to 24 analog ports.

Cisco Analog Telephone Adaptor

The Cisco Analog Telephone Adaptor (Cisco ATA) 186 (or Cisco ATA 188) is an analog telephony adapter that can connect two analog devices to the IP telephony network. The difference between the Cisco ATA 186 and Cisco ATA 188 is that the former has only one 10BaseT Ethernet connection while the later has an integrated Ethernet switch providing two 10BaseT/100BaseT Ethernet connections for itself and a co-located PC or other Ethernet-based device. The Cisco ATA 186 or Cisco ATA 188 supports only unicast Music on Hold (MoH).

The Cisco ATA 186 and Cisco ATA 188 can be configured in any of the following ways:

- Cisco ATA web configuration page
- Cisco ATA voice configuration menu
- Configuration file downloaded from the TFTP server

The SCCP-based ATA behaves like an SCCP IP phone. The Cisco ATA 186 or Cisco ATA 188 can be configured as an H.323 client to Cisco Unified CME or as an H.323 terminal to an H.323 gatekeeper. When the Cisco ATA registers with the gatekeeper as an H.323 terminal, the H.323 proxy must be disabled for the zone in which the ATA is located.

The Cisco ATA 186 or Cisco ATA 188 can also be configured as a SIP client that registers with the SIP server to make phone calls with another endpoint. The Cisco ATA 186 or Cisco ATA 188 can act as either a user agent client (UAC) when it initiates SIP requests or as a user agent server (UAS) when it responds to requests. The Cisco ATA 186 and Cisco ATA 188 are best used with low-density analog devices connecting to the IP network. In H.323 mode, the Cisco ATA 186 and Cisco ATA 188 do not mark the voice bearer packets correctly by default. You must manually configure the ATA to mark voice bearer traffic with a Differentiated Services Code Point (DSCP) value of EF by changing the Type of Service (ToS) field from its default value to a ToS value of 0x000000B8. This configuration change is no longer necessary with Cisco ATA 3.1 and later releases.

Cisco Unified IP Phone

The Cisco Unified IP Phones include low-end, mid-range, and high-end IP phones. The applicable Cisco Unified IP Phones for a Cisco Unified CME environment are described in the following sections:

- Low-End Cisco Unified IP Phones, page 12-3
- Mid-Range Cisco Unified IP Phones, page 12-4
- High-End Cisco Unified IP Phones, page 12-4

Note For information about support for different protocols and features associated with your specific endpoints, refer to your Cisco Unified CME documentation addressing this topic. The following is an example specific to Cisco Unified CME 4.0 endpoints: http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_installation_guide09186a00805f5908.html

Low-End Cisco Unified IP Phones

The low-end units are used for low-traffic situations with limited call feature and budget requirements. The low-end Cisco Unified IP Phones include the Cisco Unified IP Phone 7902G, Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7910G, Cisco Unified IP Phone 7910G+SW, Cisco Unified IP Phone 7911G, and Cisco Unified IP Phone 7912G.

Cisco Unified IP Phone 7902G

The Cisco Unified IP Phone 7902G supports a single line, and it has a single 10BaseT Ethernet port on the back of the phone. The Cisco Unified IP Phone 7902G does not have a liquid crystal display (LCD) screen.

Cisco Unified IP Phone 7905G

The Cisco Unified IP Phone 7905G supports a single line, and it has a single 10BaseT Ethernet port on the back of the phone. The speaker operates in one-way listen mode only.

Cisco Unified IP Phone 7910G and Cisco Unified IP Phone 7910G+SW

The Cisco Unified IP Phone 7910G supports a single line, and the speaker operates in one-way listen mode only. The Cisco Unified IP Phone 7910G also has six fixed-feature access keys that can be configured in the customized phone button template by the administrator to provide various end-user call features. Because there are only six fixed-feature keys, the model Cisco Unified IP Phone 7910G cannot provide end users with all of the call features through one phone button template.

The only difference between the Cisco Unified IP Phone 7910G and Cisco Unified IP Phone 7910G+SW is that the former has a single 10BaseT Ethernet port and the latter has two 10BaseT/100BaseT Ethernet ports.

Cisco Unfied IP Phone 7911G

The Cisco Unified IP Phone 7911G supports a single line. It is similar to the Cisco Unified IP Phone 7912G, but supports IEEE 802.3af Power over Ethernet, advanced security, and an extended software roadmap to support advanced IP features.

Cisco Unified IP Phone 7912G

The Cisco Unified IP Phone 7912G supports a single line, and it has two 10BaseT/100BaseT Ethernet connections. The speaker operates in one-way listen mode only.

Mid-Range Cisco Unified IP Phones

The midrange Cisco Unified IP Phone used for high-traffic situations with extensive call features, such as speakers, headset, and so forth. The mid-range Cisco Unified IP Phones include the Cisco Unified IP Phone 7940G, Cisco Unified IP Phone 7941G, Cisco Unified IP Phone 7960G, and Cisco Unified IP Phone 7961G.

The Cisco Unified IP Phone 7940G and Cisco Unified IP Phone 7941G can each have up to two directory numbers, and the Cisco IP Phone 7960G and Cisco Unified IP Phone 7961G can each have a total of six directory numbers. All four phone models are compatible with Cisco VT Advantage video-enabled endpoints for making video calls.

High-End Cisco Unified IP Phones

The Cisco Unified IP Phone 7970G and Cisco Unified IP Phone 7971G, the high-end Cisco Unified IP Phones, are used for high-traffic situations with extensive call features. The Cisco Unified IP Phone 7970G has a high-resolution, color touch-screen display, more function keys, and more security features than the midrange Cisco Unified IP phones. The Cisco Unified IP Phone 7970G can also have up to eight directory numbers.

The Cisco Unified IP Phone 7970G is also compatible with Cisco VT Advantage video-enabled endpoints for making video calls. The Cisco Unified IP Phone 7970G is the only Cisco Unified IP phone that supports both Cisco prestandard Power-over-Ethernet (PoE) and the IEEE 802.3af PoE. For the Cisco Unified IP Phone 7970G to have full display brightness, you must use the external power adapter (CP-PWR-CUBE2) with both inline power and IEEE 802.3af PoE.

The Cisco Unified IP Phone 7971G can have up to eight directory numbers and is the equivalent of the Cisco Unified IP Phone 7970G with the exception that it includes two 10/100/1000 BaseT Ethernet connections. The addition of gigabit throughput capability allows for high bit-rate and bandwidth-intensive applications on a co-located PC.

Wireless Endpoint

Cisco wireless endpoints use a wireless LAN (WLAN) infrastructure through wireless access points (APs) to provide telephony functionality and features. This type of endpoint is ideal for environments with the need for mobile users within a area where traditional wired phones are undesirable or problematic. (See the "Wireless LAN Infrastructure" section on page 3-33, for more information about wireless network design.)

The Cisco Unified Wireless IP Phone 7920G is a hardware-based phone with a built-in radio antenna that enables 802.1b wireless LAN connectivity to the network. These phones register with Cisco Unified CallManager using Skinny Client Control Protocol (SCCP).

The following sections summarizes wireless endpoint considerations in a Cisco CME environment:

- Site Survey, page 12-5
- Authentication, page 12-5
- Capacity, page 12-6
- Phone Configuration, page 12-6
- Roaming, page 12-7
- AP Call Admission Control, page 12-8

Site Survey

Before deploying the Cisco Unified Wireless IP Phone 7920G, you must perform a complete site survey to determine the appropriate number and location of APs required to provide radio frequency (RF) coverage. Your site survey should take into consideration which types of antennas will provide the best coverage and where sources of RF interference might exist. A site survey requires the use of the Site Survey tool on the Cisco Unified Wireless IP Phone 7920G (accessed through the **Menu** > **Network Config** > **Site Survey** windows path) and the Aironet Client Utility Site Survey Tool used with a Cisco Aironet NIC card on a laptop or PC. Additional third-party tools can also be used for site surveys; however, we highly recommend that you conduct a final site survey using the Cisco Unified Wireless IP Phone 7920G because each endpoint or client radio can behave differently depending on antenna sensitivity and survey application limitations.

Authentication

To connect to the wireless network, the Cisco Unified Wireless IP Phone 7920G must first use one of the following authentication methods to associate and communicate with the AP:

- Cisco LEAP

  This method allows the Cisco Unified Wireless IP Phone 7920G and AP to be authenticated mutually based on a username and password. Upon authentication, the dynamic key is generated and used for encrypting traffic between the Cisco Unified Wireless IP Phone 7920G and the AP. A Cisco LEAP-compliant Radius authentication server, such as the Cisco Secure Access Control Server (ACS), is required to provide access to the user database.

- Static Wired Equivalent Privacy (WEP)

  This method involves the configuration of static 10 (40-bit) or 26 (128-bit) character keys on the Cisco Unified Wireless IP Phone 7920G and the AP. This method is AP-based authentication in which access to the network is gained if the device has a matching key.

- Open Authentication

  This method requires no exchange of identifying information between the Cisco Unified Wireless IP Phone 7920G and the AP. We do *not* recommend this method because it provides no secure exchange of voice or signaling, and it allows any rouge device to associate to the AP.

Capacity

Each AP can support a maximum of seven active G.711 voice calls or eight G.729 calls. If these numbers are exceeded, poor quality can result due to dropped or delayed voice packets or dropped calls. AP rates set lower than 11 Mbps will result in lower call capacity per AP.

Based on these active call capacity limits, and using Erlang ratios, you can calculate the number of Cisco Unified Wireless 7920G IP Phones that each AP can support. For example, given a typical user-to-call capacity ratio of 3:1, a single AP can support 21 to 24 Cisco Unified Wireless 7920G IP Phones, depending whether the codec used is G.711 or G.729. However, this number does not take into consideration the possibility that other Cisco Unified Wireless 7920G IP Phones could roam to this AP, so a lower number of phones per AP is more realistic.

The number of APs per VLAN or Layer 2 subnet should also be considered. To optimize memory and performance on the APs we recommend deploying no more than 30 APs on a single VLAN or subnet. This recommendation, taken with typical user-to-call capacity ratios, limits the number of Cisco Unified Wireless 7920G IP Phones per Layer 2 subnet to approximately 500 (or about 15 to 17 Cisco Unified Wireless 7920G IP Phones per AP).

These capacities were calculated with voice activity detection (VAD) disabled and a packetization sample size of 20 milliseconds (ms). VAD is a mechanism for conserving bandwidth by not sending RTP packets while no speech is occurring during the call. We recommend leaving VAD (Silence Suppression) *disabled* to provide better overall voice quality.

At a sampling rate of 20 ms, a voice call will generate 50 packets per second (pps) in either direction. We recommend setting the sample rate to 20 ms for almost all cases. By using a larger sample size (for example, 30 or 40 ms), you can increase the number of simultaneous calls per AP, but a larger end-to-end delay will result. In addition, the percentage of acceptable voice packet loss within a wireless environment decreases dramatically with a larger sample size because more of the conversation is missing when a packet is lost. For more information about voice sampling size, see the "Bandwidth Provisioning" section on page 3-19.

Phone Configuration

You can configure the Cisco Unified Wireless IP Phone 7920G either through the phone's keypad or with the Cisco Unified Wireless IP Phone 7920 Configuration Utility running on a PC that is attached to the phone using a USB cable. In either case, you must configure the following parameters:

- Network Configuration

  Configure either the DHCP server address or static settings such as IP address, subnet mask, default gateway, TFTP server, and DNS server, as appropriate for the network. These settings can be found on the Cisco Unified Wireless IP Phone 7920G under **Menu** > **Network Config** > **Current Config**.

- Wireless Configuration

  Configure the service set identifier (SSID) for the voice VLAN and the authentication type, including the WEP key and/or LEAP username and password when appropriate. These settings can be found on the Cisco Unified Wireless IP Phone 7920G under **Menu** > **Network Config** > **802.11b Configuration**.

Roaming

The Cisco Unified Wireless IP Phone 7920G is able to roam at Layer 2 (within the same VLAN or subnet) and still maintain an active call.

Layer 2 roaming occurs in the following situations:

- During the initial boot-up of the Cisco Unified Wireless IP Phone 7920G, the phone roams to a new AP for the first time.
- If the Cisco Unified Wireless IP Phone 7920G receives no beacons or responses from the AP to which it is associated, the phone assumes that the current AP is unavailable and it attempts to roam and associate with a new AP.
- The Cisco Unified Wireless IP Phone 7920G maintains a list of eligible AP roam targets. If conditions change on the current AP, the phone consults the list of available AP roam targets. If one of the roam targets is determined to be a better choice, then the phone attempts to roam to the new AP.
- If the configured SSID or authentication type on the Cisco Unified Wireless IP Phone 7920G is changed, the phone must roam to reassociate with an AP.

In trying to determine eligible AP roam targets for Layer 2 roaming, the wireless IP phone uses the following variables to determine the best AP to associate with:

- Relative Signal Strength Indicator (RSSI)

  Used by the wireless IP phone to determine the signal strength and quality of available APs within an RF coverage area. The phone will attempt to associate with the AP that has the highest RSSI value and matching authentication/encryption type.

- QoS Basis Service Set (QBSS)

  Enables the AP to communicate channel utilization information to the wireless phone. The phone will use the QBSS value to determine if it should attempt to roam to another AP, because APs with high channel utilization might not be able to handle VoIP traffic effectively.

- RSSI-Differential Threshold

  The wireless IP phone will roam if the next AP RSSI is higher than the current AP RSSI by at least this threshold amount. The default threshold is 15.

- QBSS-Differential Threshold

  The wireless IP phone will roam if the next AP QBSS is lower than the current AP QBSS by at least this threshold amount. The default threshold is 15.

The wireless IP phone uses the following steps to determine which AP it should roam to:

1. Find APs that are advertising QBSS in their beacons. If any of these APs meet the QBSS-differential threshold criteria, then begin the roaming process to one of them.
2. If no APs are advertising QBSS, or if the advertising APs do not meet the differential threshold criteria, then look for APs that are not advertising QBSS but that have acceptable RSSI levels, and begin the roaming process to one of them.

Layer 2 roaming times for the wireless IP phone depend on the type of authentication used. If static WEP keys are used for authentication between the phone and the AP, Layer 2 roaming occurs in less than 100 ms. If LEAP (with local Cisco Secure ACS authentication) is used, Layer 2 roaming occurs in 200 to 400 ms. Use of Fast Secure Roaming can decrease the LEAP authentication time to less than 150 ms for Layer 2 roams.

Layer 3 roaming occurs when the Cisco Unified Wireless IP Phone 7920 moves from one AP to another AP and crosses a subnet boundary. With the release of the new Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), the Cisco Unified Wireless IP Phone 7920 now supports Layer 3 mobility with survivable calls while using Static WEP. Cisco Centralized Key Management (Cisco CKM) enables the Cisco Unified Wireless IP Phone 7920 to achieve full Layer 3 mobility while using LEAP.

AP Call Admission Control

Call admission control mechanisms in Cisco Unified CallManager or in a gatekeeper can control WAN bandwidth utilization and provide QoS for existing calls, but both mechanisms are applied only at the beginning of a call. For calls between static devices, this type of call admission control is sufficient. However, for a call between two mobile wireless devices such the Cisco Unified Wireless IP Phone 7920G, there must also be a call admission control mechanism at the AP level because the wireless devices may roam from one AP to another.

The AP mechanism for call admission control is QBSS, which is the beacon information element that enables the AP to communicate channel utilization information to the wireless IP phone. As previously mentioned, this QBSS value helps the phone determine whether it should roam to another AP. A lower QBSS value indicates that the AP is a good candidate to roam to, while a higher QBSS value indicates that the phone should not roam to this AP.

While this QBSS information is useful, it does not provide a 100 percent guarantee that calls will retain proper QoS during roaming. When a Cisco Unified Wireless 7920 IP Phone is associated to an AP with a high QBSS, the AP will prevent a call from being initiated or received by rejecting the call setup and sending a Network Busy message to the initiating phone. However, when a call is set up between a wireless IP phone and another endpoint, the phone may roam and associate with an AP with a high QBSS, thus resulting in an oversubscription of the available bandwidth on that AP.

Cisco Unified IP Conference Station

The Cisco Unified IP Conference Station combines conference room speaker-phone technology with Cisco Unified IP Communications technology. The Cisco Unified IP Conference Station is used in conferencing environments providing 360-degree room coverage.

The Cisco Unified IP Conference Station 7936 has an external speaker and three built-in microphones. The Cisco Unified IP Conference Station 7936 also features a pixel-based LCD display with backlighting, and optional extension microphones can be connected to it for extended microphone coverage in larger rooms.

QoS Recommendations

This section provides the basic QoS guidelines and configurations for the Cisco Catalyst switches most commonly deployed with IP Telephony endpoints. QoS is summarized in the following sections:

- Cisco VG224, page 12-9
- Cisco ATA 186 and Conference Station, page 12-10
- Cisco ATA 188 and Cisco Unified IP Phones, page 12-10
- Cisco Unified Wireless IP Phone 7920G, page 12-14

Cisco VG224

Analog gateways are trusted endpoints. For Cisco VG224 gateway, configure the switch to trust the DSCP value of the VG224 packets. The following sections list the commands to configure the most common Cisco Catalyst switches for the Cisco VG224 analog gateways.

Note In the following sections, *vvlan_id* is the voice VLAN ID and *dvlan_id* is the data VLAN ID.

Cisco 2950

```
CAT2950(config)# interface interface-id
CAT2950(config-if)# mls qos trust dscp
CAT2950(config-if)# switchport mode access
CAT2950(config-if)# switchport access vlan vvlan_id
```

Note The **mls qos trust dscp** command is available only with Enhanced Image (EI).

Cisco 2970 or 3750

```
CAT2970(config)# mls qos
CAT2970(config)# interface interface-id
CAT2970(config-if)# mls qos trust dscp
CAT2970(config-if)# switchport mode access
CAT2970(config-if)# switchport access vlan vvlan_id
```

Cisco 3560

```
CAT3560(config)# mls qos
CAT3560(config)# interface interface-id
CAT3560(config-if)# mls qos trust dscp
CAT3560(config-if)# switchport mode access
Cat3560(config-if)# switchport access vlan vvlan_id
```

Cisco 4500 with SUPIII, IV, or V

```
CAT4500(config)# qos
CAT4500(config)# interface interface-id
CAT4500(config-if)# qos trust dscp
CAT4500(config-if)# switchport mode access
CAT4500(config-if)# switchport access vlan vvlan_id
```

Cisco 6500

```
CAT6500>(enable) set qos enable
CAT6500>(enable) set port qos 2/1 vlan-based
CAT6500>(enable) set vlan vvlan_id mod/port
CAT6500>(enable) set port qos mod/port trust trust-dscp
```

Cisco ATA 186 and Conference Station

Because the Cisco Analog Telephone Adaptor (ATA) 186 and IP Conference Station are trusted endpoints, their QoS configurations are identical to those described in the "Cisco VG224" section on page 12-9.

Cisco ATA 188 and Cisco Unified IP Phones

For the Cisco ATA 188 and Cisco Unified IP Phones, we recommend segregating the voice VLAN from the data VLAN. For the Cisco ATA 186, Cisco Unified IP Phone 7902, Cisco Unified IP Phone 7905, Cisco Unified IP Phone 7910, and Cisco Unified IP Conference Station, we still recommend configuring voice and data VLAN segregation and an auxiliary voice VLAN. In this way, the same access-layer configurations can be used with different Cisco Unified IP Phone models and Cisco ATA units, and end users can plug their IP phones or Cisco AT units into different access ports on the switch and get the same treatment. For the Cisco ATA 186, Cisco Unified IP Phone 7902, Cisco Unified IP Phone 7905, Cisco Unified IP Phone 7910, and Cisco Unified IP Conference Stations, the command to override the CoS value of the frames from the attached PC has no effects because these devices do not have a PC connected to them.

The following sections list the configuration commands for IP phones on the most commonly deployed Cisco Catalyst switches.

Cisco 2950

```
CAT2950(config)#
CAT2950(config)# class-map VVLAN
CAT2950(config-cmap)# match access-group name VVLAN
CAT2950(config-cmap)# class-map VLAN
CAT2950(config-cmap)# match access-group name DVLAN
CAT2950(config-cmap)# exit
CAT2950(config)#
CAT2950(config)# policy-map IPPHONE-PC
CAT2950(config-pmap)# class VVLAN
CAT2950(config-pmap-c0# set ip dscp 46
CAT2950(config-pmap-c)# police 1000000 8192 exceed-action-drop
CAT2950(config-pmap)# class DVLAN
CAT2950(config-pmap-c0# set ip dscp 0
CAT2950(config-pmap-c)# police 5000000 8192 exceed-action-drop
CAT2950(config-pmap-c)# exit
CAT2950(config-pmap)# exit
CAT2950(config)#
CAT2950(config)# interface interface-id
CAT2950(config-if)# mls qos trust device cisco-phone
CAT2950(config-if)# mls qos trust cos
CAT2950(config-if)# switchport mode access
CAT2950(config-if)# switchport voice vlan vvlan_id
CAT2950(config-if)# switchport access vlan dvlan_id
CAT2950(config-if)# service-policy input IPPHONE-PC
CAT2950(config-if)# exit
CAT2950(config)#
CAT2950(config)# ip access-list standard VVLAN
CAT2950(config-std-nacl)# permit voice_IP_subnet wild_card_mask
CAT2950(config-std-nacl)# exit
CAT2950(config)# ip access-list standard DVLAN
CAT2950(config-std-nacl)# permit data_IP_subnet wild_card_mask
CAT2950(config-std-nacl)# end
```

Note The **mls qos map cos-dscp** command is available only with Enhanced Image (EI). With Standard Image (SI), this command is not available and the default CoS-to-DSCP mapping is as follows:

Cos Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Cisco 2970 or 3750

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#
CAT2970(config)# class-map match-all VVLAN-VOICE
CAT2970(config-cmap)# match access-group name VVLAN-VOICE
CAT2970(config-cmap)#
CAT2970(config-cmap)# class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)# class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)# policy-map IPPHONE-PC
CAT2970(config-pmap)# class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)# interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# switchport access vlan dvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input IPPHONE-PC
CAT2970(config-if)# exit
CAT2970(config)#
CAT2970(confiig)# ip access list extended VVLAN-VOICE
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet Subnet_Mask any range 16384 32767
dscp ef
CAT2970(config-ext-nacl)# exit
CAT2970(config)# ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet Subnet_Mask any range 2000 2002 dscp
cs3
CAT2970(config-ext-nacl)# exit
CAT2970(config)# ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet Subnet_Mask any
CAT2970(config-ext-nacl)# end
CAT2970#
```

Cisco 3560

```
CAT3560(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT3560(config)# mls qos map policed-dscp 0 24 to 8
CAT3560(config)#class-map match-all VOICE
CAT3560(config-cmap)# match ip dscp 46
CAT3560(config-cmap)# class-map match-any CALL SIGNALING
CAT3560(config-cmap)# match ip dscp 26
CAT3560(config-cmap)# match ip dscp 24
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all VVLAN-VOICE
CAT3560(config-cmap)# match vlan vvlan_id
CAT3560(config-cmap)# match class-map VOICE
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all VVLAN-CALL-SIGNALING
CAT3560(config-cmap)# match vlan vvlan_id
CAT3560(config-cmap)# match class-map CALL SIGNALING
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all ANY
CAT3560(config-cmap)# match access-group name ACL_Name
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all VVLAN-ANY
CAT3560(config-cmap)# match vlan vvlan_id
CAT3560(config-cmap)# match class-map ANY
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all DVLAN-ANY
CAT3560(config-cmap)# match vlan dvlan_id
CAT3560(config-cmap)# match class-map ANY
CAT3560(config-cmap)#
CAT3560(config-cmap)# policy-map IPPHONE-PC
CAT3560(config-pmap)# class VVLAN-VOICE
CAT3560(config-pmap-c)# set ip dscp 46
CAT3560(config-pmap-c)# police 128000 8000 exceed-action drop
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT3560(config-pmap-c)# set ip dscp 24
CAT3560(config-pmap-c)# police 32000 8000 exceed-action drop
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class VVLAN-ANY
CAT3560(config-pmap-c)# set ip dscp 0
CAT3560(config-pmap-c)# police 32000 8000 exceed-action drop
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class DVLAN-VOICE
CAT3560(config-pmap-c)# set ip dscp 0
CAT3560(config-pmap-c)# police 5000000 8000 exceed-action drop
CAT3560(config-pmap-c)# exit
CAT3560(config-pmap)# exit
CAT3560(config)# interface interface-id
CAT3560(config-if)# switchport voice vlan vvlan_id
CAT3560(config-if)# switchport access vlan dvlan_id
CAT3560(config-if)# mls qos trust device cisco-phone
CAT3560(config-if)# service-policy input IPPHONE-PC
CAT3560(config-if)# exit
CAT3560(config)#
CAT3560(confiig)# ip access list standard ACL_ANY
CAT3560(config-std-nacl)# permit any
CAT3560(config-std-nacl)# end
CAT3560#
```

Cisco 4500 with SUPIII, IV, or V

```
CAT4500(config)# qos map cos 5 to dscp 46
CAT4500(config)# qos map cos 0 24 to dscp 8
```

```
CAT4500(config)#
CAT4500(config)# class-map match-all VVLAN-VOICE
CAT4500(config-cmap)# match access-group name VVLAN-VOICE
CAT4500(config-cmap)#
CAT4500(config-cmap)# class-map match-all VVLAN-CALL-SIGNALING
CAT4500(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT4500(config-cmap)#
CAT4500(config-cmap)# class-map match-all VVLAN-ANY
CAT4500(config-cmap)# match access-group name VVLAN-ANY
CAT4500(config-cmap)#
CAT4500(config-cmap)# policy-map IPPHONE-PC
CAT4500(config-pmap)# class VVLAN-VOICE
CAT4500(config-pmap-c)# set ip dscp 46
CAT4500(config-pmap-c)# police 128 kps 8000 byte exceed-action drop
CAT4500(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT4500(config-pmap-c)# set ip dscp 24
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class VVLAN-ANY
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class class-default
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 5 mpbs 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# exit
CAT4500(config-pmap)# exit
CAT4500(config)#
CAT4500(config)#
CAT4500(config)# interface interface-id
CAT4500(config-if)# switchport voice vlan vvlan_id
CAT4500(config-if)# switchport access vlan dvlan_id
CAT4500(config-if)# qos trust device cisco-phone
CAT4500(config-if)# service-policy input IPPHONE-PC
CAT4500(config-if)# exit
CAT4500(config)#
CAT4500(confiig)# ip access list extended VVLAN-VOICE
CAT4500(config-ext-nacl)# permit udp Voice_IP_Subnet Subnet_Mask any range 16384 32767
dscp ef
CAT4500(config-ext-nacl)# exit
CAT4500(config)# ip access list extended VVLAN-CALL-SIGNALING
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet Subnet_Mask any range 2000 2002 dscp
cs3
CAT4500(config-ext-nacl)# exit
CAT4500(config)# ip access list extended VVLAN-ANY
CAT4500(config-ext-nacl)# permit ip Voice_IP_Subnet Subnet_Mask any
CAT4500(config-ext-nacl)# end
CAT4500#
```

Cisco 6500

```
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable) set qos policed-dscp-map 0, 24, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate VVLAN-VOICE rate 128 burst 8000 drop
CAT6500> (enable) set qos policer aggregate VVLAN-CALL-SIGNALING rate 32 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate VVLAN-ANY rate 5000 burst 8000 policed-dscp
CAT6500> (enable) set qos policer aggregate PC-DATA rate 5000 burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 46 aggregate VVLAN-VOICE udp
Voice_IP_Subnet Subnet_Mask any range 16384 32767
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Subnet_Mask any range 2000 2002
```

```
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate VVLAN-ANY Voice_IP_Subnet
Subnet_Mask any
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate PC-DATA any
CAT6500> (enable) commit qos acl IPPHONE-PC
CAT6500> (enable) set vlan vvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust-device ciscoipphone
CAT6500> (enable) set qos acl map IPPHONE-PC mod/port
CAT6500> (enable)
```

Cisco Unified Wireless IP Phone 7920G

By default, the Cisco Unified Wireless IP Phone 7920 marks its SCCP signaling messages using a Per-Hop Behavior (PHB) value of AF31 or a Differentiated Services Code Point (DSCP) value of 26 (this corresponds to a ToS value of 0x68), and it marks RTP voice packets using a PHB value of EF or a DSCP value of 46 (ToS of 0xB8). With proper queueing on the AP and configuration on the upstream first-hop switch to trust the AP's port, the wireless IP phone traffic will receive the same treatment as wired IP phone traffic. This practice allows the QoS settings to be consistent from LAN to WLAN environments.

In addition, the Cisco Unified Wireless IP Phone 7920 will automatically announce its presence to the AP using the Cisco Discovery Protocol (CDP). The CDP packets are sent from the wireless IP phone to the AP, and they identify the phone so that the AP can place all traffic to the phone in the high-priority queue.

While Ethernet switch ports can typically transmit and receive at 100 Mbps, 802.11b APs have a lower throughput rate that allows for a maximum data rate of 11 Mbps. Furthermore, wireless LANs are a shared medium and, due to contention for this medium, the actual throughput is substantially lower. This throughput mismatch means that, with a burst of traffic, the AP will drop packets, thus adding excessive processor burden to the unit and affecting performance.

By taking advantage of the policing and rate limiting capabilities of the Cisco Catalyst 3560 and 6500 Series switches, you can eliminate the need for the AP to drop excessive packets by configuring the upstream switch port to rate-limit or police traffic going to the AP. The switch port configurations in the following sections rate-limit the port(s) to a practical throughput of 7 Mbps for 802.11b and guarantee 1 Mbps for high-priority voice and control traffic. Furthermore, as indicated in the configuration examples, packets coming from the AP should be trusted and, based on the VLAN tag of each packet, the DSCP marking should either be maintained or marked down. Thus, packets sourced from the Cisco Unified Wireless IP Phone 7920 on the voice VLAN should maintain the appropriate DSCP marking, and packets source from data devices on the data VLAN should be remarked to a DSCP value of 0.

Cisco 3560

```
CAT3560(config)# mls qos
CAT3560(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
CAT3560(config)# mls qos map policed-dscp 24 26 46 to 8
CAT3560(config)# mls qos aggregate-policer AGG-POL-1M-VOICE-OUT 1000000 8000 exceed-action
policed-dscp-transmit
CAT3560(config)# mls qos aggregate-policer AGG-POL-6M-DEFAULT-OUT 6000000 8000
exceed-action drop
CAT3560(config)#
CAT3560(config)# class-map match-all EGRESS-DSCP-0
CAT3560(config-cmap)# match ip dscp 0
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all EGRESS-DSCP-8
CAT3560(config-cmap)# match ip dscp 8
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all EGRESS-DSCP-16
```

```
CAT3560(config-cmap)# match ip dscp 16
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all EGRESS-DSCP-32
CAT3560(config-cmap)# match ip dscp 32
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all EGRESS-DSCP-48
CAT3560(config-cmap)# match ip dscp 48
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all EGRESS-DSCP-56
CAT3560(config-cmap)# match ip dscp 56
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-any VOICE-SIGNALING
CAT3560(config-cmap)# match ip dscp 24
CAT3560(config-cmap)# match ip dscp 26
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all VOICE
CAT3560(config-cmap)# match ip dscp 46
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all INGRESS-DATA
CAT3560(config-cmap)# match any
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all INGRESS-VVLAN-VOICE
CAT3560(config-cmap)# match vlan vvlan-id
CAT3560(config-cmap)# match class-map VOICE
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all INGRESS-VVLAN-VOICE-SIGNALING
CAT3560(config-cmap)# match vlan vvlan-id
CAT3560(config-cmap)# match class-map VOICE-SIGNALING
CAT3560(config-cmap)#
CAT3560(config-cmap)# class-map match-all INGRESS-DVLAN
CAT3560(config-cmap)# match vlan dvlan-id
CAT3560(config-cmap)# match class-map INGRESS-DATA
CAT3560(config-cmap)#
CAT3560(config-cmap)# policy-map EGRESS-RATE-LIMITER
CAT3560(config-pmap)# class EGRESS-DSCP-0
CAT3560(config-pmap-c)# police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class EGRESS-DSCP-8
CAT3560(config-pmap-c)# police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class EGRESS-DSCP-16
CAT3560(config-pmap-c)# police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class EGRESS-DSCP-32
CAT3560(config-pmap-c)# police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class EGRESS-DSCP-48
CAT3560(config-pmap-c)# police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3560(config-pmap-c)# class EGRESS-DSCP-56
CAT3560(config-pmap-c)# police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class EGRESS-VOICE
CAT3560(config-pmap-c)# police aggregate AGG-POL-1M-VOICE-OUT
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class EGRESS-VOICE-SIGNALING
CAT3560(config-pmap-c)# police aggregate AGG-POL-1M-VOICE-OUT
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# policy-map INGRESS-QOS
CAT3560(config-pmap)# class INGRESS-VVLAN-VOICE
CAT3560(config-pmap-c)# set ip dscp 46
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class INGRESS-VVLAN-CALL-SIGNALING
CAT3560(config-pmap-c)# set ip dscp 24
CAT3560(config-pmap-c)#
```

```
CAT3560(config-pmap-c)# class INGRESS-DVLAN
CAT3560(config-pmap-c)# set ip dscp 0
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# class class-default
CAT3560(config-pmap-c)# set ip dscp 0
CAT3560(config-pmap-c)#
CAT3560(config-pmap-c)# interface interface id
CAT3560(config-if)# description 11Mb towards Wireless Access Point
CAT3560(config-if)# switchport access dvlan-id
CAT3560(config-if)# switchport voice vvlan-id
CAT3560(config-if)# mls qos trust dscp
CAT3560(config-if)# service-policy output EGRESS-RATE-LIMITER
CAT3560(config-if)# service-policy input INGRESS-QOS
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable) set qos policed-dscp-map 24,26,46:0
CAT6500> (enable)
CAT6500> (enable) set qos policer microflow VOICE-OUT rate 1000 burst 32 policed-dscp
CAT6500> (enable) set qos policer microflow DATA-OUT rate 6000 burst 32 drop
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 24 microflow VOICE-OUT ip any any
dscp-field 24
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 24 microflow VOICE-OUT ip any any
dscp-field 26
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 46 microflow VOICE-OUT ip any any
dscp-field 46
CAT6500> (enable) set qos acl ip AP-DATA-EGRESS dscp 0 microflow DATA-OUT ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-INGRESS dscp 24 ip any any dscp-field 26
CAT6500> (enable) set qos acl ip AP-VOICE-INGRESS trust-dscp ip any any
CAT6500> (enable) set qos acl ip AP-DATA-INGRESS dscp 0 ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl map AP-VOICE-EGRESS vvlan-id output
CAT6500> (enable) set qos acl map AP-DATA-EGRESS dvlan-id output
CAT6500> (enable) set qos acl map AP-VOICE-INGRESS vvlan-id input
CAT6500> (enable) set qos acl map AP-DATA-INGRESS dvlan-id input
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port vlan-based
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port trust trust-dscp
CAT6500> (enable)
```

Endpoint Features Summary

Table 12-1 summarizes the Cisco IP Telephony features for Cisco analog gateways and Table 12-2 summarizes the features for Cisco IP Phones.

Table 12-1 Analog Gateway Features

Feature	Cisco VG224[1]	Cisco ATA 186 and Cisco ATA 188
Ethernet Connection	Y[2]	Y[3]
Maximum number of Analog Ports	24	2
Caller ID	Y	N
Call Waiting	Y	Y
Caller ID on Call Waiting	N	N
Call Hold	Y[4]	Y
Call Transfer	Y[5]	Y
Call Forward	Y	Y
Auto-Answer	N	N
Ad Hoc Conference	Y	Y
Meet-Me Conference	Y	Y
Call Pickup	Y	Y
Group Pickup	Y	Y
Redial	Y	Y
Speed Dial	Y	Y
On-hook Dialing	N	N
Voice Mail Access	Y[6]	Y[7]
Message Waiting Indicator (MWI)	Y[7]	Y[7]
Music on Hold (MoH)	Y[8]	Y[9]
Mute	N	N
Call Preservation	N	N
Call Admission Control	N	N
Local Voice Busy-Out	N	N
Private Line Automatic Ringdown (PLAR)	Y	Y
Hunt Group	Y	Y
Dial Plan Mapping	N	N
Supervisory Disconnect	N	N
Signaling Packet ToS Value Marking	0x68	0x68
Media Packet ToS Value Marking	0xA0	0xA0
Fax Pass-Through	Y	Y
Fax Relay	N	N

Table 12-1 Analog Gateway Features (continued)

Feature	Cisco VG224[1]	Cisco ATA 186 and Cisco ATA 188
Skinny Client Control Protocol (SCCP)	Y	Y
Session Initiation Protocol (SIP)	Y	Y
H.323	Y	Y
G.711	Y	Y
G.729	Y	Y
Voice Activity Detection (VAD)	Y	Y
Comfort Noise Generation (CNG)	Y	Y

1. SCCP call control
2. Two 10BaseT/100BaseT
3. Two 10BaseT/100BaseT for Cisco ATA 188; one 10BaseT for Cisco ATA 186
4. SCCP call control
5. SCCP call control
6. Only on SCCP and SIP version
7. Only on SCCP and SIP version
8. Supports only unicast MoH
9. Supports only unicast MoH

Table 12-2 Cisco Unified IP Phone Features

Feature	7902G[1]	7905G	7910G	7910 +SW	7912G	7920G	7935G, 7936G	7940G	7960G	7970G
Ethernet Connection	Y[2]	Y[2]	Y[2]	Y[3]	Y[3]	N	Y[4]	Y[3]	Y[3]	Y[3]
Ethernet Switch	N	N	N	Y	Y	N	N	Y	Y	Y
Cisco Power-Over-Ethernet (PoE)	Y	Y	Y	Y	Y	N	N	Y	Y	Y
IEEE 802.3af Power-Over-Ethernet (PoE)	N	N	N	N	N	N	N	N	N	Y
Localization	N	Y	N	N	Y	N	N	Y	Y	Y
Directory Number	1	1	1	1	1	6	1	2	6	8
Liquid Crystal Display	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Caller ID	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Call Waiting	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Caller ID on Call Waiting	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Call Hold	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Call Transfer	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Call Forward	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Auto-Answer	Y	Y	N	N	Y	Y	N	Y	Y	Y
Ad Hoc Conference	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Meet-Me Conference	N	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 12-2 Cisco Unified IP Phone Features (continued)

Feature	7902G[1]	7905G	7910G	7910 +SW	7912G	7920G	7935G, 7936G	7940G	7960G	7970G
Call Pickup	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Group Pickup	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Redial	[5]Y	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y	Y
Speed Dial	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
On-hook Dialing	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Voice Mail Access	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Message Waiting Indicator (MWI)	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Video call	N	N	N	N	N	N	N	Y	Y	Y
Music on Hold (MoH)	Y	Y	Y	Y	Y	Y[6]	Y	Y	Y	Y
Speaker	N	Y[7]	Y[7]	Y[7]	Y[7]	N	Y	Y	Y	Y
Headset Jack	N	N	N	N	N	Y[8]	N	Y	Y	Y
Mute	N	N	Y	Y	N	Y	Y	Y	Y	Y
Disable General Attribute Registration Protocol (GARP)	Y	Y	Y	Y	Y	N	N	Y	Y	Y
Signaling and Media Encryption	N	N	N	N	N	Y[9]	N	Y	Y	Y
Signaling Integrity	N	N	N	N	N	N	N	Y	Y	Y
Manufacturing-Install ed Certificate (X.509v3)	N	N	N	N	N	N	N	N	N	Y
Field-Installed Certificate	N	N	N	N	N	N	N	Y	Y	N
Third-Party XML Service	N	Y	N	N	Y	N	N	Y	Y	Y
External Microphone and Speaker	N	N	N	N	N	N	N	N	N	Y
Hunt Group	Y	Y	Y	Y	Y	YN	Y	Y	Y	Y
Dial Plan Mapping	N	N	N	N	N	N	N	N	N	N
Signaling Packet ToS Value Marking	0x60	0x68	0x68	0x68	0x60	0x68	0x68	0x60	0x60	0x60
Media Packet ToS Value Marking	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
Skinny Client Control Protocol (SCCP)	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Session Initiation Protocol (SIP)	N	Y	N	N	Y	N	N	Y	Y	N
H.323	N	Y	N	N	N	N	Y	N	N	N
G.711	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
G.729	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Voice Activity Detection (VAD)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Comfort Noise Generation (CNG)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

1. Note that the complete names of these products have been truncated to save space in this table (each product number is preceded by the phrase “Cisco Unified IP Phone.”
2. One 10BaseT
3. Two 10BaseT/100BaseT

4. One 10BaseT/100BaseT
5. Last Number Redial
6. Supports only unicast MoH
7. One-way listen mode
8. The only supported headset for the Cisco Unified IP Phone 7920 is one with a 2.5 mm jack, available at http://www.cisco.getheadsets.com.
9. Signaling and Media Encryption are available with Static WEP and LEAP security configurations.

INDEX

Numerics

508 conformance **2-6**
802.1s **3-9**
802.1w **3-9, 3-11**
802.3af PoE **3-15**

A

aaa authentication command **11-6**
aaa new-model command **11-6**
AAD **1-7**
access control list. *See* ACL
Access Control Server. *See* ACS
accessibility of IP Telephony features **2-6**
Access Layer **3-9**
access point. *See* AP
ACL
  QoS policies **3-41**
ACS **3-38, 3-39**
  centralized **3-39**
  remote **3-39**
Active Directory. *See* AD
Active Voice, LLC
  Reception system **8-12**
AD **3-39**
additional information **xii**
Address Resolution Protocol. *See* ARP
after-hours block command **10-8**
after-hours blocking
  used to prevent toll fraud **10-12**
agents for call processing **1-4, 2-5**
Alerts and Activities Display. *See* AAD
analog
  gateways **12-2**
analog signaling
  connecting to PSTN **4-2, 4-3**
analog trunks **4-4, 4-5**
  configuring **4-6**
  features **4-7**
analog voice mail **8-10, 8-11**
  Active Voice Reception **8-12**
AP **3-33, 12-4**
  call admission control **12-8**
  configuration and design **3-37**
applications **1-2, 1-5**
  TAPI **8-14**
    Cisco CCC **8-18**
    Cisco CME TAPI Light **8-16**
    Cisco CME TSP **8-16**
    Cisco Unified CME TAPI Light **8-15**
    Cisco Unified CME TSP **8-18**
  XML **8-14, 8-19**
    Cisco Unified CME services **8-19**
    example application **8-20**
    general phone services **8-19**
architecture **1-2**
ARP **3-37**
asymmetric signaling **4-2**
Asynchronous Transfer Mode. *See* ATM
ATA **12-10**
ATM **2-4, 3-23, 3-31**
authentication **3-38**
  open **12-5**
Authentication, Authorization, and Accounting. *See*AAA
auto assign comnmand **10-9**

AUTO negotiate 3-16

B

B-ACD 1-1
BackboneFast 3-11
bandwidth
  best-effort 3-22
  call control traffic 3-26
  consumption 3-24, 3-25, 3-26
  guaranteed 3-21
  provisioning 3-19, 3-21, 3-24, 3-41
  voice class requirements 3-29
Basic Automatic Call Distribution. *See* B-ACD 1-1
benefits of
  distributed call processing 2-4
  single-site deployment 2-2
best-effort bandwidth 3-22
best practices for
  distributed call processing 2-4
  single-site deployment 2-2
  WAN design 3-20
billing
  Cisco Secure ACS 11-6
  RADIUS 11-6
  role of gatekeeper 6-11
  using account codes 11-7
BPDU 3-11
branch office Cisco Unified CME deployment 7-2
bridge protocol data unit. *See* BPDU
bursting 3-32

C

CA
  SCCP signaling via TLS 10-19
cabling
  Category 3 3-16
  IBM type 1A and 2A 3-16
CALEA
  lawful intercept 6-12
call activity
  monitoring 10-10, 11-6
call admission control
  for wireless access points 12-8
call agents
  recommendations for use 2-6
call control traffic 3-26
call detail records. *See* CDR
call forward
  configuring 5-1, 5-2
  for VoIP 5-4, 5-5
  interoperability with CallManager 5-7
call forwarding 7-10, 7-12
  H.450 services 6-23, 6-24
  on SIP networks 6-35
call history
  monitoring 10-10
CallManager. *See* Cisco CallManager
call processing
  agents 1-4, 2-5
  distributed 2-3
calls between Cisco Unified CallManager and Cisco Unified CME 7-2, 7-3
call transfer 7-4, 7-5
  and call forward interoperability with CallManager 5-7
  configuring 5-1, 5-2
    on VoIP networks 5-2, 5-3
  for VoIP
    configuring 5-4
  H.323-to-H.323 7-6
  H.323 with ECS 7-5, 7-6
  H.450 services 6-19, 6-21, 6-22
  interoperability with CallManager 5-7
  intersite call transfer 7-9
  SIP REFER 6-35
  transcoding MTP 7-7

campus
  access switch 3-3
  infrastructure requirements 3-1
capacity planning for
  wireless networks 12-6
CAPF
  SCCP signaling via TLS 10-19
CAS 4-9
Category 3 cabling 3-16
CCS 4-9
CDP
  disabling 10-6
CDR
  Cisco Secure ACS 11-6
  logging 11-6
Certificate Authority Proxy Function. *See* CAPF
Certificate Trust List. *See* CTL
Certification Authority. *See* CA
channel-associated signaling. *See* CAS 4-9
channels for wireless devices 3-34
CIR 3-32
Cisco CallManager
  described 1-4
Cisco CCC
  defined 8-18
  with Microsoft CRM 8-18
Cisco Centralized Key Management. *See* Cisco CKM
Cisco CKM 3-34
Cisco CRM Communications Connector. *See* Cisco CCC
Cisco Discovery Protocol. *See* CDP
Cisco IOS firewall
  with Cisco Unified CME 10-16
Cisco IOS translation rules 4-16, 4-17
Cisco IP Communicator 12-17
Cisco IP SoftPhone 12-17
Cisco LEAP 3-34, 3-38, 12-5
Cisco Networking Services Zero Touch 11-11
Cisco Secure Access Control Server. *See* Cisco Secure ACS
Cisco Secure ACS
  logging CDRs 11-6
Cisco Unified CallManager
  call processing agents 2-5
  calls to Cisco Unified CME 7-2, 7-3
  call transfer 7-4, 7-5
    H.323 with ECS 7-5, 7-6
    intersite call transfer 7-9
    transcoding MTP 7-7
  connecting to Cisco Unified CME systems 7-9
  connecting to CME systems 7-8
  H.450.x support 6-27
  recommended call agent 2-6
Cisco Unified CME 3-4
  AXL/SOAP interface
    network management 11-1, 11-2, 11-3
  branch office deployment 7-2
  calls from Cisco Unified CallManager IP phones 7-2, 7-3
  call transfer 7-4, 7-5
    H.323-to-H.323 7-6
    H.323 with ECS 7-5, 7-6
    intersite call transfer 7-9
    transcoding MTP 7-7
  Cisco IOS PSTN telephony interfaces
    analog trunks 4-4, 4-5, 4-6, 4-7
    digital trunks 4-7, 4-8, 4-9, 4-10
    DSP hardware 4-11
  commonly used port 10-23
  compared with Cisco Unity 8-3
  configuring for Cisco Unity 8-4, 8-5
  configuring for Octel analog integration 8-11, 8-12
  connecting to Cisco Unified Callmanager 7-8, 7-9
  connecting to PSTN 4-2
    with analog signaling 4-2, 4-3
    with digital signaling 4-3
  deployment models
    multisite business model 3-6, 3-8
    standalone office model 3-5, 3-6

  MWI Relay 8-6, 8-8
  recommended call agent 2-6
  SSAM
    configuring 8-9
  supported MIBs 11-8
  TAPI Light capability 8-15, 8-16
  TSP 8-16, 8-18
  with Cisco IOS Firewall 10-16
  with Cisco Unity 8-3, 8-4
  with integrated PSTN gateway 4-12
  with SSAM 8-8
Cisco Unified IP Conference Station 12-10
Cisco Unified IP Conference Station 7935 12-8
Cisco Unified IP Phone 7902G 12-3
Cisco Unified IP Phone 7905G 12-3
Cisco Unified IP Phone 7910G 12-3
Cisco Unified IP Phone 7910G+SW 12-3
Cisco Unified IP Phone 7912G 12-4
Cisco Unified IP Phone 7940G 12-4
Cisco Unified IP Phone 7960G 12-4
Cisco Unified IP Phone 7970G 12-4
Cisco Unified Operations Manager 11-14
Cisco Unified Service Montior 11-14
Cisco Unified Wireless IP Phone 7920G 12-4, 12-14
Cisco Unifed CallManager
  call transfer
    H.323-to-H.323 7-6
Cisco Unity 1-6
  compared with Cisco Unified CME 8-3
  compared with Cisco Unity Express 8-2
  configuring on Cisco Unified CME 8-4, 8-5
  licensing for voice mail-only deployment 8-2
  MWI relay 8-6, 8-8
  with multiple Cisco Unified CME systems 8-3, 8-4
  with MWI 8-6
  with standalone Cisco Unified CME system 8-3
Cisco Unity Express
  with Cisco Unified CME 8-1
CiscoWorks 2000 1-7
classification of
  traffic 3-9, 3-18, 3-40, 12-8
Class of Restriction. *See* COR
Class of Service. *See* CoS
CNS
  Zero Touch deployment 11-11
CO-based voice mail 8-13, 8-14
codecs
  G.711 2-1
  transcoding 6-25, 6-26
commands
  aaa authentication 11-6
  aaa new-model 11-6
  after-hours block 10-8
  auto assign 10-9
  dial-peer-cor 10-6
  dialplan-pattern 4-17, 4-18, 6-15
  gk ipaddr 6-9
  ip http authentication enable 10-1
  no auto-reg-ephone 10-9
  voicemail 6800 8-5
Committed Information Rate. *See* CIR
common channel signaling. *See* CCS 4-9
Common Information Additional Network Feature for H.323 6-24
commonly used ports
  Cisco Unified CME 10-23
Communications Assistance to Law Enforcement Agencies. *See* CALEA
Communicator 12-17
comparing call transfer in Cisco Unified CME and CallManager
  H.323-to-H.323 7-6
comparing call transfer in Cisco Unified CME and Cisco Unified CallManager 7-4, 7-5
  H.323 with ECS 7-5, 7-6
  intersite call transfer 7-9
  transcoding MTP 7-7
comparing Cisco Unified CME and Cisco Unity 8-3
compressed Real-Time Transport Protocol. *See* cRTP

conferencing
  MeetingPlace Express 1-5
  rich media 1-2
configuration examples for
  QoS 12-8
configuring
  analog trunks
    configuring on Cisco Unified CME 4-6
  call forwarding 5-1, 5-2, 5-4, 5-5
  call transfer 5-1, 5-2
    for VoIP 5-4
    on VoIP networks 5-2, 5-3
  Cisco Unified CME for Cisco Unity 8-4, 8-5
  Cisco Unified CME for Octel analog integration 8-11, 8-12
  Cisco Unified CME for SSAM 8-9
  dial plan
    digit manipulation features 9-3
    POTS dial peers 9-1
    VoIP dial peers 9-2
  digital trunks 4-8, 4-9
  DTMF relay 6-18
  H.450.x services 6-26
    proxy services 6-28, 6-29
  local/remote access 10-3, 10-6, 10-7, 10-8
  MWI for SSAM 8-10
conformance with Section 508 2-6
connected party name and number services 7-12, 7-13
connecting
  Cisco Unified CallManager to Cisco Unified CME systems 7-8, 7-9
connecting to PSTN 4-2
  analog signaling 4-2, 4-3
  digital signaling 4-3
connectivity options 2-4
control signaling 3-26
conventions xvi
COR
  used to prevent toll fraud 10-10
core switch 3-3
CoS 3-9, 12-10
cRTP 3-23, 3-28
CSR
  monitoring voice performance statisics 11-8
CTL
  SCCP signaling via TLS 10-19
customer contact 1-1

D

denial of service. *See* DoS
deploying
  Zero Touch 11-11
deployment models
  described 2-1
  DHCP 3-13
  multisite business model 3-6
    small enterprise 3-8
  multi-site WAN with distributed call processing 2-3
  single site 2-1
  standalone office model
    network architecture 3-4, 3-5, 3-6
desktop phones 12-3
devices
  codecs
    transcoding 6-25, 6-26
DHCP 3-12
  deployment models 3-13
  lease times 3-13
  Option 150 3-13
dial peer commands 4-15, 4-16
dial-peer cor command 10-6
dial plan
  digit manipulation features
    configuring 9-3
  POTS dial peers
    configuring 9-1
  VoIP dial peers

    - configuring 9-2
- dialplan-pattern command 4-17, 4-18, 6-15
- differential 12-7
- differential threshold 12-7
- differentiated services code point. *See* DSCP
- digital signaling
  - connecting to PSTN 4-3
- digital trunks 4-7, 4-8
  - configuring 4-8, 4-9
  - features 4-10
- digit manipulation 4-15
  - Cisco IOS translation rules 4-16, 4-17
  - dial peer commands 4-15, 4-16
  - dialplan-pattern command 4-17, 4-18
- digit manipulation features
  - configuring 9-3
- distributed call processing 2-3
- DNS 3-12
- document
  - conventions xvi
- documentation
  - related xii
- Domain Name System. *See* DNS
- DoS
  - protection against 3-10
- DSCP 3-9, 3-27
- DSP hardware 4-11
- DSP resources 6-25
  - in single-site deployment model 2-1
  - transcoding 6-25, 6-26
- DTMF
  - used with H.323 6-16
- DTMF relay
  - for SIP 6-33
  - on H.323 networks 6-16, 6-17, 6-18
- dual-tone multifrequency. *See* DTMF
- Dynamic Host Configuration Protocol. *See* DHCP

E

- E.164 4-15
- E.164 numbers 6-12, 6-13
- EAP 3-34, 3-38, 3-39
- ECS
  - call transfer on VoIP networks 5-3
- efficiency of links 3-28
- Empty Capabilities Set. *See* ECS
- endpoints
  - analog gateways 12-2
  - defined 1-5
  - features 12-17
  - wireless 12-4
- equations for calculating
  - bandwidth 3-27
- example XML application 8-20
- Extensible Authentication Protocol. *See* EAP

F

- features of endpoints 12-17
- forwarding calls
  - on SIP networks 6-35
  - VoIP 5-4, 5-5
  - with H.450 services 6-23, 6-24
- fractional T1 service 4-8
- Frame Relay 2-4, 3-23, 3-31
- full-blind transfers 6-22
- full-duplex 3-16
- FXO interfaces
  - features 4-7
- FXO Power Failover 4-18

G

- G.711 2-1
- G.711 codec
  - best practice 2-2

gatekeeper
  call admission control 2-4
  H.323
    role in billing 6-11
gatekeepers
  H.323
    role of 6-8, 6-10, 6-11
  Routed Signaling Gatekeepers 6-12
  routed signaling gatekeepers 6-11
gateways
  analog 12-2
  features 12-17
  QoS configuration examples 12-8
  VG224 12-2
  voice applications 4-1, 12-2
gk ipaddr command 6-9
guaranteed bandwidth 3-21
GUI
  access, securing 10-1
  HTTPS 10-2, 10-3

H

H.245 digit relay 6-18
H.323
  Cisco Unified CME integration 6-1, 6-2, 6-3
    internal call handling 6-15, 6-16
    multinode networks 6-6, 6-7, 6-8
    role of gatekeeper 6-8, 6-10, 6-11
    two-node networks 6-4, 6-6
  DTMF relay 6-16, 6-17, 6-18
  E.164 numbers 6-12, 6-13
  gatekeepers
    registering individual numbers 6-14, 6-15
  H.450.x services
    configuring 6-26
    proxy services 6-28, 6-29
  H.450 services
    call forwarding/transfer 6-19, 6-21, 6-22, 6-23, 6-24
  Routed Signaling Gatekeepers 6-12
  routed signaling gatekeepers 6-11
H.323 Facility Message
  call forwarding 5-5
H.323 gatekeeper
  routed signaling
    call forwarding/transfer 5-8
H.323-to-H.323 call transfer 7-6
H.323 with ECS 7-5, 7-6
H.450.12
  supplementary services capabilities 6-24
H.450.12 protocol
  call transfer on VoIP networks 5-3
H.450.2/3
  connected party name and number services 7-12, 7-13
H.450.2 transfer method 5-2
H.450.3 call forwarding 5-5
H.450.x services
  and Cisco Unified CallManager 6-27
  configuring 6-26
  proxy services 6-28, 6-29
H.450 services
  call transfer/forwarding 6-19, 6-21, 6-22, 6-23, 6-24
H.450 Tandem Gateway
  transfer and forward proxy function 5-6
H.450 Tandem Gateways
  configuring 6-29
H.450 Tandem IP-to-IP gateway 7-13
hairpin routing
  call forwarding 5-5
hairpin-routing VoIP call transfers 5-3
half-duplex 3-16
headers for voice packets 3-25
high availability of network services 3-9
his 7-8
Hot Standby Routing Protocol. *See* HSRP
HSRP 2-4
HTTPS
  GUI management 10-2, 10-3

hub-and-spoke topology 2-4, 3-3

I

IBM cabling
  1A and 2A cabling 3-16
IBM Cabling System (ICS) 3-16
IBM Cabling System. *See*ICS
ICS 3-16
impairments without QoS 3-20
infrastructure. *See* network infrastructure
inline power 3-15
Integrated Services Router. *See* ISR
integrating
  Cisco Unfied CME in VoIP networks
    SIP 6-29, 6-30, 6-32, 6-33, 6-34, 6-35
  Cisco UnfiedCME in VoIP networks
    SIP 6-35
  Cisco Unified CME in VoIP networks 6-1, 6-2
    H.323 6-3, 6-4, 6-6, 6-7, 6-8, 6-10, 6-11, 6-15, 6-16
  Cisco Unified CME with SSAM 8-8
interference
  WLAN 3-36
internal calls
  on VoIP networks 6-15, 6-16
intersite call transfer 7-9
IP Communicator 12-17
ip http authentication enable command 10-1
IP phones 12-3
  monitoring registration 10-10
  monitoring with syslog messages 11-5
  registering 10-9
IP Precedence 3-9, 3-27
IPSec 2-4
IP Security Protocol. *See* IPSec
IP Telephony 1-1, 1-2
IP Telephony Environment Monitor. *See* ITEM
ISR
  AP support 3-37
  DSP modules
    DSPresourses
      ISRs 6-25
ITEM 1-7
ITU-T H.450 services
  call transfer/forwarding 6-19, 6-21, 6-22, 6-23, 6-24

J

Java Telephony Applications Programming Interface. *See* JTAPI.
JTAPI
  SIP 1-6

L

LAN infrastructure 3-9
Layer 2 2-4, 3-9
Layer 3 3-9
LEAP 3-39
leased lines 2-4, 3-23
LFI 3-23, 3-28, 3-29
line speed mismatch 3-31
link efficiency 3-28
link fragmentation and interleaving. *See* LFI
LLQ 3-23, 3-27
LMHOSTS file 3-12
local access
  configuring 10-3, 10-6, 10-7, 10-8
low-latency queuing. *See* LLQ

M

management of the network 1-7
managing
  multisite Cisco Unified CME systems 11-13
  standalone Cisco Unified CME systems 11-11
Media Termination Point. *See* MTP
media termination point. *See* MTP

MeetingPlace Express 1-5

Message Waiting Indicator. *See* MWI

MIBs supported by Cisco Unified CME 11-8

MISTP 3-9

MLP 3-23

models for deployment. *See* deployment models

monitoring

- call activity 10-10, 11-6
- call history 10-10
- CSRs 11-8
- IP phones with syslog messages 11-5

MPLS 2-4, 3-20, 3-23

MTP

- call forwarding 7-11
- call transfer 7-7
- in single-site deployment model 2-1

multicast traffic

- WLAN 3-36

Multilink Point-to-Point Protocol. *See* MLP

multinode networks (H.323) 6-6, 6-7, 6-8

multi-party voice conferencing 1-5

multiple Cisco Unified CME system

- with Cisco Unity 8-3, 8-4

Multiple Instance Spanning Tree Protocol. *See* MISTP

Multiprotocol Label Switching. *See* MPLS

multisite business model 3-6

- small enterprise 3-8

multisite Cisco Unified CME systems

- managing 11-13

multi-site WAN with distributed call processing 2-3

MWI

- configuring for SSAM 8-10
- with Cisco Unity 8-6

MWI Relay 8-6, 8-8

N

NAT

- used with Cisco Unified CME 10-13

NetIQ Vivinet Manager 11-15, 11-16, 11-21

Network Address Translation. *See* NAT 10-13

network infrastructure

- access layer 3-9
- high availability 3-9
- LAN 3-9
- overview 1-3
- requirements 3-1
- roles 3-3
- WAN 3-20
- WLAN 3-33

network management 1-7

- with Cisco Unified CME AXL/SOAP interface 11-1, 11-2, 11-3

network services 3-12

Network Time Protocol. *See* NTP

no auto-reg-ephone command 10-9

NTP 3-14

O

Octel

- configuring on Cisco Unified CME 8-11, 8-12

open authentication 3-38, 12-5

Option 150 3-12

overlapping channels 3-34

oversubscription 3-32

P

packets

- headers 3-25

performance statistics

- monitoring 11-8

phones

- configuration 12-6
- desktop IP models 12-3
- features 12-17
- QoS 12-10

  roaming 3-34, 12-7
  software based 1-5
  web services 1-6
  wireless 12-4, 12-14
PoE 3-15
PortFast 3-11
POTS dial peers
  configuring 9-1
Power over Ethernet. *See* PoE
precedence settings
  network traffic 3-27
precedence settings for network traffic 3-9
prioritization of traffic 3-27
protocols
  ARP 3-37
  cRTP 3-23, 3-28
  DHCP 3-12
  HSRP 2-4
  IPSec 2-4
  MISTP 3-9
  MLP 3-23
  NTP 3-14
  RSTP 3-9, 3-11
  RTP 2-4
  SIP 2-4
  SRTP 3-25
  STP 3-11
  TFTP 3-14
  UDP 2-4
proxy services
  H.450.x configuration 6-28, 6-29
PSTN 2-1
  call switching 4-12
    with DID enabled 4-13
    with DNIS 4-13, 4-14
    with no DNIS 4-14
  connecting to 4-2
    with analog signaling 4-2, 4-3
    with digital signaling 4-3
  IP WAN 2-3
  trunk failover 4-18
PSTN-based voice mail 8-13, 8-14
Public Switched Telephone Network. *See* PSTN

Q

QBSS 12-7
QBSS-Differential Threshold 12-7
QCT 11-13
QoS
  configuration examples 12-8
  general 1-4
  LAN 3-17
  WAN 3-20, 3-22
  WLAN 3-40
QoS Basis Service Set. *See* QBSS
Quality of Service. *See*QoS
Quality of Service. *See* QoS.
queuing of voice traffic 3-19, 3-40
Quick Configuration Tool
  See QCT.

R

radio frequency. *See* RF
RADIUS 3-38, 3-39
  logging CDRs 11-6
Rapid Spanning Tree Protocol. *See* RSTP
Real-time Transport Protocol. *See* RTP
Reception analog integration 8-12
registering individual numbers with H.323 gatekeepers 6-14, 6-15
related documentation xii
Relative Signal Strength Indicator. *See* RSSI
remote addresses
  wtih public IP addresses 10-14
Remote Authentication Dial-In User Service. *See* RADIUS
remote phones

over VPN 10-15
with private IP addresses 10-14
remote system access
configuring 10-3, 10-6, 10-7, 10-8
RF
coverage 12-5
rich-media conferencing 1-2
RJ-45 3-16
roaming 3-34, 12-7
roles in the network infrastructure 3-3
root guard 3-11
routed signaling
call forwarding/transfer 5-8
Routed Signaling Gatekeepers 6-12
routed signaling gatekeepers 6-11
routers
roles and features 3-3
RSSI 12-7
RSSI-Differential Threshold 12-7
RSTP 3-9, 3-11
RTP 2-4
RTP-based digit relay 6-18
RTP-based DTMF digit relay 6-17

S

SCCP
blocking access by external phones 10-9
integrating external applications to Cisco Unified CME 8-1
procedure for configuring TLS signaling 10-20
signaling via TLW 10-19
Section 255 2-6
Section 508 2-6
security
Cisco Unified CME
best practices 10-1
controlling incoming and outgoing calls 10-6
GUI access 10-1
GUI management with HTTPS 10-2, 10-3
local/remote system access
configuring 10-3, 10-6, 10-7, 10-8
overview 1-6
troubleshooting 10-22
wireless network 3-38
Sequenced Routing Update Protocol. *See* SRTP
Service Inter-Working. *See* SIW
Service Set Identifier. *See* SSID
service set identifier. *See*SSID
Session Initiation Protocol. *See* SIP.
shaping traffic 3-31
shielded twisted-pair. *See*STP
Simple Object Access Protocol. *See* SOAP
single-site deployment model 2-1
SIP
Cisco Unfied CME integration 6-29, 6-30
call forwarding 6-35
DTMF relay 6-33
role of SIP proxy/registrar/redirect server 6-32
SIP REFER 6-35
supplementary services 6-34
two-node topology 6-30
Cisco Unified CME integration 6-1, 6-2
for distributed call processing 2-4
JTAPI 1-6
SIP REFER 6-35
site survey 12-5
SIW 2-4, 3-23
Skinny Client Control Protocol. *See* SCCP
small enterprise multisite business model 3-8
SNMP
access list 10-6
MIBs supported on Cisco Unified CME 11-8
SOAP
network management 11-1, 11-2, 11-3
SoftPhone 12-17
software-based phones 12-17
Solution Reference Network Design. *See* SRND.

Spanning Tree Protocol. *See* STP

SRND xi

SRTP 3-25

SSAM

- configuring on Cisco Unified CME 8-9

SSID 3-34, 3-37

- AP configuration 3-38

standalone Cisco Unified CME system

- with Cisco Unity 8-3

standalone Cisco Unified CME systems

- managing 11-11

standalone office model 3-4

- network architecture 3-4, 3-5, 3-6

Stonevoice 11-21, 11-28

Stonevoice Switch Answering Machine. *See* SSAM

STP 3-11, 3-16

supplementary services

- for SIP 6-34

survey of wireless network 12-5

switches, roles and features 3-3

symmetric signaling 4-2

syslog messages

- IP Phones, monitoring 11-5

T

TAPI 8-1

- application architecture 8-14
  - Cisco CCC 8-18
  - Cisco Unified CME TAPI Light 8-15, 8-16
  - Cisco Unified CME TSP 8-16, 8-18

TcL

- hookflash operation 8-12

Telecommunications Act 2-6

Telephony Application Programming Interface. *See* TAPI

TFTP 3-14

third-party

- software applications 1-2

threshold 12-7

Token Ring 3-16

toll fraud

- preventing 10-10, 10-12

Tool Command Language. *See* TcL

TouchTone digits 6-16, 6-17, 6-18

traffic

- call control 3-26
- classification 3-9, 3-18, 3-40, 12-8
- provisioning for 3-25
- queuing 3-19, 3-40
- shaping 3-31

traftraffic

- prioritization 3-27

transcoding 6-25, 6-26

transcoding MTP call transfer 7-7

transferring calls 5-1

- for VoIP 5-4
- on VoIP networks 5-2, 5-3
- SIP REFER 6-35
- with H.450 services 6-20, 6-21, 6-22

Transport Layer Security. *See* TLS

Trivial File Transfer Protocol. *See* TFTP

tromboning 6-24

troubleshooting

- security 10-22

trunk signaling systems 4-2

- analog 4-2, 4-3
- digital 4-3

trust 12-8

two-node networks (H.323) 6-4, 6-6

two-node topology (SIP) 6-30

U

UDC 3-16

UDLD 3-11

UDP 2-4, 3-28

UniDirectional Link Detection. *See* UDLD

unified communications 1-2

unified messaging 1-6
  See also messaging
uniform resource identifiers. *See* URI
uninterrupted power supplies. *See* UPS
Unity. *See* Cisco Unity
UplinkFast 3-11
UPS 3-15
URI
  endpoint resolution 2-5
User Datagram Protocol. *See* UDP

V

V3PN 2-4
VAD
  disabled 12-6
VAF 3-30
VATS 3-32
VG224 Voice Gateway 12-2
video telephony 1-2
virtual LAN. *See*VLAN
Virtual Private Network *See*VPN
VLAN 3-9, 3-34, 12-8
voice activity detection. *See* VAD
Voice-Adaptive Fragmentation. *See* VAF
Voice-Adaptive Traffic Shaping. *See* VATS
Voice and Video Enabled IPSec VPN. *See* V3PN
voice class bandwidth requirements 3-29
voice cut-through delay 7-3
voice gateway functionality 4-1
voice gateways 4-1, 12-2
voice mail
  analog 8-10, 8-11
    Active Voice Reception 8-12
  Cisco Unity
    Cisco Unity
        voice mail 8-2
    comparing with Cisco Unified CME 8-3
    configuring on Cisco Unified CME 8-4, 8-5
    licensing for voice mail-only deployment 8-2
    MWI Relay 8-6, 8-8
    with multiple Cisco Unified CME systems 8-3, 8-4
    with MWI 8-6
    with standalone Cisco Unified CME system 8-3
  CO-based 8-13, 8-14
  Octel
    configuring on Cisco Unified CME 8-11, 8-12
  SSAM 8-8
    configuring on Cisco Unified CME 8-9
voicemail 6800 command 8-5
voice over IP. *See* VoIP
voice performance statistics
  monitoring 11-8
VoIP 3-25
  call forward 5-4
  call forwarding 5-5
  call transfer configuration 5-4
  H.323
    call forwarding/transfer with H.450 service 6-24
    call forwarding/transfer with H.450 services 6-19, 6-21, 6-22, 6-23
    DTMF relay 6-16, 6-17, 6-18
    H.450.x services, configuring 6-26, 6-28, 6-29
VoIP dial peers
  configuring 9-2
VoIP networks
  Cisco Unified CME integration 6-1, 6-2
  H.323
    Cisco Unified CME integration 6-3, 6-4, 6-6, 6-7, 6-8, 6-10, 6-11
    E.164 numbers 6-12, 6-13
    internal call handling 6-15, 6-16
    registering individual numbers with gatekeepers 6-14, 6-15
  SIP
    call forwarding 6-35
    Cisco Unfied CME integration 6-29, 6-30
    DTMF relay 6-33
    role of SIP proxy/registrar/redirect server 6-32

    SIP REFER 6-35
    supplementary services 6-34
    two-node topology 6-30
VPN 2-4
  with remote phones 10-15

W

WAN
  network infrastructure 3-20
WAN aggregation router 3-3
web services 1-6
weighted fair queuing 3-27
WEP 12-5
  staic 3-38
Wire Equivalent Privacy. *See* WEP
wireless IP phones 12-4, 12-14
Wireless LAN Services Module. *See* WLSM 3-34
WLAN
  design and confifguration 3-33
  infrastructure 3-33
  multicast traffic 3-36
  QoS 3-40
  security 3-38
  wireless interference 3-36
WLSM 3-34

X

XML
  application architecture 8-14, 8-19
  applications
    Cisco Unified CME phone services 8-19
    example application 8-20
    general phone services 8-19

Z

Zero Touch
  deploying 11-11